Projet eCMR : le cadre légal de la lettre de voiture (CMR) et la protection de la vie privée dans le secteur du transport routier : rapport de Recherche n°2/Annexe 1 au Rapport d'Activité n°4 V.4 - Juillet 2010

Dos Santos, Cristina

Publication date:
2010

Document Version
le PDF de l'éditeur

Convention n°5750 relative au programme de recherche intitulé eCMR, mis en œuvre par le pôle de compétitivité « Logistics in Wallonia »

‘Projet eCMR’

Le cadre légal de la lettre de voiture (CMR) et la protection de la vie privée dans le secteur du transport routier

Rapport Recherche n°2

Annexe 1 – Rapport d’Activité n°4

V.4. - Juillet 2010

Centre de Recherches Informatique et Droit (C.R.I.D.)
F.U.N.D.P.

Auteur : Cristina Dos Santos

TABLE DES MATIERES

Introduction

1. Objet de la recherche

L'objet de la recherche du « Projet eCMR » est l'utilisation de CMR (lettres de voiture) papiers avec reconnaissance de l'écriture manuscrite, complétées par des informations CAN BUS et GPS, à des fins de gestion de flottes de véhicules et de respect des réglementations UE sans changement d'habitude.

A. Rappel des objectifs du projet[1]

Dans le domaine du transport et de la logistique, le CMR (lettre de voiture) est un maillon indispensable, obligatoire (transport pour compte propre et tiers/autrui) et légal (19 mai 1956, Genève). Il est cependant fastidieux à remplir et à exploiter, en particulier pour les petites et moyennes flottes, qui prestent des services pour des tiers.

Dans ce contexte, les Technologies de l'Information et de la Communication sont en mesure d'apporter une solution efficace, mais également une plus-value. Au delà du cadre légal définissant l'utilisation du CMR, il y a une opportunité :

- d'encoder automatiquement les informations du CMR,
- d'assurer une traçabilité sans faille,
- de rapatrier automatiquement les données vers le siège du transporteur,
- de croiser les données avec d'autres informations provenant du véhicule, afin d'associer coût et opération effectuée.

L'innovation principale consiste à doubler le CMR « papier » d'une copie digitale et à enrichir celle-ci d'informations pertinentes provenant du véhicule, du chauffeur et du système de géolocalisation. En effet, la généralisation de nouvelles technologies IT (tablettes électromagnétiques légères et basse consommation), de l'électronique au sein des véhicules (CAN, GPS), de moyens de communications multiples, (GSM/GPRS, BT, DSRC,…) offre de nouvelles opportunités. Certaines sont assez matures (par exemple suivi et routage de véhicules via GPS et module GPRS), d'autres sont encore mal exploitées au niveau du transport.

Les aspects de recherche et développement du projet CRM portent dès lors sur les domaines suivants :

- L'intégration et le traitement, par le biais des technologies TIC les plus récentes (*embedded-GRID*), des données disponibles au sein du véhicule,
- La reconnaissance automatique de l'information saisie au niveau de la tablette d'acquisition électromagnétique,
- La transmission de l'ensemble des informations de façon intelligente (routage opportuniste) vers les différents acteurs, mais également de véhicule à infrastructure et de véhicule à véhicule.
- Les aspects juridiques multiples liés au concept général du projet.

[1] Contenu repris en partie à la Convention n° 5750 relative au programme de recherche intitulé eCMR, mis en œuvre par le pôle de compétitivité « Logistics in Wallonia » : *Convention type Pôles – Version du 27.02.2007*, point 23 et suivants.

Au terme de la recherche, le consortium vise à réaliser l'acquisition de données CMR (en accord avec les réglementations UE), à des fins de gestion, d'échange d'informations et d'archivage, et parvenir à les associer aux données CAN BUS en vue d'une gestion fine de flottes de véhicules. Une attention particulière sera donnée à la localisation des remorques (qui relève également d'une problématique énergétique), ainsi qu'à la remontée de données à des fins environnementales.

L'innovation technologique de cette RECHERCHE consistera dans l'intégration de ces différentes technologies dans le cadre précis de systèmes embarqués sur véhicule, ainsi que via l'ajout d'un nouveau mode d'interaction avec un système embarqué M2M : l'acquisition et la commande via un formulaire manuscrit.

Une tablette d'acquisition d'informations introduites à main levée permet de créer un CMR électronique, tout en respectant les prescrits et habitudes liés à l'existence du CMR papier.

Cette approche conjointe permet au titulaire de gérer et de partager électroniquement l'information, tout en restant compatible avec des partenaires utilisant un équipement standard.

Orientations de la recherche du projet eCMR :

- Contrôle et traitement de l'information accélérés, par communication sans fil directe à courte portée avec le véhicule (chargement, contrôle, etc.).
- Acquisition numérique de données des formulaires CMR, recoupage avec l'information issue du véhicule (distance, consommation) et du chauffeur (données sociales).
- Routage opportuniste en utilisant plusieurs types de communication sans fil, via un réseau de téléphonie pour les données urgentes, via une communication locale chez le transporteur pour les autres données, etc.
- Exploitation des réseaux locaux au sein du véhicule regroupant les différents équipements présents (Tablette d'acquisition, GSM, PDA, ordinateur de bord).

L'objectif de ce projet est de proposer des solutions innovantes d'aide à la planification et surtout la traçabilité des matières transportées et produits dangereux, via l'utilisation de la feuille de route électronique.

Justifications économiques pour les flottes de transport:

- Maîtrise très précise des coûts.
- Gain de temps à l'encodage.
- Gain de temps pour la gestion de traçabilité
- Utilisation optimale des flottes et des temps de conduite.
- Optimisation des coûts de communication opportuniste.

B. Recherche du CRID

1) Tout d'abord, le CRID considérera la **validation du projet vis-à-vis de la législation européenne CMR**, étant donné que le cadre légal en la matière est très complexe et spécifique (***Partie 1***).

Toute la première partie de ce rapport a fait l'objet du Rapport de Recherche n°1 (*Annexe 1 au Rapport d'Activité n°1 de juillet 2008*). Nous l'intégrons au présent rapport afin d'assurer la cohérence et la compréhension de la recherche juridique effectuée tout au long du projet. Cependant, **quelques mises à jour ont dû être réalisées, car c'est un secteur où la législation change rapidement pour s'adapter à l'ère du numérique.**

2) Puis, la recherche du Crid portera surtout sur les **matières qui concernent la validation du projet en matière de respect de la vie privée** : analyse de l'application des législations de protection des données dans un contexte pouvant conduire à une (télé)surveillance, entre autres, **en s'attachant particulièrement à la protection des données dans le cadre des relations d'emploi.**

Dans cette partie, les questions de responsabilités des serveurs de tels systèmes de suivi des flottes de véhicule seront abordées sous les points spécifiques de la loi « vie privée », dans la mesure où l'absence de disponibilité des données à transmettre ou le défaut de qualité des données transmises pourront engendrer des dommages pour les entreprises participant au système, étant donné les exigences de « qualité des données » imposées par la législation (***Partie 2***).

N.B. : LE SOULIGNEMENT DANS LE TEXTE ET/OU LE GRAS SERVENT A UNE LECTURE PLUS « TRANSVERSALE » A L'INTENTION DES AUTRES PARTENAIRES NON JURISTES, ET A ATTIRER L'ATTENTION DU LECTEUR SUR DES POINTS LES PLUS IMPORTANTS DANS LE CADRE DU PROJET QUI NOUS INTERESSE.

Première partie : Les aspects juridiques liés à la lettre de voiture (CMR)

I/ Le cadre légal de la lettre de voiture (CMR)

La lettre de voiture (ou CMR, pour 'Contrat de Marchandises par Route') est **un document de voyage pour les marchandises que l'on transporte par route**, dont l'utilité principale est de **mentionner les principales caractéristiques du contrat de transport conclu entre le transporteur, l'expéditeur des marchandises et, éventuellement, le (ou les) destinataire(s)**.

Etant donné que souvent ce transport va se faire transfrontières, **dès 1956, l'Organisation des Nations Unies (ONU) est intervenue au niveau international afin de régler d'une manière uniforme les conditions du contrat de transport international de marchandises par route à titre onéreux**, surtout en ce qui concerne les documents à utiliser pour ce transport et la responsabilité du transporteur impliqué. Selon cette convention internationale, dite '**Convention CMR**'[2], les véhicules visés par celle-ci sont : les automobiles, les véhicules articulés, les remorques et les semi-remorques[3].

En **Belgique**, depuis la **loi « Transport » du 3 mai 1999**[4], la Convention CMR s'applique aussi au transport national, avec en plus quelques spécificités nationales, comme on le verra ci-après.

A. Les textes juridiques applicables au niveau international et communautaire

1) La Convention internationale CMR du 19 mai 1956

La convention de Genève, dite **Convention C.M.R. (Convention relative au contrat de transport international de Marchandise par Route)**, est intervenue au niveau international pour régler de manière uniforme les conditions de transport international par route et la responsabilité du transporteur. Elle a été signée le 19 mai 1956, dans le cadre de l'Organisation des Nations Unies, et **ses dispositions sont applicables de plein droit au transport entre deux pays, dont au moins l'un est un pays contractant**.

Actuellement, plus de cinquante pays ont déjà ratifié cette convention, dont tous les Etats membres de l'Union Européenne, la Norvège, la Suisse, la Biélorussie, la Bosnie-Herzégovine, la Croatie, la Fédération de Russie, le Kazakhstan, la Moldavie, la Yougoslavie, le Maroc et la Tunisie[5].

Toutefois, cette convention ne s'applique pas à certains types de transports, notamment aux :

- transports effectués sous l'empire de conventions postales internationales,

[2] Cf. Convention relative au contrat de transport international de marchandises par route (CMR) et Protocole de Signature, signés à Genève, en date du 19 mai 1956, Organisation des Nations Unies (ONU).

[3] Tels que définis par l'article 1 de la Convention sur la circulation routière du 19 septembre 1949 (références en bibliographie).

[4] Loi du 3 mai 1999 relative au transport de choses par route, *M.B. du 30/06/1999, p. 24507*.

[5] Toute la liste des pays qui ont ratifié la Convention CMR se trouve sur :
http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XI-B-11&chapter=11&lang=en

- transports funéraires,

- et transports de déménagement.

2) Le Protocole Additionnel à la Convention CMR concernant la lettre de voiture électronique du 21 février 2008

Depuis le mois de **février 2008, un Protocole Additionnel[6] à la Convention CMR a été adopté par la Commission Economique pour l'Europe (ONU), afin de « *faciliter l'établissement optionnel de la lettre de voiture par les procédés employés pour l'enregistrement et le traitement électroniques des données* ».**

Ce Protocole a été ouvert à la signature des Etats signataires de la Convention CMR du 27 mai 2008 au 30 juin 2009[7] dernier, toutefois il n'est **pas encore entré en vigueur (mi 2010)**. A ce jour, seuls huit pays ont déjà signé ce Protocole, dont la Belgique, la Finlande, la Lettonie, la Lituanie, la Norvège, la Suède et la Suisse, ainsi que les Pays-Bas[8].

Selon le SPF Mobilité et Transports[9], dès que le Protocole Additionnel aura été ratifié par le nombre de pays nécessaire[10], il sera directement applicable en droit belge. Il sera ensuite « confirmé »/transposé dans la réglementation nationale par une modification législative : **fin 2009, le Conseil des ministres belge a approuvé un Avant-projet de loi visant à approuver le Protocole additionnel à la Convention relative au contrat de transport international de marchandises par route (CMR) en matière de lettre de voiture électronique** (sur proposition de M. Steven Vanackere, ministre des Affaires étrangères), qui vise à *« compléter la Convention CMR, afin de permettre aux parties intéressées à un contrat de transport d'utiliser une lettre de voiture électronique qui, sous réserve des conditions du Protocole, aura la **même force probante que l'exemplaire papier*** ».

L'Avant-projet de loi belge précise également que : *« **une lettre de voiture électronique comprend les mêmes données que la lettre de voiture papier**. Elle **répond aux normes concernant la sûreté et la sécurité**, entre autres par **l'inaltérabilité de la communication** et par **l'identification et l'authentification des signatures de l'expéditeur et du destinataire**. La*

[6] Protocole Additionnel du 21 février 2008 à la Convention relative au Contrat de Transport International de Marchandises Par Route (CMR) concernant la Lettre de Voiture Electronique, Conseil Economique et Social de l'ONU (Commission Economique pour L'Europe, Comité des Transports Intérieurs, 70ème session), Genève, 19 – 21 Février 2008, Nations Unies (ONU).

[7] Selon l'article 7 du Protocole, celui-ci se trouvait à Genève pour signature du 27 au 30 mai 2008 inclus, puis au siège des Nations Unies à New York jusqu'au 30 juin 2009. Depuis, il est sujet à ratification par les Etats signataires et ouvert à l'adhésion des Etats non signataires. Cette ratification ou adhésion ne sont effectives qu'après dépôt d'un instrument auprès du Secrétaire général de l'ONU. Voir état des signatures et des ratifications sur : http://treaties.un.org/doc/publication/mtdsg/volume%20i/chapter%20xi/xi-b-11-b.fr.pdf

[8] Voir informations disponibles (en anglais) sur le site : http://www.unece.org/trans/main/sc1/sc1cmr.html, sur la *« Signing Ceremony for The Electronic Contract for the International Carriage of Goods by Road (e-CMR) »* du 27 mai 2008, aux « Palais des Nations » (ONU) à Genève.

[9] Ces informations ont été obtenues par un échange de mails en mai 2008 et en octobre 2009 avec un Agent Conseiller du SPF Mobilité.

[10] Actuellement, seuls trois pays (sur les huit qui ont déjà signé le protocole) l'ont déjà ratifié : les Pays-Bas (le 7 janvier 2009), la Suisse (le 26 janvier 2009) et la Lettonie (le 3 février 2010). Or, il faut qu'au moins 5 pays le ratifient pour que le Protocole entre d'office en vigueur (selon les dispositions de l'article 8 du Protocole).

fiabilité *de la lettre de voiture* ***sera garantie par une signature numérique ou électronique***[11]. *Tous les autres documents habituellement associés à la lettre de voiture, par exemple les pièces de douanes, pourront désormais être établis sous forme numérique. Pour les transporteurs, la numérisation de la lettre de voiture et des documents afférents constitue une simplification permettant de réduire les frais.* »[12]

De plus, le 'Document Informel n°12' de la Commission Economique pour l'Europe (Comité des transports intérieurs) des 23-25 février 2010 fait acte de l'adoption de la liste des principales décisions prises par le Comité des transports intérieurs à sa 72ème session, **dont différents points peuvent intéresser le partenariat de ce projet**, soit :

> *« À sa soixante-douzième session, le Comité des transports intérieurs:]*[13]
>
> *9 :* ***A noté*** *que, selon les termes mêmes de l'AETR, toute décision concernant la mise en œuvre de l'accord, y compris les aspects relatifs au tachygraphe numérique, relevait de la responsabilité des Parties contractantes à l'accord et non à celle du Comité, et* ***a noté*** *également que, malgré tous les efforts faits, la majorité des Parties contractantes à l'AETR qui ne sont pas membres de l'UE présentes à la réunion pourrait ne pas être en mesure de réaliser la mise en œuvre complète du tachygraphe numérique dans les délais impartis et, par conséquent, envisagerait la nécessité d'une prolongation;*
>
> *10.* ***A exhorté*** *les Parties contractantes à l'AETR qui ne sont pas membres de l'UE à prendre toutes les mesures nécessaires pour la mise en œuvre du tachygraphe numérique dans les délais prévus, et* ***a invité*** *les États membres de l'UE qui sont parties contractantes à l'AETR ainsi que le secteur privé à continuer à apporter toute l'aide possible aux pays non membres de l'UE concernés, pour leur permettre de respecter le délai fixé; (…)*
>
> *15.* ***A invité*** *les Parties contractantes à la Convention relative au contrat de transport international de marchandises par route (CMR) à adhérer au Protocole additionnel à la CMR permettant l'utilisation de la lettre de voiture électronique (e-CMR) ou à le ratifier;*
>
> *16.* ***A approuvé*** *l'établissement d'un groupe spécial informel d'experts sur les systèmes de transport intelligents (STI) relevant de la compétence du WP.1;*
>
> *17.* ***A décidé*** *de prolonger le mandat du groupe spécial informel d'experts des aspects théoriques et techniques de l'informatisation du régime TIR pour l'année 2010; (…)*
>
> *25.* ***A accueilli favorablement*** *la préparation opportune d'une feuille de route sur le travail et le fonctionnement futurs du Groupe de travail du transport modal et de la logistique (WP.24) devant servir de modèle aux autres organes de la CEE;*
>
> *26. A demandé au WP.24 de poursuivre son travail, si possible par le biais d'un groupe informel d'experts et la préparation d'un document soumis à discussion, sur les régimes de responsabilité civile régissant le transport intermodal et la résolution de conflits éventuels entre les dispositions juridiques du CMR (route), la COTIF (rail), la convention de Montréal (air) et les règles de Rotterdam récemment adoptées (mer);*
>
> *27. A recommandé que la Division des transports de la CEE, en collaboration avec les Etats membres, les organisations internationales, le secteur privé et les milieux universitaires, continue ses efforts en vue*

[11] Souligné par l'auteur pour accentuer l'importance des dispositions de cet avant-projet de loi (non encore disponible).

[12] Voir Communiqué de presse du Conseil des ministres du 27 novembre 2009, Service Communication du Conseil des ministres, Direction générale Communication externe - Chancellerie du Premier ministre, sous le titre « *Reconnaissance de la lettre de voiture électronique au même titre que la lettre papier* », p. 6, http://www.residencepalace.be/repository/news/e60/fr/e60c8ac3d5ebfc05abe3bd09347ffb6d-fr.pdf

[13] Souligné par l'auteur afin **d'attirer l'attention sur les points d'intérêt pour le partenariat du projet eCMR**. Les mots en gras font partie du texte original.

d'améliorer la sécurité des transports intérieurs, en organisant notamment l'échange d'informations et des meilleures pratiques; (…) »[14]

3) Le Règlement (CEE) n° 881/92 du 26 mars 1992 et le Règlement (CEE) n° 3118/93 du 25 octobre 1993

Ces deux règlements européens[15] sont également venus régler, d'une part, l'accès au marché des transports de marchandises par route dans la Communauté exécutés au départ ou à destination du territoire d'un État membre, ou traversant le territoire d'un ou de plusieurs États membres (Règlement n°881/92) et, d'autre part, les conditions de l'admission de transporteurs non-résidents aux transports nationaux de marchandises par route dans un État membre (Règlement n°3118/93), afin d'instaurer une **politique communautaire des transports commune à l'ensemble des Etats membres de l'Union Européenne**.

Ainsi, le Règlement n°881/92[16] instaure **l'obligation d'avoir une licence de transport communautaire pour pouvoir effectuer des transports internationaux de marchandises** à l'intérieur du territoire de l'Union Européenne (cf. art. 3 du Règlement, qui prévoit aussi un modèle européen de licence à son Annexe 1er[17]). Et le Règlement n°3118/93[18] instaure la **possibilité d'effectuer des « transports de cabotage »**[19], à titre temporaire, pour tout transporteur de marchandises par route pour compte d'autrui qui est titulaire de la licence communautaire prévue au règlement (CEE) n°881/92.

B. Les principes juridiques découlant de la Convention CMR

Comme nous l'avons déjà mentionné, la Convention CMR est intervenue au niveau international afin d'assurer une réglementation uniforme des conditions du contrat de transport international de marchandises par route à titre onéreux concernant les documents utilisés pour le transport (dont le contrat commercial entre transporteur et « client » est constaté par une lettre de voiture, le CMR), la responsabilité du transporteur et la responsabilité de l'expéditeur.

L'établissement de la lettre de voiture ou CMR lorsqu'il y a un transport international de marchandises est donc devenu obligatoire avec cette Convention **: ce document contient des renseignements importants relatifs au contrat de transport en lui-même, qui est lui aussi**

[14] Document informel N° 12, COMMISSION ECONOMIQUE POUR L'EUROPE, COMITE DES TRANSPORTS INTERIEURS, Soixante-douzième session, ONU, Genève, 23-25 février 2010, *Adoption de la liste des principales décisions prises par le Comité à sa soixante-douzième session.*

[15] Les règlements issus du droit européen sont directement applicables dans le système juridique des Etats membres (sans nécessité d'une loi de transposition).

[16] Règlement (CEE) n° 881/92 du Conseil du 26 mars 1992, concernant l'accès au marché des transports de marchandises par route dans la Communauté exécutés au départ ou à destination du territoire d'un État membre, ou traversant le territoire d'un ou de plusieurs États membres, J*.O. L 95 du 9.4.1992, p. 1–7.*

[17] Voir Annexe 6 au 'Rapport d'Activité n°1 du CRID' (juillet 2008).

[18] Règlement (CEE) n° 3118/93 du Conseil, du 25 octobre 1993, fixant les conditions de l'admission de transporteurs non-résidents aux transports nationaux de marchandises par route dans un État membre, J*.O. L 279 du 12.11.1993, p. 1–16.*

[19] Il s'agit ici de *« transports nationaux de marchandises par route pour compte d'autrui dans un autre État membre, sans y disposer d'un siège ou d'un autre établissement »* (art. 1er du Règlement n°3118/93 et son Annexe 1 qui prévoit le modèle européen d'« Autorisation de Cabotage »).

obligatoire. Il est donc de l'intérêt du transporteur de le compléter avec un maximum de précisions et de le faire signer par l'expéditeur car, **en cas de litige, seul son contenu fera foi** (sauf preuve du contraire).

Selon les nouvelles dispositions du Protocole Additionnel à la Convention CMR du 21 février 2008, il sera également possible d'établir des lettres de voiture CMR électroniques dès qu'il sera entré en vigueur[20]. **Toutefois,** leur établissement sera **subordonné à des conditions de mise en œuvre supplémentaires** car, en effet, l'article 5 de ce Protocole dispose que :

> « *1. **Les parties intéressées à l'exécution du contrat de transport conviennent des procédures et de leur mise en œuvre** pour se conformer aux dispositions du présent Protocole et de la Convention [CMR], notamment en ce qui concerne :*
>
> *(a) **la méthode pour établir et remettre la lettre de voiture électronique à la partie habilitée** ;*
>
> *(b) l'assurance que la lettre de voiture électronique conservera son **intégrité** ;*
>
> *(c) la façon dont le titulaire des droits découlant de la lettre de voiture électronique peut démontrer qu'il en est le titulaire ;*
>
> *(d) **la façon dont il est donné confirmation que la livraison au destinataire a eu lieu** ;*
>
> *(e) **les procédures permettant de compléter ou de modifier la lettre de voiture électronique** ;*
>
> *(f) les procédures de remplacement éventuel de la lettre de voiture électronique par une lettre de voiture établie par d'autres moyens.* »[21]

Nous allons donc voir ci-après quelles sont les conditions d'établissement du CMR, tel qu'il existe aujourd'hui, tout en anticipant sur le futur modèle électronique (**1)** ; sa valeur légale et son « utilité » juridique (**2)** ; le contenu de cette lettre de voiture (mentions obligatoires et facultatives à y apposer) (**3)** ; ainsi que les divers régimes juridiques concernant la responsabilité du transporteur (**4)**, et de l'expéditeur tels qu'ils ont été prévus par la Convention CMR (**5)**.

1) Les conditions légales relatives à l'établissement de la lettre de voiture

La Convention CMR prévoit plusieurs conditions d'établissement de la lettre de voiture CMR internationale. Ainsi, afin que le contrat de transport soit bien exécuté par les parties, la lettre de voiture **doit être obligatoirement établie (au moins) en trois exemplaires originaux, signés par l'expéditeur et par le transporteur** : le premier exemplaire doit être remis à l'expéditeur, le **deuxième doit accompagner la marchandise** et le troisième doit être retenu par le transporteur[22].

La lettre de voiture doit être **complétée avec un maximum de précisions et signée par l'expéditeur** (et, si elle est signée par toutes les parties, cela équivaut à acceptation par tous

[20] Voir partie précédente à ce propos. Rappelons qu'en Belgique il y a déjà une proposition d'avant projet de loi annoncée.

[21] Souligné par l'auteur. En outre, le point 2. du même article dispose que *« **les procédures énoncées doivent être mentionnées dans la lettre de voiture électronique et être aisément vérifiables** ».*

[22] Cf. dispositions de l'article 5 de la Convention CMR.

des mentions y apportées). De plus, si la nature de la (ou des) marchandise(s) l'exige, l'expéditeur (ou le transporteur) a le droit d'exiger l'établissement d'autant de lettres de voiture que nécessaire.

Puisque avec l'adoption du Protocole Additionnel à la Convention CMR du 21 février 2008 l'établissement d'une lettre de voiture électronique[23] sera bientôt possible, cela **permettra la communication électronique[24] des données enregistrées sur ce CMR sous certaines conditions** (souligné par l'auteur) :

- la lettre électronique devra contenir les **mêmes indications que la lettre de voiture papier visée par la Convention CMR**,
- le **procédé employé pour l'établissement de la lettre de voiture devra garantir** ***« l'intégralité des indications*** *qu'elle contient à compter du moment où elle a été établie pour la première fois sous sa forme définitive*[25] ».
- les indications contenues dans la lettre de voiture électronique pourront être complétées ou modifiés dans les cas admis par l'article 6 de la Convention CMR, **en tenant compte toutefois que « *la procédure employée pour [la] compléter ou [la] modifier [devra] permettre la détection en tant que telle de tout complément ou toute modification et assurer la préservation des indications originales de la lettre de voiture électronique* »**[26].
- Et enfin, l'article 6 du Protocole prévoit également que **tous les documents remis au transporteur** (et éventuellement faisant partie des mentions facultatives contenues dans le CMR) comme, par exemple, ceux permettant de faire passer la marchandise à la douane, **pourront être « *fournis par l'expéditeur au transporteur sous forme de communication électronique si ces documents existent sous cette forme et si les parties ont convenu des procédures permettant d'établir un lien*** *entre ces documents et la lettre de voiture électronique visée par le présent Protocole* ***dans des conditions de nature à en garantir l'intégrité.*** »

Les notions d'intégralité des informations, d'intégrité et de qualité du support seront donc fondamentales dans ce nouveau contexte numérique. Il s'agit là de conditions techniques à établir préalablement à toute utilisation numérique du document CMR et en tout état de cause selon « l'état de l'art » et le respect d'un « coût raisonnable »[27].

---

[23] La 'lettre de voiture électronique' a été définie par l'article 1er du Protocole Additionnel comme : *« une lettre de voiture émise au moyen d'une communication électronique par le transporteur, l'expéditeur ou toute autre partie intéressée à l'exécution d'un contrat de transport auquel la Convention s'applique, y compris les indications logiquement associées à la communication électronique sous forme de données jointes ou autrement liées à cette communication électronique au moment de son établissement ou ultérieurement de manière à en faire partie intégrante »*.

[24] Selon ce même article, une 'communication électronique' est *« l'information enregistrée, envoyée, reçue ou conservée par des moyens électroniques, optiques, numériques ou des moyens équivalents faisant que l'information communiquée soit accessible pour être consultée ultérieurement »*.

[25] Cf. article 4, 2. du Protocole, qui dispose que: «… ***Il y a intégrité des indications lorsque celles-ci sont restées complètes et n'ont pas été altérées****, exception faite de tout ajout et de toute modification intervenant dans le cours normal de la communication, de la conservation et de l'exposition* » (souligné par l'auteur).

[26] Cf. article 4, 3. du Protocole Additionnel.

[27] Par analogie aux conditions imposées par la législation « vie privée » (voir partie suivante).

Toutefois, les lois nationales devront préciser ces notions afin qu'il existe une certaine standardisation des procédures à travers les Etats signataires de la Convention CMR et du Protocole Additionnel. Comme nous l'avons mentionné plus haut, le Comité pour les Transports Intérieurs de la Commission de l'ONU a instauré un groupe de travail à ce sujet, invitant toutes les « parties prenantes » à s'investir dans l'élaboration de « standards » internationaux.

2) La valeur légale de la lettre de voiture

L'établissement d'une lettre de voiture CMR pour le transport routier est nécessaire et utile principalement parce qu'elle **fait foi, jusqu'à preuve du contraire, des conditions du contrat et de la bonne réception de la marchandise par le transporteur**. De plus, en cas d'absence de 'réserves motivées' sur la lettre de voiture, il existe automatiquement une **présomption légale que la marchandise et son emballage étaient en bon état apparent** au moment de la prise en charge par le transporteur[28].

Au-delà de ces considérations liées à la preuve, la Convention CMR établit également des **délais légaux d'action communs à tous les pays signataires** : ainsi, en cas d'action en justice éventuelle contre un transport soumis à la Convention CMR, les actions légales sont présumées être prescrites dans le délai d'un an, sauf en cas de dol ou de faute considérée comme équivalente au dol (d'après la loi de la juridiction saisie) où la prescription est de 3 ans[29].

En outre, en vertu de l'article 33 de la Convention CMR, le contrat de transport pourra également contenir une clause attribuant la compétence à un tribunal arbitral (à condition que celui-ci applique lui-même la Convention).

Enfin, selon les dispositions de l'article 2 du nouveau Protocole Additionnel de 2008, **la lettre de voiture électronique sera, quant à elle, considérée « *comme équivalent à la lettre de voiture visée à la Convention [CMR] et, de ce fait, aura la même force probante et produira les mêmes effets que cette dernière* »[30]**.

Cependant, il y aura une **formalité supplémentaire à respecter puisque son authentification sera soumise à une procédure particulière** : en effet, la lettre de voiture électronique **devra être authentifiée par les parties au contrat de transport «*moyennant une signature électronique[31] fiable garantissant son lien avec [la lettre de voiture]*[32] » ou**

[28] Cf. article 9 de la Convention CMR.

[29] Cette prescription (délai légal maximum d'action en justice) courra :

- soit à partir du jour où la marchandise a été livrée, dans le cas de perte partielle, d'avarie ou de retard ;
- soit à partir du 30ème jour après l'expiration du délai convenu, ou sinon, à partir du 60ème jour après la prise en charge de la marchandise par le transporteur, en cas de perte totale ;
- ou à partir de l'expiration d'un délai de 3 mois à dater de la conclusion du contrat de transport, dans tous les autres cas (cf. dispositions de l'article 32 de la Convention CMR).

[30] Souligné par l'auteur.

[31] Selon les définitions données par l'article 1 du Protocole Additionnel, une 'signature électronique' *« signifie des données sous forme électronique qui sont jointes ou liées logiquement à d'autres données électroniques et qui servent de méthode d'authentification. »*.

[32] Cf. article 3, 1. du Protocole Additionnel, qui précise que :

bien par « *tout autre procédé d'authentification électronique permis par la législation du pays où la lettre de voiture électronique a été établie* » (cf. article 3, §2 du Protocole Additionnel).

Il faudra donc rester attentif à l'adoption de la loi belge qui transposera les dispositions de ce Protocole, afin de pouvoir déterminer les conditions de cette authentification et quel choix sera effectué en matière d'authentification.

3) Le contenu obligatoire du CMR international

La lettre de voiture CMR est un document standard qui **doit reprendre quelques mentions obligatoires minimum du contrat de transport**, mais qui pourra contenir également d'autres mentions (facultatives, mais vivement recommandées) spécifiant des dispositions liées au transport en lui-même, et qui pourraient servir de preuve supplémentaire en cas de litige[33].

Comme nous l'avons déjà mentionné ci-dessus, en cas d'établissement d'une lettre de voiture électronique, le Protocole Additionnel de 2008 prévoit que celle-ci contienne toutes les indications de la lettre de voiture papier, et que celles-ci puissent être complétées ou modifiées seulement dans les cas admis par la Convention CMR et exposés ci-dessous[34].

a. Mentions obligatoires (art. 6 de la Convention CMR):

Selon les dispositions de l'article 6 de la Convention CMR, la lettre de voiture (CMR) internationale **doit contenir au moins** les indications suivantes :

1. le lieu et la date de son établissement;
2. le nom et l'adresse de l'expéditeur;
3. le nom et l'adresse du transporteur;
4. le lieu et la date de prise en charge de la marchandise et le lieu prévu pour la livraison;
5. le nom et l'adresse du destinataire;
6. la dénomination courante de la nature de la marchandise et le mode d'emballage**, et, pour les marchandises dangereuses, leur dénomination généralement reconnue**;
7. le nombre de colis, leurs marques particulières et leurs numéros;
8. le poids brut ou la quantité autrement exprimée de la marchandise;
9. les frais afférents au transport (prix de transport, frais accessoires, droits de douane et autres frais survenant à partir de la conclusion du contrat jusqu'à la livraison);

---

*« **La fiabilité** du procédé de signature électronique **est présumée**, jusqu'à preuve contraire, **lorsque la signature électronique :***

(a) est liée uniquement au signataire ;

(b) permet d'identifier le signataire ;

(c) a été créée par des moyens que le signataire puisse garder <u>sous son contrôle exclusif</u> ;

*(d) est liée aux données auxquelles elle se rapporte **de telle sorte que toute modification ultérieure des données soit détectable »*** (souligné et gras par l'auteur).

[33] Cf. article 6 de la Convention CMR.

[34] Toutefois, en cas de non-constatation du contrat de transport par une lettre de voiture, « *l'absence, l'irrégularité ou la perte de la lettre de voiture n'affecte ni l'existence ni la validité du contrat de transport qui reste soumis aux dispositions de [la Convention CMR]* » (cf. article 4 de la Convention CMR).

10. les instructions requises pour les formalités de douane et autres;
11. et l'indication que le transport est soumis, *« nonobstant toute clause contraire »*, au régime établi par la Convention CMR[35].

b. Autres mentions (facultatives):

De plus, s'il était nécessaire pour la bonne conclusion du contrat de transport, la lettre de voiture doit aussi contenir les suivantes indications :

1. l'interdiction du transbordement;
2. les frais que l'expéditeur prend à sa charge;
3. le montant du remboursement à percevoir lors de la livraison de la marchandise;
4. la valeur déclarée de la marchandise et la somme représentant l'intérêt spécial à la livraison;
5. les instructions de l'expéditeur au transporteur en ce qui concerne l'assurance de la marchandise;
6. le délai convenu dans lequel le transport doit être effectué;
7. et la liste des documents remis au transporteur.

Ces mentions sont facultatives, toutefois lorsque le contrat de marchandise se révèle plus complexe qu'un transport « habituel », ces mentions peuvent se révéler essentielles pour établir d'éventuelles responsabilités en cas de problèmes. L'article 6 de la Convention CMR précise également à son §3 que *« les parties peuvent porter sur la lettre de voiture toute autre indication qu'elles jugent utile. »*. Il est important de bien remplir toutes les parties de la lettre de voiture puisque, une fois qu'elle sera signée par toutes les parties, cela signifiera qu'elles en acceptent toutes les clauses (telles qu'elles ont été remplies).

Enfin, en cas de conclusion d'une lettre de voiture électronique, **les indications qui y seront inscrites devront être rendues accessibles « *à toute personne habilitée à cet effet* »**, c'est-à-dire par les parties qui l'ont signée au moyen d'une signature électronique *« fiable »*[36]. Ce qui exclut implicitement que ces indications soient communiquées à des tiers « non habilités » (voir implications dans la deuxième partie du rapport, concernant la protection des données à caractère personnel pouvant être contenues dans le CMR : ceci est fondamental pour le respect de la confidentialité des traitements de données où le responsable du traitement doit mettre en œuvre des mesures de sécurité techniques et organisationnelles).

4) Le régime de responsabilité du transporteur[37]

Selon les dispositions de **l'article 8 de la Convention CMR**, lors de la prise en charge de la marchandise, il appartient au transporteur de vérifier (pour autant que cela soit *« raisonnablement possible »*) plusieurs choses, soit :

[35] En effet, selon l'article 41 de la Convention CMR *« est nulle et de nul effet toute stipulation qui, directement ou indirectement, dérogerait aux dispositions de la Convention »*, cependant *« la nullité de telles stipulations n'entraîne pas la nullité des autres dispositions du contrat »*.

[36] Cf. article 3 du Protocole Additionnel. Cette notion de « fiabilité » devra toutefois être ultérieurement clarifiée par le droit national.

[37] Les dispositions légales se rapportant à la responsabilité du transporteur se trouvent aux articles 17 et suivants de la Convention CMR.

- l'exactitude des mentions fournies par l'expéditeur (sur la lettre de voiture CMR) relatives au nombre de colis, à leurs marques et leurs numéros ;
- ainsi que l'*« état apparent »* de la marchandise et de son emballage.

Toutefois, cette vérification se limite à l'*« apparence extérieure de la marchandise et à son emballage »* et, si elle s'avère impossible, le transporteur devrait apporter des observations sur le CMR, ce que l'on appelle « réserves »[38] (ex. : si l'emballage est défectueux ou insuffisant ; s'il y a un trop grand nombre de colis ; si le déchargement a été exécuté par le conducteur dans des conditions atmosphériques défavorables pour la marchandise à la demande du destinataire ; etc.).

Il faut souligner que, **à défaut de réserves, le transporteur sera présumé avoir reçu la marchandise et que son emballage était en bon état apparent, ainsi que d'avoir le nombre exact de colis (comme indiqué sur la lettre de voiture)**[39].

Concernant les obligations du transporteur, selon la Convention CMR, celui-ci est également tenu de mettre à la disposition de l'expéditeur *« un véhicule adapté aux marchandises à transporter »* et à procéder à l'enlèvement de la marchandise aux jours et heures convenus (ou, à défaut, dans un *« délai raisonnable »*). Toutefois, même si la Convention ne précise pas qui doit assumer la responsabilité des opérations de chargement, de déchargement et d'arrimage de la marchandise, elle précise que ces opérations peuvent faire l'objet d'une convention supplémentaire entre les parties.

En outre, **en cas de nouvelles instructions par le destinataire, c'est le transporteur qui sera tenu de répondre du préjudice résultant de l'inexécution de ces nouvelles instructions**, ainsi que du préjudice subi par l'exécution des nouvelles instructions, lorsque le premier exemplaire de la lettre de voiture CMR ne lui aurait pas été présenté. Ainsi, si les nouvelles instructions ne s'avéraient pas réalisables, il devrait en aviser immédiatement la personne qui donne ces instructions par écrit, afin d'avoir la preuve que la démarche a bien été effectuée.

Enfin, si l'exécution du contrat de transport devait être rendue impossible pour un motif quelconque (devant toutefois être *« sérieux »*[40]), selon la Convention CMR, avant l'arrivée de la marchandise à destination le transporteur doit demander instruction à la personne qui a le droit de disposer de la marchandise (qui sera, en général, l'expéditeur). Le même principe vaudra si le destinataire refuse de prendre livraison de la marchandise. En outre, si le transporteur n'a pas pu obtenir des instructions *« en temps utile »*, alors qu'il les a demandées en bonne et due forme, il « *devra prendre les mesures qui lui paraissent les meilleures dans l'intérêt de la personne ayant le droit de disposer de la marchandise* ». Cependant, il ne pourra en aucun cas se désintéresser ou abandonner la marchandise, car c'est lui qui sera responsable de la perte totale ou partielle, ou de l'avarie de la marchandise qui se produirait entre le moment de sa prise en charge et de sa livraison, ou du retard de la livraison.

Il existe, toutefois, quelques **exceptions à ce régime de responsabilité**, notamment si la perte, l'avarie ou le retard résultent de:

- une faute de l'ayant droit (expéditeur ou destinataire) ;

[38] Cf. article 8, §2 de la Convention CMR.

[39] Cf. article 9, §2 de la Convention CMR.

[40] Les notions de « sérieux », de « délai raisonnable », etc., pourront donner lieu à une libre appréciation par le juge en cas de litige, et seront définies au cas par cas (et selon usages de la profession).

- un ordre de l'ayant droit ;
- s'il existe un vice propre à la marchandise transportée ;
- ou encore s'il existe « *d'autres circonstances que le transporteur ne pouvait éviter* »[41].

Or, le transporteur devra prouver à ce moment-là que le dommage a pu découler d'un de ces cas invoqués, mais il ne pourra invoquer ni des défectuosités de son véhicule, ni une faute commise par son chauffeur, par exemple, pour se décharger de sa responsabilité[42].

Au-delà de ces exceptions, **le transporteur doit indemniser l'ayant droit en cas de perte totale ou partielle de la marchandise** : la Convention CMR prévoit que cette indemnité soit calculée sur base de la valeur de la marchandise au lieu et à l'époque de sa prise en charge (limitée toutefois à 8.33 DTS[43] par kilo de poids brut manquant[44]). De plus, le transporteur devra aussi rembourser (en totalité ou au *prorata* de la perte partielle) le prix du transport, les frais de douane et les autres frais encourus à l'occasion du transport. Toutefois, il pourra exiger un supplément de prix dès la conclusion du contrat de transport pour la responsabilité supplémentaire qui lui incombe (sauf si la perte, l'avarie ou le retard résultent d'une faute lourde ou d'un dol de la part du transporteur ou de son préposé). De même, l'ayant droit pourra considérer la marchandise comme perdue si elle n'a pas été livrée dans les 30 jours qui suivent l'expiration du délai convenu, ou dans les 60 jours qui suivent la prise en charge de la marchandise, lorsqu'aucun délai n'a été convenu.

Enfin, **le transporteur sera aussi tenu pour responsable s'il omettait de mentionner l'applicabilité de la Convention CMR dans son contrat** (de plus, **toute stipulation expresse contraire est nulle**[45]). Selon l'article 6, 1. du Protocole Additionnel, lorsqu'il y aura émission d'une lettre de voiture électronique, *« le transporteur [devra remettre] à l'expéditeur, à la demande de ce dernier, un récépissé des marchandises et toute indication nécessaire pour l'identification de l'envoi et l'accès à la lettre électronique visée par le [Protocole]. »*

Seules les parties au contrat de transport auront le droit d'invoquer la responsabilité du transporteur pour obtenir réparation d'un dommage et intenter des actions en justice contre lui : il s'agit donc soit de l'expéditeur, soit du destinataire. Toutefois, la Convention CMR prévoit que toute action en justice doit être intentée dans un délai d'un an, tant pour les questions de responsabilité que pour le paiement du prix du transport, sinon il y aura

[41] Cf. article 17 de la Convention CMR.

[42] En effet, l'article 3 de la Convention CMR dispose que : *« …le transporteur répond, comme de ses propres actes et omissions, des actes et omissions de ses préposés et de toutes autres personnes aux services desquelles il recourt pour l'exécution du transporteur lorsque ces préposés ou ces personnes agissent dans l'exercice de leurs fonctions. »*.

[43] DTS signifie 'Droit de Tirage Spécial', tel que défini par le Fonds Monétaire International (FMI). Selon le Protocole du 5 juillet 1978 à la Convention CMR *« le montant visé est converti dans la monnaie nationale de l'Etat dont relève le tribunal saisi du litige sur la base de la valeur de cette monnaie à la date du jugement ou à la date adoptée d'un commun accord par les parties »*.

[44] Selon le cours du DTS (voir site http://users.swing.be/airel.express/fr/convention_cmr.htm - source: U.P.T.R.), cela équivaut plus ou moins à environ 10 € par kg de marchandise (version : fin décembre 2009).

[45] Cf. article 41 de la Convention CMR.

prescription[46]. Ce délai est porté à trois ans en cas de dol ou de faute considérée par la loi comme équivalente au dol.

a. En cas de transporteurs successifs[47] :

Dans les cas où le transport est effectué par plusieurs transporteurs successivement, **le régime de responsabilité prévu par la Convention CMR est différent, puisque chaque transporteur sera tenu pour responsable du transport total**. Le transporteur qui accepte la marchandise du transporteur précédent devra délivrer à celui-ci un reçu daté et signé, et indiquer son nom et adresse sur le deuxième exemplaire de la lettre de voiture CMR, où il pourra, le cas échéant, y apposer ses propres réserves.

Dans ce cas précis, en cas d'action en responsabilité (en cas de perte, avarie ou retard), la partie lésée pourra la diriger soit contre le premier transporteur, soit contre le dernier transporteur, soit contre le transporteur qui aurait exécuté la partie du transport au cours de laquelle s'est produit le fait. Toutefois, celui qui aura payé l'indemnité aura le droit d'exercer un recours contre le (ou les) autres transporteurs, responsables du dommage.

Enfin, lorsque le dommage aura été causé par deux ou plusieurs transporteurs, chacun devra payer seulement un montant proportionnel à sa part de responsabilité ou à sa part de rémunération du transport.

5) Le régime de la responsabilité de l'expéditeur[48]

L'article 12 de la Convention CMR précise, quant à lui, que *« l'expéditeur a le droit de disposer de la marchandise pendant toute la durée du transport »*, celui-ci pourra donc : soit faire arrêter le transport, soit modifier le lieu de destination, soit décider de faire livrer la marchandise à un destinataire différent de celui prévu sur la lettre de voiture. Toutefois, dès l'arrivée à destination de la marchandise, lorsque le deuxième exemplaire de la lettre de voiture aura été remis au destinataire, c'est seulement ce dernier qui pourra disposer de la marchandise : il pourra donc exiger que la marchandise lui soit livrée ou qu'elle soit livrée à un autre destinataire (mais ce dernier ne pourra pas désigner à son tour d'autres destinataires).

Il existe des conditions supplémentaires à respecter en cas de nouvelles instructions par l'expéditeur :

- L'expéditeur ou le destinataire devront inscrire les nouvelles instructions sur le premier exemplaire de la lettre de voiture et le présenter au transporteur ;
- L'expéditeur devra dédommager le transporteur des frais et du préjudice occasionné par l'exécution des nouvelles instructions ;
- L'exécution devra être possible au moment où les instructions sont données ;
- Les instructions ne devront pas entraver « l'exploitation normale » de l'entreprise de transport, ni porter préjudice aux expéditeurs ou destinataires d'autres envois ;

[46] Cette prescription court à partir du jour où la marchandise est livrée en cas de perte partielle, d'avarie ou de retard ; et à partir du 30ème jour après l'expiration du délai de livraison convenu, ou à défaut de celui-ci, à partir du 60ème jour après la prise en charge de la marchandise, en cas de perte totale de la marchandise. Dans tous les autres cas, elle court après 3 mois à dater de la conclusion du contrat. Ce délai de prescription sera suspendu en cas de réclamation écrite (cf. article 32 de la Convention CMR).

[47] Cf. articles 34 et suivants de la Convention CMR.

[48] Cf. article 10 et suivants de la Convention CMR.

- Et les instructions ne pourront pas avoir pour effet de diviser l'envoi.

De plus, **l'expéditeur pourra être considéré comme le responsable envers le transporteur des frais et dommages causés aux personnes, au matériel ou à d'autres marchandises s'il s'agit d'une défectuosité de l'emballage de sa marchandise ou s'il n'a pas indiqué la mention « marchandises dangereuses » quand il y avait lieu de le faire**. Il est aussi **responsable de la mise à la disposition de tous les documents nécessaires pour l'accomplissement des formalités de douane ou autres par le transporteur**.

En conclusion, l'on peut dire qu'en ce qui concerne le transport des marchandises sur le territoire européen, étant donné que tous les pays membres de l'UE sont signataires de la Convention CMR, même si le document CMR en lui-même n'est pas identique sur la forme (langue différente, disposition différente des rubriques obligatoires, etc[49]), il devra contenir toutes les mentions obligatoires imposées par cette Convention et respecter les dispositions légales susmentionnées[50].

C. Le régime juridique CMR applicable en Belgique[51]

En Belgique, la Convention CMR s'applique de plein droit depuis 1962 et plusieurs dispositions législatives sont venues compléter les obligations légales en la matière, ce que nous étudierons ci-après.

1) Champ d'application de la loi du 3 mai 1999[52] :

Selon l'article 38, §1er (cf. « contrat de transport ») de la loi du 3 mai 1999 relative au transport de choses par route :

> « *Les dispositions de la Convention relative au contrat de transport international de marchandises par route, ou Convention CMR, signée à Genève le 19 mai 1956 et approuvée par la loi du 4 septembre 1962 ainsi que les dispositions du Protocole à la convention précitée, signé à Genève le 5 juillet 1978 et approuvé par la loi du 25 avril 1983, sont applicables au transport national de choses par route.* »

Toutefois, par dérogation, *« le Roi peut décider que [les mentions figurant à l'article 6 de la Convention CMR] ne sont pas applicables aux transports nationaux de choses par route qu'il*

[49] Voir un exemple sur le document reprenant un « Tableau comparatif des régimes français et CMR du contrat de transport routier de marchandises », *Comparaison CMR et droit interne*, de F. Letacq – IDIT, disponible sur : http://www.idit.asso.fr/docenligne/documents/comparaison_cmr.pdf?PHPSESSID=e5cdad1062601f8c5b9c90884af82a50.

[50] Voir modèle CMR international délivré par l'IRU (Union internationale des transports routiers - *International Road Transport Union*) sur son site :

http://www.iru.org/index/cms-filesystem-action?file=services_download/lettrevoitrefinal.pdf (ou notre 'Annexe 7' du « Rapport d'Activité n°1 » de juillet 2008).

Ainsi que le 'Protocole additionnel à la CMR du 17-19 octobre 2006' concernant l'*« Harmonisation des prescriptions applicables aux opérations de transport international par route et facilitation de ces opérations »*, Conseil Economique et Social de l'ONU.

[51] Toutes les informations pertinentes concernant le transport pour compte de tiers pour les entreprises établies en Belgique se trouvent sur le site du SPF Mobilité et Transports sur : http://www.mobilit.fgov.be/fr/index.htm (Rubrique: Route - Transport de marchandises).

[52] Loi du 3 mai 1999 relative au transport de choses par route, *M.B. 30.06.1999.* Les articles qui nous concernent sont surtout les articles 23 et 24, et 38 et suivants.

détermine », c'est-à-dire que sont exclus : les transports postaux effectués dans le cadre d'un service public; les transports funéraires et les déménagements[53].

Depuis la loi du 3 mai 1999 le principe qui s'applique est que **tout 'envoi'[54] doit donner lieu à l'établissement d'une lettre de voiture** (cf. art. 23 de la loi).

Selon les dispositions de l'article 24 :

> *« §1* ***Le Roi détermine*** *(ou délègue au Ministre des Transports) :*
>
> *1° les* ***différents modèles de lettre de voiture et les indications qui doivent y figurer****,*
>
> *2° le nombre d'exemplaires des lettres de voiture et l'usage qui doit en être fait,*
>
> *3° les* ***organismes habilités à délivrer les lettres de voiture****, ainsi que les conditions de cette délivrance et le contrôle qui y est relatif. »* (souligné par l'auteur).

De plus, cette loi **impose que cette lettre de voiture soit présentée sur demande *« à tout agent désigné par le Roi pour contrôler et constater des infractions à la loi »*** (cf. art. 26, §2.c)), et des peines à cette infraction sont prévues au 'Livre Ier' (Chap. VII, art. 85) du Code pénal[55].

En ce qui concerne le **régime de responsabilité**, l'article 37 de la loi du 3 mai 1999, modifié par l'article 12 de la loi du 24 mars 2003 relative au transport de choses par route, prévoit une **responsabilité accrue du donneur d'ordre[56], du chargeur[57] et de l'intermédiaire de transport[58]** :

- Du **chargeur**, car celui-ci **doit s'assurer que la lettre de voiture (CMR) requise a bien été ou non établie préalablement à l'exécution d'un transport de choses** (il sera tenu pour responsable même si *« par défaut de prévoyance et de précaution »*) (cf. art.37, §1, 2°).

Il est utile de préciser que, **pour vérifier la légalité d'une lettre de voiture (CMR) fournie, on peut distinguer deux situations** :

---

[53] Cf. article 38, §3 de la loi. Et l'article 3 de l'A.R. du 7 mai 2002 concernant les « dispenses ».

[54] Par "envoi" on entend: *« une ou plusieurs choses chargées en un ou plusieurs endroits pour un seul donneur d'ordre et destinées à être transportées en un seul voyage et au moyen d'un seul véhicule automobile ou d'un seul train de véhicules, vers un ou plusieurs lieux de déchargement, pour un seul destinataire.»* (cf. art. 2, 12° de la loi du 3 mai 1999).

[55] L'on retrouve également les sanctions pécuniaires (amendes de 50 €) en cas d'absence de lettre de voiture établie pour l'envoi à bord du véhicule (cf. art. 23 et 26, §2, 2°, c de la Loi du 3 mai 1999 et art. 56 de l'AR du 7 mai 2002).

[56] La loi belge entend par "donneur d'ordre" *« toute personne physique ou morale qui a conclu un contrat de transport avec le transporteur »*.

[57] Et par "chargeur" *« toute personne physique ou morale qui met matériellement les choses à transporter à la disposition du transporteur »*.

[58] L'"intermédiaire de transport " est *« le commissionnaire de transport ou le commissionnaire-expéditeur »* (cf. informations fournies sur le site : http://www.mobilit.fgov.be/fr/index.htm, rubrique « La co-responsabilité des donneurs d'ordre, chargeurs et intermédiaires de transport »).

- si la lettre CMR est produite par un transporteur belge (ou par un transporteur étranger effectuant du cabotage en Belgique), le chargeur pourra la comparer avec les modèles de lettres de voiture existants[59] ;
- par contre, s'il s'agit d'un transporteur étranger, le chargeur pourra **s'assurer que la lettre de voiture reprend au moins les mentions obligatoires requises par l'article 6 de la Convention CMR**[60].
    - Du donneur d'ordre (ou, le cas échéant, de l'intermédiaire de transport) : en ce qui concerne la **vérification de la capacité d'un transporteur à effectuer un transport**, il **doit s'assurer**, au moment de la conclusion du contrat de transport, **qu'une "copie" de la licence de transport[61] (requise également par la loi) a bien été délivrée pour le véhicule automoteur utilisé**[62].

En effet, les objectifs du législateur belge en matière de responsabilité sont, d'une part, de dissuader les « co-acteurs » au transport à utiliser les services d'un transporteur qui ne serait pas en ordre et, d'autre part, de réduire la pression à laquelle certains « co-acteurs » peuvent soumettre les transporteurs.

En ce qui concerne le sujet qui nous occupe, nous devons attirer l'attention aussi que **le donneur d'ordre, le chargeur, le commissionnaire de transport ou le commissionnaire-expéditeur sont également punissables s'il est prouvé qu'ils ont donné des instructions ou posé des actes ayant entraîné plusieurs conséquences, dont** :

- un dépassement des masses (surcharge) et des dimensions maximales autorisées des véhicules;
- le non-respect des prescriptions relatives à la sécurité du chargement des véhicules;
- **le non-respect des prescriptions relatives aux temps de conduite et de repos des conducteurs de véhicules**;
- **et/ou le dépassement de la vitesse maximale autorisée des véhicules**[63].

Ce qui implique que ces derniers puissent vouloir augmenter le contrôle et la surveillance tant de leurs véhicules que de leurs conducteurs en interconnectant les informations obtenues par

[59] Voir Annexes 2, 3 et 4 du 'Rapport d'Activité n°1' du CRID (juillet 2008).

[60] Citées précédemment (voir « contenu obligatoire du CMR international » pt. a. et b.)

[61] Il existe ainsi un **modèle de licence de transport international analogue pour tous les Etats extérieurs à l'Union Européenne** (voir 'Annexe 5' du 'Rapport d'Activité n°1' du CRID) **et des modèles de licence de transport communautaire en plusieurs langues** (voir modèle en français en 'Annexe 6' du 'Rapport d'Activité n°1' du CRID).

[62] S'il s'agit d'un transporteur belge, le **moyen de vérification le plus efficace** pour qu'il s'assure qu'un transporteur déterminé est bien autorisé à effectuer des transports, consiste à **consulter la rubrique « Recherche d'entreprises de transport autorisées » (sous le site : http://www.mobilit.fgov.be/fr/index.htm), à y rechercher le transporteur concerné, et à s'assurer ainsi qu'il est bien autorisé à effectuer le transport**. Ou bien, s'il s'agit d'un transporteur étranger, cette vérification peut être assurée en lui demandant de produire, préalablement à la conclusion du contrat, une copie de sa licence de transport communautaire (s'il s'agit d'un transporteur établi dans l'Union européenne) ou de sa licence de transport international (s'il s'agit d'un transporteur établi hors de l'Union européenne). Ces copies peuvent être transmises par la poste, par télécopie ou par tout autre moyen de télécommunication.

[63] Cf. article 37, §2 de la loi du 3 mai 1999.

les différents systèmes embarqués dans le véhicule (tachygraphe, CMR, etc) : une balance des intérêts devra donc être effectuée lorsque ces informations impliquent des traitements de données à caractère personnel**, en tenant compte qu'il existe d'autres obligations légales (dont celle-ci) qui imposent à ces acteurs un certain « contrôle » de leur flotte (qui passe par une surveillance accrue des conducteurs)** [64].

En ce qui concerne l'établissement du prix du transport, la loi dispose également que le transporteur, le donneur d'ordre ou le commissionnaire de transport seront punissables s'il est prouvé qu'ils ont *« offert, exécuté ou fait exécuter un transport moyennant un prix 'abusivement bas'*[65] *»*, ce qui entraînerait un **problème de concurrence** dans le marché du transport de marchandises pour le compte d'autrui. La loi de 1999 prévoit en outre que les actions récursoires dérivant du contrat de transport de marchandises par route doivent, sous peine de déchéance, être introduites dans un délai d'un mois à dater de l'assignation qui donne lieu au recours (cf. art.38, §4 de la loi).

2) L'Arrêté Royal du 7 mai 2002[66]:

L'arrêté royal du 7 mai 2002 vient compléter les dispositions de la loi du 3 mai 1999 et concerne tout spécialement les transports effectués sur le territoire de l'Union européenne ou de l'Espace économique européen au moyen d'un véhicule immatriculé à l'étranger (art. 56) : en effet, ceux-ci ne sont pas soumis à l'établissement d'une lettre de voiture conforme au modèle déterminé par le Ministre belge lorsque les marchandises sont accompagnées d'une lettre de voiture CMR telle que visée aux articles 5 et 6 de la Convention CMR (ou par un accord conclu entre la Belgique et le pays d'immatriculation du véhicule concerné ; ou conforme aux prescriptions du Règlement (CEE) n°11 du 27 juin 1960 du Conseil de la Communauté économique européenne[67]).

De plus, **l'article 3 de cet A.R. crée toute une série de dispenses pour l'établissement d'une lettre de voiture** (CMR), qui ne sera pas requise pour les transports suivants:

- en trafic national[68] pour :
    1. les transports de choses effectués au moyen d'un véhicule automobile ou d'un train de véhicules dont la charge utile n'excède pas 500 kg;
    2. les transports de choses effectués hors de la voie publique;
    3. les transports de bagages effectués au moyen d'un véhicule automobile construit exclusivement pour le transport de personnes ou au moyen d'une remorque couplée à ce véhicule automobile;

[64] Voir partie suivante sur la protection des données à caractère personnel dans la relation d'emploi.

[65] On entend par "prix abusivement bas" : *« un prix insuffisant que pour couvrir à la fois : les postes inéluctables du prix de revient du véhicule, notamment l'amortissement ou le loyer du véhicule, son entretien et le carburant; les coûts découlant des obligations légales ou réglementaires, notamment en matières sociale, fiscale et de sécurité; et les coûts découlant de l'administration et de la direction de l'entreprise. »* (cf. indications sur le site SPF Mobilité et Transports, précité).

[66] Arrêté royal du 7 mai 2002 relatif au transport de choses par route, *M.B. 30.05.2002.*

[67] Cf. Article 6 du Règlement n° 11 concernant la suppression de discriminations en matière de prix et conditions de transport : celui-ci établit la responsabilité du transporteur pour l'établissement régulier des documents de transport (dont le CMR).

[68] C'est-à-dire si les véhicules concernés ne franchissent pas la frontière belge.

4. les transports de véhicules endommagés ou en panne;
5. les transports de véhicules déplacés sur réquisition des agents qualifiés à cet effet;
6. les transports locaux effectués en vue de l'épandage sur la voie publique de matières destinées à protéger la circulation lorsque celle-ci est rendue dangereuse par des phénomènes météorologiques ou autres;
7. les transports postaux effectués dans le cadre d'une mission de service public;
8. les transports de valeurs effectués dans au moyen de véhicules spécialement conçus à cet effet;
9. les transports funéraires;
10. et les transports de médicaments, d'appareils et d'équipements médicaux ainsi que d'autres articles nécessaires en cas de secours d'urgence, notamment en cas de catastrophes.

- et en trafic international[69] pour :
  1. les transports postaux effectués dans le cadre d'une mission de service public;
  2. et pour les transports funéraires.

De plus, selon l'article 57 de cet arrêté, **c'est le Ministre des Transports qui détermine :**

« 1° les différents modèles de lettres de voiture *;*

2° le nombre d'exemplaires des lettres de voiture, à qui ils sont destinés ainsi que les indications qui doivent y figurer ;

3° ***les organismes habilités à délivrer les lettres de voiture, les conditions de cette délivrance et le contrôle y relatif.*** *»*

Ce **contrôle** est, quant à lui, **prévu par l'article 58** qui dispose que :

« Sont désignés pour rechercher et constater les infractions à la loi et à ses arrêtés d'exécution:

1° les fonctionnaires de police de la police fédérale et de la police locale;

2° les agents de l'administration compétente pour le transport de choses par route, qui sont investis d'un mandat de police judiciaire;

3° les agents de l'Administration des Douanes et Accises. » (souligné par l'auteur).

3) L'Arrêté Ministériel du 8 mai 2002[70] :

Alors que le précédent arrêté royal donnait mission au Ministre des Transports de déterminer les conditions légales à l'établissement d'une lettre de voiture CMR, **l'arrêté ministériel du 8**

[69] C'est-à-dire si les véhicules concernés franchissent la frontière belge.

[70] Arrêté ministériel du 8 mai 2002 pris en exécution de l'arrêté royal du 7 mai 2002 relatif au transport de choses par route, *M.B. 30.05.2002*.

mai 2002 est intervenu pour régler tant les conditions de délivrance de la lettre de voiture CMR, que les modèles du CMR (modèle pré-imprimé légal fixé par l'Annexe 8[71] de l'A.M.[72]) et l'utilisation de la lettre de voiture CMR sur le territoire belge, **tout en créant un régime de « cas particuliers »** (cf. transport de déménagement et transport de marchandises de moins de 50 km).

a. Le modèle légal de la lettre de voiture (CMR)

Selon l'AM du 8 mai 2002, la lettre de voiture CMR doit être établie conformément au modèle légal prescrit par son Annexe 8 (voir articles 33 à 37 de l'A.M.), et ceci vaut tant pour le trafic national qu'international, afin de reprendre les points importants du contrat de transport de marchandises tel qu'il a été établi par les parties au contrat.

Selon l'article 34 de l'A.M. *« la lettre de voiture CMR doit être établie au moins en trois exemplaires originaux, conformes au modèle fixé par l'annexe 8 »*.

En ce qui concerne le remplissage des rubriques de ce modèle, **avant que le transport ne commence, tous les exemplaires des lettres de voiture CMR doivent être remplis dans toutes leurs rubriques (à l'exception de celle portant le n° 16 – « signature, date et cachet du destinataire »). Après l'exécution du transport, le troisième exemplaire doit être complété dans toutes ses rubriques.**

Par dérogation, les rubriques numéro 6 (« transporteur sous-traitant »), 7 (« transporteur successif »), 8 (« frais afférents au transport »), 9 (« réserves du transporteur lors de la prise en charge de la marchandise »), 11 (« documents annexes transmis par l'expéditeur ») et 13 (« instructions de l'expéditeur ») ne doivent être remplies que s'il y a lieu de le faire.

Néanmoins, les parties intéressées peuvent porter sur la lettre de voiture CMR « *toute autre indication qu'elles jugent utile* »[73], puisque ces mentions obligatoires sont *a minima*, en ce sens qu'elles doivent toujours faire partie du document CMR (tel que prévu par la Convention internationale CMR), mais que celui-ci pourra comporter d'autres rubriques nécessaires ou utiles au bon déroulement du transport selon le souhait des parties contractantes en cause.

b. Conditions de délivrance du CMR (art. 33 de l'AM):

Selon les dispositions de l'article 33, § 1er, de l'A.M. **la lettre de voiture CMR *« …est délivrée, aux frais du demandeur, par les organismes suivants*:**

1° Fédération Royale Belge des Transporteurs (FEBETRA), rue de l'Entrepôt 5A, 1020 Bruxelles;

2° Koninklijke Beroepsvereniging Goederenvervoerders Vlaams Gewest en Brussels Hoofdstedelijk Gewest (SAV), Land van Rodelaan 20, 9050 Gent;

---

[71] Cf. Annexe 2 de notre Rapport d'Activité n°1 (juillet 2008), précité. Ou modèle sur le site : http://www.code-de-la-route.be/wet.php?wet=51&node=bijl8

[72] Gras et souligné par l'auteur, qui attire l'attention des autres partenaires sur ce point précis. En effet, la création d'une tablette numérique de lecture des CMR papier impose qu'elle soit « dessinée » de façon à pouvoir s'adapter à ce modèle pré-imprimé belge, tout en n'excluant pas que d'autres modèles soient également utilisés par les transporteurs puisque chaque pays européen possède son modèle à soi (tout en intégrant les mentions obligatoires de la Convention CMR), donc le format peut varier considérablement (à tenir en compte techniquement).

[73] Cf. article 35, §2 de l'AM du 8 mai 2002.

3° Union Professionnelle du Transport par Route (U.P.T.R.), rue Denis Lecocq, s.n°, 4031 Liège. (...)»

Ces organismes ont l'obligation légale de délivrer les lettres de voiture CMR, même aux entreprises qui n'en sont pas membres. De plus, l'A.M. du 8 mai 2002 prévoit plusieurs **conditions de forme assez restrictives**, dont notamment :

- qu'un **bordereau soit établi et que celui-ci indique** la date de délivrance, le nom et l'adresse du destinataire, **ainsi que le nombre et le numérotage des CMR** (cf. art.33, §2) ;
- **que ce bordereau soit conservé par l'organisme fournisseur pendant 5 ans[74] (au moins) pour permettre un « *examen aisé par le Ministre ou son délégué* »** (l'organisme fournisseur doit aussi leur transmettre une photocopie si la demande en est faite) (cf. art. 33, §2) ;
- **et, enfin, la lettre de voiture CMR doit comporter un numéro imprimé précédé de la lettre B dans le coin supérieur droit, la numérotation doit être continue et tous les exemplaires d'une même lettre de voiture doivent porter le même numéro** (cf. art. 33, §3).

c. Utilisation du CMR (art. 35) :

L'A.M. du 8 mai 2002 prévoit aussi d'autres **conditions strictes d'utilisation du CMR**, qui reprennent les dispositions de la Convention CMR, ainsi :

- Le premier exemplaire de la lettre de voiture CMR est destiné à l'expéditeur, le deuxième exemplaire est destiné au destinataire, et le troisième exemplaire est destiné au transporteur.
- **Le deuxième et le troisième[75] exemplaires doivent se trouver à bord du véhicule et accompagner la marchandise; ils doivent être présentés à toute réquisition des agents chargés du contrôle**.
- **Le troisième exemplaire doit être conservé par l'entreprise au moins pendant les cinq ans[76] qui suivent la date du transport et classé par ordre chronologique, d'une manière permettant un contrôle aisé par les agents chargés de veiller à l'application de la loi du 3 mai 1999 relative au transport de choses par route et de ses arrêtés d'exécution**. **Cet exemplaire peut être conservé *« sur tout autre support d'information pour autant que la visualisation et l'impression de l'intégralité du document puissent aisément être opérées »* (art. 35, §1, 3ème alinéa de l'AM du 8 mai 2002, modifié par l'AM du 5 février 2007)**.

[74] Donc des dispositions précises devront être prises pour la conservation et l'archivage de ces documents, qu'ils soient sous forme papier et/ou numérique d'ailleurs. Sous ce dernier support l'on suppose que le gouvernement belge indiquera des dispositions précises à ce propos en ce qui concerne l'adoption du CMR électronique.

[75] Ce troisième exemplaire n'a été imposé que par la modification faite par l'A.M. du 5 février 2007 (voir prochain point).

[76] **L'article 60 du Code TVA étend toutefois cette obligation à 7 ans (en vue de contrôles fiscaux). Cette obligation devra donc être prise en compte pour la période de conservation concernant l'archivage (papier ou électronique) de ces exemplaires**.

Avant que le transport ne commence, tous les exemplaires de la lettre de voiture CMR doivent être remplis dans toutes leurs rubriques, à l'exception de celle portant le numéro 16[77]. Toutefois, après l'exécution du transport, le troisième exemplaire devra être complet dans toutes ses rubriques. Par dérogation, les rubriques numéros 6, 7, 8, 9, 11 et 13[78] ne doivent être remplies que *« s'il y a lieu »* et les parties intéressées peuvent porter sur la lettre de voiture CMR *« toute autre indication qu'elles jugent utile »*[79].

d. Le régime des cas particuliers (art. 36 et s.) :

Avec l'A.M. du 8 mai 2002 **deux cas particuliers, dérogeant à la règle générale de la lettre de voiture CMR**, ont été introduits :

1. **la 'lettre de voiture pour déménagement'** : en effet, il existe un modèle spécifique pour ce cas de transport-ci, dont le **modèle spécial est prévu à l'Annexe 9 de l'A.M.**[80]. Même si le modèle légal de lettre de voiture CMR pourra toujours être utilisé de façon alternative.

Là aussi, l'article 36 établit des conditions de forme strictes car:

- La 'lettre de voiture pour déménagement' doit être établie au moins en deux exemplaires originaux conformes au modèle fixé par l'annexe 9 : le premier exemplaire est destiné au client, et le second au déménageur. Les deux exemplaires doivent se trouver à bord du véhicule et accompagner les choses déménagées, et ils doivent être présentés à toute réquisition des agents chargés du contrôle.
- De plus, le second exemplaire doit être conservé par l'entreprise au moins pendant les cinq ans qui suivent la date du transport et classé par ordre chronologique, d'une manière permettant un contrôle aisé par les agents chargés de veiller à l'application de la loi du 3 mai 1999 relative au transport de choses par route et de ses arrêtés d'exécution. Ici encore, cet exemplaire peut être conservé sur *« tout autre support d'information pour autant que la visualisation et l'impression de l'intégralité du document puissent aisément être opérées »*[81].

2. la '**lettre de voiture pour transports à courte distance**' : en effet, par dérogation au cadre général, les entreprises peuvent utiliser 'la lettre de voiture pour transports à courte distance **(50 Km et moins)**' **(modèle prévu à l'Annexe 10 de l'A.M.[82]) pour les transports effectués à l'intérieur des frontières de la Belgique**, pour autant que la distance parcourue n'excède pas 50 Km par envoi (du premier lieu de chargement au dernier lieu de déchargement)[83].

---

[77] Voir ci-dessus le point sur « le modèle légal de CMR ».

[78] *Ibidem*.

[79] Cf. article 35, §3 de l'AM du 8 mai 2002.

[80] Voir l'Annexe 3 du Rapport d'Activité n°1 du CRID (cité ci-dessus) ou sur :

http://www.code-de-la-route.be/wet.php?wet=51&node=bijl9

[81] Article 36 de l'AM du 8 mai 2002.

[82] Voir l'Annexe 4 du Rapport d'Activité n°1 (ibidem) ou sur :

http://www.code-de-la-route.be/wet.php?wet=51&node=bijl10

[83] De plus, ces entreprises pourront également utiliser une lettre de voiture pour chaque envoi ou une liste reprenant plusieurs envois, mentionnant (au moins): la date du transport; le lieu de chargement et de

En outre, les 'lettres de voiture pour déménagement' ainsi que les 'lettres de voiture pour transports à courte distance' doivent également être complétées dans toutes leurs rubriques et les parties intéressées pourront apporter sur ces lettres de voiture toute autre indication qu'elles jugent utile.

4) L'Arrêté Ministériel du 5 février 2007 (en vigueur depuis le 1er mars 2007)[84] :

L'arrêté ministériel du 5 février 2007 **a introduit une nouveauté pour la délivrance de la lettre de voiture puisque, depuis sa mise en vigueur, la lettre de voiture CMR peut également être directement délivrée par un *« imprimeur agréé »* (cf. Art. 1er, modifiant l'art. 33 de l'A.M. du 8 mai 2002), en plus des organismes professionnels cités dans les points précédents**.

Toutefois, ce texte ne donne pas beaucoup d'indications sur ce qu'il entend par ce terme, car il précise seulement que *« Les imprimeurs qui souhaitent être agréés pour l'impression de lettres de voiture CMR doivent adresser une demande en ce sens auprès de l'Administration de la fiscalité des entreprises et des revenus - Services centraux Direction II/1 A, North Galaxy, Avenue Albert II 33, boîte 25, à 1030 Bruxelles. Ils doivent déposer une caution de 2.500 EUR.) »* (cf. art.33, §1er de l'A.M.).

Le SPF Finances[85] nous a précisé seulement qu'une documentation sera transmise aux éventuels demandeurs reprenant les conditions mises à l'octroi de l'agrément, les obligations de l'imprimeur agréé et la présentation matérielle des documents à imprimer.

Cette procédure d'agrément d'*« imprimeur agréé »* a été établie afin de pouvoir accorder l'authenticité nécessaire aux documents qui sont délivrés par l'imprimeur, toutefois il n'y a pas de conditions particulières imposées par le SPF Finances, à part le dépôt de cette caution[86] (qui pourrait être entamée en cas de fraude ou d'insolvabilité).

Une liste des imprimeurs agréés est aussi fournie (et mise à jour) par le SPF Finances[87].

Selon nos contacts établis[88] avec l'administration fédérale pour être reconnu en qualité d'imprimeur agréé il faut que la société qui en fait la demande ait déjà ou obtienne la qualité d'*« imprimeur classique »* (reconnaissance par la Banque Carrefour des Entreprises).

---

déchargement de chaque envoi; le nom et l'adresse du transporteur, de l'expéditeur et du destinataire (voir conditions particulières à l'art. 37, §1, 2° a) et b)).

[84] Arrêté ministériel du 5 février 2007 modifiant l'arrêté ministériel du 8 mai 2002 pris en exécution de l'AR du 7 mai 2002 relatif au transport de choses par route, *M.B. du 15.02.2007.*

[85] Cette information se retrouve sur le site du SPF Mobilité qui renvoie au site du SPF Finances (et qui reprend toute la procédure et les personnes de contact pour l'agrément des imprimeurs). Voir sur : http://fiscus.fgov.be/interfaoiffr/erkendedrukkers/inleiding.htm (rubrique « AFER - imprimeurs agréés »).

[86] Cf. le préambule de l'Arrêté Ministériel.

[87] Voir *« Liste des imprimeurs agréés pour la confection des lettres de voiture des entreprises de Transport (mise à jour le 09.02.2010) »* sur :

http://fiscus.fgov.be/interfaoiffr/ErkendeDrukkers/CMRerkenning2010.pdf

[88] En effet, ces informations ont été obtenues par échange de courriels et par téléphone avec le SPF Finances établis dès 2008 (voir point « remerciements » du Rapport d'Activité n°1).

Pour garantir un certain contrôle là-dessus, le SPF Finances se réserve le droit de procéder à des contrôles *a posteriori* de la « bonne conformité » à cette condition un an après l'obtention de l'agrément. Donc, si une entreprise de transports souhaitait imprimer ses propres bordereaux de CMR, il faudrait que l'une de ses filiales, par exemple, possède cette qualité[89]. Cela vaut également comme règle pour la délivrance des lettres de voiture pour déménagement (cf. art. 2, modifiant l'art. 36, §1[90] de l'A.M. du 8 mai 2002).

En outre, **depuis cet arrêté, toute délivrance de CMR est également portée à la connaissance du responsable du contrôle de la TVA du ressort du contribuable au nom duquel les lettres de voiture CMR sont établies**.

Il existe aussi un troisième cas particulier, qui concerne les lettres de voiture *« non normalisées »* : en effet, par dérogation à la règle générale que constitue la lettre de voiture CMR, les entreprises peuvent utiliser une 'lettre de voiture non normalisée' pour chaque envoi ou une liste non normalisée reprenant plusieurs envois, pour les trois catégories de transports ci-après (effectués à l'intérieur des frontières de la Belgique) :

- les transports consistant dans l'enlèvement ou la remise à domicile de choses, effectués préalablement ou consécutivement à un transport ferroviaire;
- les transports consistant dans le ramassage ou la distribution de choses, pour autant qu'ils comportent plus de quatre lieux de chargement ou plus de quatre lieux de déchargement par jour;
- et pour les transports de choses à la demande d'une entreprise de commerce de gros ou de détail du secteur de la distribution, pour autant que les lieux de chargement et de déchargement appartiennent à cette même entreprise ou à une entreprise de commerce de gros ou de détail y liée, tel que défini à l'article 11 du Code des sociétés, ou dans le cadre d'un accord de coopération économique permanent.

Toutefois, la lettre de voiture ou liste *« non normalisée »* (reprenant plusieurs envois) signifie seulement que le modèle de ces documents est libre mais qu'il doit néanmoins toujours contenir certaines indications obligatoires (reprenant les mentions obligatoires de l'article 6 de la Convention CMR).

[89] Par exemple, il nous a été cité un cas où un opérateur informatique (entreprise tierce), qui avait développé un logiciel pour que l'impression des CMR se fasse à travers ses services et par un transporteur belge, ait essuyé un refus d'agrément par le SPF Finances au motif qu'il *« n'était pas un imprimeur au sens classique du terme »*.

Les raisons invoquées pour justifier ce refus sont les conditions de garantie de l'authenticité du document légal (tel que prévu à l'Annexe 8 de l'A.M. du 8 mai 2002) et son « étanchéité » fiscale.

Pourtant, le gros « paradoxe » qui nous a été signalé est que, à l'heure actuelle, le SPF Finances ne connait pas la qualité des imprimeurs des organisations professionnelles traditionnelles qui sont également autorisées à délivrer des bordereaux CMR. Toutefois cela s'expliquerait par une « présomption de bonne foi » vis-à-vis de celles-ci par l'AM lui-même (voir son préambule), puisque ce sont elles qui, historiquement, ont toujours été chargées de cette délivrance et qu'elles ont toujours respecté les dispositions légales en vigueur dans cette matière.

[90] Et qui dispose : *« La lettre de voiture pour déménagement est délivrée aux entreprises concernées, à leur demande et à leur frais, par la Chambre Belge des Entrepreneurs de Déménagements (C.B.E.D.), rue Picard 69, boîte 4, 1080 Molenbeek-Saint-Jean. »*.

Deuxième partie : Les aspects juridiques liés au respect de la vie privée

Après avoir abordé les problèmes juridiques posées par le respect de la législation CMR pour la réussite du projet eCMR, nous allons passer à l'étude des problématiques liées au respect de la législation « vie privée » et de la protection des données à caractère personnel dans le secteur du transport routier et de la logistique.

En effet, les autres partenaires du projet ont également développé des outils techniques pour arriver à transférer les données fournies par le CMR papier via une tablette électronique au serveur du transporteur et par après, éventuellement, aux clients des transporteurs et/ou à l'entreprise tierce, fournisseur de services à valeur ajoutée (comme, par exemple, une entreprise de services qui gèrerait la fourniture de CMR et leur conservation/archivage ultérieur).

On conserve donc le CMR sous format papier, tout en l'attachant à une tablette électronique, qui envoie les informations contenues dans le CMR par le biais d'un PC embarqué et/ou de toute autre solution de communication électronique, afin de faciliter l'échange rapide des informations collectées et transmises par tous les systèmes embarqués des véhicules (pratiquement on pourrait savoir en temps réel où se trouve le véhicule par le biais du chargement/déchargement de la marchandise concernée par un CMR précis, par exemple). Cela va donc favoriser l'interconnexion de ces données afin qu'elles soient traitées et analysées par le serveur du transporteur, par exemple, à des fins de gestion de sa flotte de véhicules, d'optimisation du service de livraison, etc (voir points détaillés ci-dessous).

Actuellement, selon notre partenaire CETIC, **l'outil privilégié est une solution de communication embarquée de type GSM/GPRS[91] qui permettra la transmission des informations à l'aide du protocole TCP[92] supporté par la liaison GPRS entre le terminal embarqué dans le véhicule et le serveur de gestion de flotte**[93]. Selon les derniers rapports techniques du CETIC[94], les véhicules seront reliés à la plateforme de gestion des données par une liaison TCP/IP sur canal GPRS et le module GSM/GPRS devra permettre la transmission des données des équipements embarqués dans le véhicule à cette plateforme de gestion.

Nous avons donc **identifié plusieurs questions juridiques**, dont le choix de les analyser a été porté sur les deux problèmes suivants principalement :

- Quels sont les types de données qui sont transmises du véhicule au « tiers »? **Quel est l'état actuel de la législation en matière de transfert des données dans le secteur transport routier ?** Et quels sont les types de données à caractère personnel dont on parle ici ? **La loi « vie privée » s'applique-t-elle et à quoi?** ***(I)***
- Le cas échéant, quand on parle de traitements de données à caractère personnel, le **problème majeur que l'on voit ici est le contrôle et la surveillance à caractère**

[91] Le choix du CETIC (avec les autres partenaires - entreprises) s'est porté sur terminal GSM/GPRS/GPS "SteppIII de Falcom » (voir 'Rapport technique pour le premier semestre 2009' du CETIC - juillet 2009).

[92] Pour toutes les explications techniques, voir les rapports des autres partenaires.

[93] *Ibidem*.

[94] Voir 'Rapport technique pour le deuxième semestre 2008' du CETIC (de janvier 2009) et le 'Rapport technique pour le premier semestre 2009' du CETIC (de juillet 2009) principalement.

« permanent » des conducteurs de ces véhicules. Nous allons donc procéder à l'étude du **cas spécifique du respect à la vie privée des travailleurs dans leur relation d'emploi** (quel est le régime juridique qui s'applique alors - par exemple, que dit la loi à propos des méthodes de géolocalisation des travailleurs ?) ***(II)***.

Nous essayerons d'apporter des réponses à ces deux questions principales dans cette deuxième partie du rapport de recherche, afin que nos autres partenaires réalisent pleinement les défis technologiques en accord avec le respect de la législation en vigueur.

Par ailleurs, nous n'excluons pas que des traitements de données à caractère personnel aient lieu également par rapport à d'autres « personnes concernées » (tels que les clients des transporteurs, les donneurs d'ordre, les tiers intermédiaires de service, etc), toutefois les principes envisagés au ***point I*** s'appliqueront à tous ces traitements là d'une manière plus générale, donc nous ne les reformulerons pas en tant que tels.

I/ Le cadre juridique en matière de protection de données à caractère personnel :

Selon les derniers rapports techniques du CETIC (année 2009 essentiellement), **différentes données en provenance du véhicule vont être amenées à être transmises par une interface GPS/GPRS du système embarqué à une plate-forme externe (ou à un serveur) de gestion et de collecte de données**.

Avant que l'on puisse distinguer clairement les traitements de données à caractère personnel concernés par le projet, nous allons voir quel est le cadre juridique existant en la matière (**A**), puis nous distinguerons les différents outils techniques permettant ce(s) traitement(s) dans un souci de clarté (**B**), avant de voir quelles seraient les données à caractère personnel concernées par le projet eCMR (**C**).

A. Le régime légal de la protection des données

Au niveau juridique européen, c'est la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (dite aussi « **Convention 108** »), signée à Strasbourg en janvier 1981[95], qui **a posé les principes-clés en matière de protection des données personnelles des individus (personnes physiques)**, en tant que corolaire du **droit au respect à la vie privée**. Celui-ci ayant été également consacré comme **droit de l'homme et liberté fondamentale par l'article 8**[96] **de la Convention de Sauvegarde des**

[95] Cette convention a été adoptée par le Conseil de l'Europe (qui recoupe 47 Etats membres, dont les Etats membres de l'Union européenne et la quasi-totalité du continent européen). Voir sur : http://www.coe.int/aboutCoe/index.asp?page=quisommesnous&l=fr

[96] Ainsi l'article 8 (« Droit au respect de la vie privée et familiale ») dispose que :

*« 1° Toute personne a **droit au respect de sa vie privée** et familiale, de son domicile et de sa correspondance.*

*2° Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit **que pour autant que cette ingérence est prévue par la loi** et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale**, ou à la protection des droits et libertés d'autrui**. »* (souligné par l'auteur)

Droits de l'Homme et des Libertés fondamentales[97], afin de pallier à la *« nécessité de concilier les valeurs fondamentales du respect de la vie privée et de la libre circulation de l'information entre les peuples »*.

Au niveau de l'Union européenne, il existe également un cadre législatif qui vise à harmoniser les dispositions concernant la protection des données à caractère personnel au sein des Etats membres de l'UE, qui est la Directive 95/46/CE du 24 octobre 1995[98]. A l'heure actuelle, celle-ci a été transposée dans tous les Etats membres par des lois nationales, même si parfois quelques dispositions peuvent différer plus ou moins légèrement selon les Etats[99] (par exemple, en Italie et au Luxembourg leur loi « vie privée » protège aussi les données à caractère personnel des personnes morales, c'est-à-dire des sociétés[100]).

Nous commencerons d'abord par définir le cadre légal européen, puisque les transports par route s'effectuent la plupart du temps entre plusieurs pays au sein de l'Europe (et même au-delà), car il est important pour les autres partenaires de savoir quels sont les principes généraux concernant la protection des données à caractère personnel qui peuvent être communs aux Etats membres de l'Union européenne. Nous terminerons par une mise en exergue des principes et des conditions juridiques posés également par la loi « vie privée » belge (qui recoupent bien souvent ceux de la « législation » européenne avec quelques précisions intéressantes) puisque nos partenaires sont basés dans ce pays.

1) La Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

Au niveau du cadre légal de l'Union Européenne, la Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données a été adoptée le 24 octobre 1995 et est devenue le **texte juridique européen de référence dans le domaine de la protection des données**, favorisant ainsi une harmonisation des cadres légaux entre les Etats de l'UE.

Cette directive vise à protéger les droits et les libertés des personnes par rapport au traitement de données à caractère personnel en définissant quelques « acteurs-clés » dans cette matière et en établissant des principes directeurs déterminant la licéité de ces traitements.

---

[97] Cf. Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales, signée à Rome le 4 novembre 1950, par les Etats membres du Conseil de l'Europe. Déjà le 10 décembre 1948, la Déclaration Universelle des Droits de l'Homme au niveau de l'Organisation des Nations Unies (ONU), qui consacrait le droit à la vie privée dans son article XII, avait été adoptée au niveau international.

[98] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *JO L 281 du 23.11.1995, p. 31–50.*

[99] Pour avoir un aperçu complet des différentes lois adoptées par le Etats membres, ainsi que des différences majeures de transposition, voir sur : http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm et http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_fr.htm.

[100] Cela pourra avoir une incidence dans le cadre de notre projet si, par exemple, des flux de données à caractère personnel ont lieu en provenance de/vers ces pays (application de leur loi nationale si le responsable du traitement concerné est situé sur ces territoires – voir points suivants).

Nous verrons ci-après quels sont-ils, en tenant bien présent que ces notions générales se retrouvent dans les lois de transposition des Etats membres, dont la Belgique.

a. Le champ d'application de la Directive 95/46/CE

L'article 2 de la Directive 95/46/CE définit quelques **mots-clés en matière de protection des données afin d'établir le champ d'application de la directive**, il est donc essentiel que l'on soit en présence :

- d'une « ***donnée à caractère personnel*** », qui est définie comme « ***toute information concernant une personne physique*** *identifiée ou identifiable*[101] *(personne concernée)…* » (art.2, a. de la directive) ;
- et/ou d'un « ***traitement de donnée à caractère personnel*** », qui est défini comme « ***toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel*** *, telles que la* ***collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction*** » (art.2, b. de la directive)[102].

En effet, presque tous les traitements de données vont être concernés par la législation « vie privée » lorsqu'ils permettront l'identification aisée ou par des « moyens raisonnable » d'une personne donnée (ainsi une donnée relative au moteur du véhicule, pour vérifier son niveau d'huile, par exemple, ne va pas être considérée comme « à caractère personnel » puisque elle ne donne aucune indication relative à un individu, et donc ne relève pas du champ d'application de la directive, sauf si on va l'associer avec la façon de conduire de tel ou tel conducteur à des fins de contrôle).

De plus, l'article 3, §1 de la directive précise qu'elle « ***s'applique au traitement de données à caractère personnel, automatisé*** *en tout ou en partie,* ***ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier*** »[103].

L'article 4 de la directive règle les questions de droit national applicable et dispose ainsi que :

> « *1. Chaque État membre applique les* ***dispositions nationales*** *qu'il arrête en vertu de la présente directive aux traitements de données à caractère personnel* ***lorsque****:*
>
> *a)* ***le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'État membre****; si un même responsable du traitement est établi sur le territoire de plusieurs États membres, il doit prendre les mesures*

[101] Gras et souligné par l'auteur.
[102] Souligné par l'auteur (idem pour les textes cités qui suivent).
[103] Sont ainsi **exclus les traitements de données « *effectués par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques* »** (art. 3, §2, al.2 de la directive) et ceux « *mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire* (…) *et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal* » (art.3, §2, al.1 de la directive).

nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable[104]*;*

b) le responsable du traitement n'est pas établi sur le territoire de l'État membre mais en un lieu où sa loi nationale s'applique en vertu du droit international public;

c) le responsable du traitement n'est pas établi sur le territoire de la Communauté ***et recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire dudit État membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit*** *sur le territoire de la Communauté.*

2. Dans le cas visé au paragraphe 1 point c), ***le responsable du traitement doit désigner un représentant établi sur le territoire dudit Etat membre****, sans préjudice d'actions qui pourraient être introduites contre le responsable du traitement lui-même.* » (gras et souligné par l'auteur).

Donc, selon que l'on se trouve sur le territoire de tel ou tel autre Etat membre, il faudra tenir compte de ces dispositions pour établir où se trouve le responsable du traitement (voir ci-dessous) et déterminer ainsi quelle loi nationale va trouver à s'appliquer au traitement de données concerné.

Si l'on se trouve dans le cadre de flux transfrontières avec des pays tiers/hors Union Européenne ce sont les règles de droit international privé qui s'appliqueront. **La Commission européenne a par ailleurs établit une sorte de « liste blanche » des Etats tiers dont les règles en matière de protection des données à caractère personnel offrent des « garanties similaires » aux règles européennes et un « niveau de protection » considéré comme « adéquat »**[105].

b. Les acteurs-clé en matière de protection des données

Lorsque des données à caractère personnel, c'est-à-dire des données permettant d'identifier facilement ou « avec des moyens raisonnables » des personnes physiques[106], **font l'objet d'un traitement la législation européenne impose plusieurs conditions pour que ces traitements soient licites, définit plusieurs « acteurs-clé » et leur attribue respectivement certains droits et obligations.**

Ainsi, **au préalable de tout traitement** de données à caractère personnel, **il faut désigner un** « **responsable de traitement** », défini comme étant : « ***la personne physique ou morale****, l'autorité publique, le service ou tout autre organisme* ***qui, seul ou conjointement avec***

[104] Souligné par l'auteur : il se peut que les transporteurs de marchandises possèdent plusieurs établissements sur le territoire de l'UE et qu'ils doivent ainsi contrôler la législation nationale spécifique de chaque Etat en matière de « vie privée ».

[105] Voir sur son site 'Décision de la Commission relative à la constatation du caractère adéquat de la protection des données dans les pays tiers' : http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_fr.htm

[106] Voir sur ce point l'*Avis 4/2007 sur le concept de données à caractère personnel* (WP 136) du Groupe de Travail européen « Article 29 » sur la protection des données du 20 juin 2007, qui précise que : *« on peut considérer une personne physique comme «identifiée» lorsque, au sein d'un groupe de personnes, elle se «distingue» de tous les autres membres de ce groupe. La personne physique est donc «identifiable» lorsque, même sans avoir encore été identifiée, il est possible de le faire (…) c'est le* ***contexte du cas d'espèce*** *qui déterminera si certains identifiants sont suffisants pour permettre l'identification (…) »* (cf. pp. 13 à 24).

d'autres, détermine les finalités et les moyens du traitement[107] ***de données à caractère personnel(…)*** » (souligné par l'auteur).

En effet, c'est cet acteur-ci qui va être responsable de la mise en place des conditions et des obligations prévues par la loi pour que les traitements de données à caractère personnel soient licites et lors de tout contrôle éventuel postérieur.

La désignation d'un responsable de traitement est donc un préalable obligatoire inconditionnel en matière de protection de la vie privée. Il peut également en exister plusieurs qui vont être considérés comme « coresponsables » du traitement concerné, du moment que plusieurs personnes (physiques et/ou morales) décident conjointement ces finalités et moyens de ces traitements de données personnelles (la 'finalité' étant comprise comme le but pour lequel un traitement a lieu, et les 'moyens' comme l'ensemble des mesures techniques, organisationnelles ou autres, qui vont être mises en place pour assurer ce traitement)[108].

Ensuite, il faut déterminer qui est (ou sont) la(les) « **personne(s) concernée(s)** » par ces traitements, dont la définition découle de celle de « donnée à caractère personnel » et qui est définie comme : **toute « *personne physique identifiée ou identifiable* »**[109] au moyen d'un traitement de données. **Cette personne va jouir de droits, qui vont être protégés par les dispositions de cette directive**, comme : le **droit à l'information**[110] ; le **droit d'accès, de rectification, l'effacement ou le verrouillage des données**[111] qui la concernent ; et/ou le **droit d'opposition**[112] à ce qu'un traitement de ses données personnelles soit fait.

D'autres acteurs peuvent également intervenir dans le cadre d'un traitement de données à caractère personnel, il est donc important d'en souligner déjà quelques-uns, dont :

---

[107] En gras et souligné par l'auteur pour insister sur l'importance de ces notions.

[108] Voir également sur ce point *l'Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant »* (WP 169) du Groupe de Travail européen « Article 29 » sur la protection des données du 16 février 2010, qui précise que : *« (…) même si la capacité de «déterminer» peut procéder d'une attribution faite expressément par la loi, elle se déduira généralement d'une* ***analyse des éléments factuels ou des circonstances de l'espèce:*** *il conviendra d'examiner les opérations de traitement en question et de comprendre qui les détermine, en répondant dans un premier temps aux questions «pourquoi ce traitement a-t-il lieu? » et «qui l'a entrepris?». (…)* ***la détermination des finalités et des moyens revient à établir respectivement le «pourquoi» et le «comment» de certaines activités de traitement****. Dans cette optique, et puisque ces deux éléments sont indissociables, il est nécessaire de donner des indications sur le degré d'influence qu'une entité doit avoir sur le «pourquoi» et le «comment» pour être qualifiée de responsable du traitement. (…)* » (pp. 10 à 35) (souligné par l'auteur).

[109] Cf. article 2, a. de la Directive 95/46/CE et qui précise que : « *est réputée identifiable une personne qui peut être identifiée, directement ou indirectement,* ***notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité*** *physique, physiologique, psychique, économique, culturelle ou sociale* » (souligné par l'auteur).

[110] En effet, l'articles 10 de la Directive 95/45/CE dispose que : « *Les États membres prévoient que le responsable du traitement ou son représentant doit fournir à la personne auprès de laquelle il collecte des données la concernant au moins les informations énumérées ci-dessous, sauf si la personne en est déjà informée(…)* » et l'article 11 prévoit certaines dispositions lorsque ces données n'ont pas été collectées directement auprès de la personne concernée.

[111] Cf. article 12 de la Directive 95/46/CE : ce droit va pouvoir s'exercer sans « *délais ou frais excessifs* » qu'il existe ou non un traitement de données concernant la personne, quelles que soient les données traitées (et finalités du traitement).

[112] Cf. art. 14 de la Directive 95/46/CE.

- le « **sous-traitant** », qui est défini par la directive comme : « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme **qui traite des données à caractère personnel pour le compte du responsable du traitement*** »[113] (art.2, e. de la directive) (ex. : on va souvent faire appel à des « sous-traitants techniques » pour gérer les traitements de données, leur collecte, leur encodage, leur archivage, etc)[114];
- le « **tiers** », qui est défini comme : « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes **qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données*** » (art. 2, f. de la directive) (il s'agit des employés des services comptables ou du service du personnel d'une entreprise, qui gèrent les dossiers personnels des employés, par exemple) (souligné par l'auteur) ;
- et le « **destinataire** », qui est : « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme **qui reçoit communication de données**, qu'il s'agisse ou non d'un tiers (…)* »[115] (art. 2, g. de la directive) (dans le cadre de ce projet, ce sera souvent le client – destinataire des marchandises transportées, qui va recevoir l'information d'où se trouve sa marchandise par le transporteur ou l'entreprise tierce de services, par exemple).

Il est **important de distinguer ces différents acteurs dès le début de chaque traitement de données à caractère personnel puisque tous ne vont pas être responsables de la même façon vis-à-vis de la personne concernée en cas de non-respect des dispositions de la législation « vie privée »**.

c. Les principes à respecter en cas d'existence de traitement de données à caractère personnel

La directive impose également le respect de quelques **principes très importants relatifs tant à la qualité des données qu'à la légitimité des traitements de données** (et qui vont se retrouver dans les lois nationales de transposition des Etats membres), et qui sont :

- ***Le principe de légalité et de finalité du traitement de données***

En effet, **toute collecte de données à caractère personnel doit d'être « *loyale et licite* »** (art. 6, §1, a.), ceci implique que **les données à caractère personnel doivent être collectées pour des « *finalités déterminées, explicites et légitimes* »** de façon loyale (la collecte de la donnée doit être faite de la façon la plus transparente possible, ce qui dépend beaucoup de l'information fournie à ce moment-là ; et être effectuée seulement pour les raisons acceptées par le droit national applicable[116]), et ne « *pas être traitées ultérieurement et de manière incompatible avec ces finalités* » (art. 6, §1, b. de la directive).

[113] Gras et souligné par l'auteur (idem pour les textes cités qui suivent).

[114] Cf. WP 169 du Groupe « Article 29 » cité ci-dessus.

[115] Souligné par l'auteur.

[116] Cf. article 5 de la Directive qui dispose que : *« Les États membres précisent, dans les limites des dispositions du présent chapitre, les conditions dans lesquelles les traitements de données à caractère personnel sont licites. »*

Par exemple, si une entreprise collecte des données à caractère personnel par le biais du CMR (par exemple, la donnée est le nom du conducteur du véhicule sur une partie du trajet global de la marchandise) et qu'elle déclare un premier traitement comme ayant la finalité de la « gestion et le suivi des marchandises », elle ne pourra pas « détourner » ce premier traitement pour d'autres finalités incompatibles, du type « contrôle du travailleur », sans effectuer une nouvelle déclaration pour cet autre traitement. Donc, en cas de nouvelle finalité (qui ne soit pas liée au premier traitement) on considèrera qu'il y a un nouveau traitement de données à caractère personnel (et on devra mettre en œuvre toutes les dispositions de la directive une nouvelle fois et distinctement du premier traitement déclaré).

En outre, selon les dispositions de l'article 8 de la Directive 95/46/CE, **certaines catégories particulières de traitements ne sont pas possibles, sauf si un certain nombre de conditions sont réunies,** ainsi les traitements concernant les données dites « sensibles », c'est-à-dire celles révélant « *l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle* »[117].

En principe, les traitements de ces données sont interdits, sauf si :

- la personne concernée a donné « *son consentement explicite* »,
- ou que c'est « *nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par une législation nationale prévoyant des garanties adéquates* »,
- ou que les autres conditions strictement prévues par la directive sont respectées[118].

- ***Le principe de légitimité du traitement de données***

Le fait qu'un traitement de données soit licite (c.à.d. qu'il réunisse les conditions de licéité prévu ci-dessus) ne veut pas automatiquement dire que ce traitement soit légitime. En effet, le principe de légitimité **implique plusieurs conditions** :

- que la **personne concernée ait donné son consentement de manière indubitable**[119] (et le « **consentement** » est défini par la directive comme : « *toute manifestation de volonté, **libre, spécifique et informée** par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement* »[120]) ;

Et que ce traitement ait lieu :

- soit parce qu'il est **nécessaire à l'exécution d'un contrat ou de mesures précontractuelles,**

[117] Cf. art. 8, §1 de la Directive 95/46/CE.

[118] Cf. article 8, §2, §3, §4, §5 et §6 de la Directive 95/46/CE.

[119] Cf. article 7, a. de la Directive 95/46/CE.

[120] Définition à l'art. 2, h. de la Directive 95/46/CE (souligné par l'auteur).

- **soit parce qu'il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis**[121],
- soit qu'il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée, etc.

Donc un traitement de données à caractère personnel ne sera licite et légitime que s'il remplit au moins l'une de ces conditions (alternatives) de légitimité énumérées limitativement par l'article 7 de la directive, **sous réserve qu'il y ait également une mise en balance des différents intérêts en cause et le respect du principe de proportionnalité par rapport aux finalités poursuivies** (voir ci-après).

- ***Les principes de proportionnalité et de nécessité***

Ces deux **principes** sont **essentiels** en matière de droit à la protection des données personnelles et de la vie privée[122] : en effet, d'une part, **les données traitées** doivent être « ***adéquates, pertinentes et non excessives*** *au regard des finalités pour lesquelles elles sont collectées* » (art. 6, §1, c. de la directive), ce qui implique le **respect des principes relatifs à la qualité des données prévus à l'article 6 de la directive**, tels qu'on les a énumérés ci-dessous (collecte loyale, etc). Et, d'autre part, ces données doivent être « ***exactes et, si nécessaire, mises à jour*** » (art. 6, §1, d. de la directive) **et ne peuvent être « *conservées* [que] *pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités* »** (art. 6, §1, e.). Concernant la durée de conservation, il se peut donc que plusieurs durées de conservation soient tolérées selon les différentes finalités poursuivies, le tout étant que cette durée ne soit pas « excessive » par rapport au but du traitement envisagé et de s'en tenir à la durée minimum nécessaire pour cette conservation[123].

Il appartient au responsable du traitement d'assurer le respect de ces principes (art. 6, §2 de la directive), le mieux est donc qu'il précise la durée de conservation dès le début du traitement envisagé, et qu'il définisse bien au préalable la finalité des traitements envisagés afin de déterminer quelles sont les informations qui devront vraiment être collectées, par exemple, pour atteindre le but recherché, afin de respecter également le principe de nécessité.

- ***La sécurité et la confidentialité des traitements***

La directive 95/46/CE met également en place un **devoir de confidentialité et de sécurité des traitements à l'égard du responsable du traitement**, qui **doit mettre en œuvre des *« mesures techniques et organisationnelles appropriées***[124] *pour protéger les données à*

---

[121] Par exemple, dans le projet eCMR un traitement de données à caractère personnel pour contrôler le respect de la législation sur le respect des temps de travail et de repos va être admis, via les traitements à effectuer sur le tachygraphe, par exemple, par contre l'utilisation ultérieure de ce traitement pour une finalité incompatible et non prévue par cette législation va être considérée comme non légitime (et illicite) (voir points suivants).

[122] Bien souvent les juges vont y faire référence pour déterminer la licéité d'un traitement en cas de contestation par la personne concernée, par exemple.

[123] Tel est le « discours » adopté par le Contrôleur Européen pour la protection des données (CEPD/EDPS) et certains membres des Commissions nationales pour la protection des données (CNIL française et CPVP belge notamment) concernant la durée de conservation (cf. conférences et workshop divers organisés pendant 2009 et 2010 sur la protection des données – par ex. : *3rd International Conference in Data Protection*, 29-30 janvier 2010 à Bruxelles : http://www.cpdpconferences.org/index.html).

[124] Et « *ces mesures doivent assurer, **compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre**, un **niveau de sécurité approprié au regard des risques présentés** par le traitement **et de la nature des données** à protéger* » (cf. article 17, §1, al.2 de la Directive 95/46/CE).

caractère personnel ***contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau****, ainsi que contre toute autre forme de traitement illicite »* (il doit également s'assurer que tous ses éventuels sous-traitants respectent bien cela et qu'ils agissent seulement sous son autorité et sur son instruction[125]).

Ainsi, l'on soulignera qu'en vertu de ces principes, le responsable du traitement aura tout intérêt à respecter également les dispositions du paragraphe 3 de l'article 17 de la directive concernant la sécurité des traitements : **il est de son intérêt à établir un contrat écrit qui liera son (ou ses) sous-traitant(s) lorsqu'il réalisera un traitement de données à caractère personnel en sous-traitance, afin que celui-ci soit également lié par ces obligations de sécurité et de confidentialité (et qu'il ne puisse agir que sur ses instructions), et que sa responsabilité vis-à-vis du responsable du traitement soit établie.**

En plus du respect des dispositions de la législation protection des données, il sera assuré par le respect du droit contractuel.

- ***Le principe de transparence***

En vertu de ce principe, le responsable du traitement a non seulement un **devoir d'information avant tout traitement à l'égard de la personne concernée** (article 10 de la directive), mais il a également une **obligation de notification des traitements** qu'il compte effectuer **à l'autorité de contrôle indépendante du pays où le traitement a lieu**[126].

Ainsi, selon les dispositions de l'art. 10, le responsable du traitement doit informer la personne concernée de :

« a) l'identité du responsable du traitement et, le cas échéant, de son représentant;

b) les finalités du traitement auquel les données sont destinées;

c) toute information supplémentaire telle que:

- les destinataires ou les catégories de destinataires des données,

[125] En vertu des articles 16 et 17 de la Directive 95/46/CE.

[126] Cf. article 18 de la Directive 95/46/CE. Chaque Etat a donc instauré une autorité de contrôle indépendante de contrôle de la législation protection des données. Ces autorités sont prévues à l'article 28 de la Directive 95/46/CE.

L'article 19 de la directive donne quant à lui les informations concernant le « contenu de la notification », qui doivent être au minimum:

« a) ***le nom et l'adresse du responsable du traitement*** *et, le cas échéant, de son représentant;*

b) ***la ou les finalités du traitement****;*

c) une ***description de la ou des catégories de personnes concernées*** *et des données ou des catégories de données s'y rapportant;*

d) les ***destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées****;*

e) les transferts de données envisagés à destination de pays tiers;

f) une ***description générale permettant d'apprécier de façon préliminaire le caractère approprié des mesures prises pour assurer la sécurité du traitement en application de l'article 17****. »* (souligné par l'auteur)

- le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences éventuelles d'un défaut de réponse,

- l'existence d'un droit d'accès aux données la concernant et de rectification de ces données,

dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont ***nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données****. »*

Si les informations n'ont pas été récoltées auprès de la personne concernée, l'article 11 dispose que : *« …les États membres prévoient que le responsable du traitement ou son représentant doit, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard lors de la première communication de données, fournir à la personne concernée au moins les informations énumérées ci-dessous [art.10], sauf si la personne en est déjà informée »*.

Nous nous permettons d'insister sur le fait que ces deux types d'« informations » **doivent être faites avant le début de tout traitement de données à caractère personnel, car c'est la condition nécessaire pour que la personne concernée puisse exercer ses droits en toute connaissance de cause, et parce qu'un contrôle préalable par l'autorité de contrôle peut être nécessaire pour certains types de *« traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées »*** (article 20 de la directive). Cette autorité doit également pouvoir assurer la **publicité des traitements déclarés** (article 21 de la directive) **au moyen d'un registre accessible au public** (article 21 de la directive).

Comme nous l'avons déjà mentionné, **la Directive 95/46/CE régit également le transfert de données vers des pays tiers** aux articles 25 et suivants[127], **ainsi que les actions et recours juridictionnels que les Etats membres doivent offrir aux personnes concernées en cas de violation des dispositions de la directive**[128], pour que le respect et l'application de la législation « vie privée » soit effective.

2) La Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques

En ce qui concerne le projet eCMR, et comme nous allons le voir dans les points suivants, les données à caractère personnel qui vont être concernées ici vont être transmises/communiquées essentiellement par le kit de transmission GPRS via le Stepp III, outil de communication choisi par le partenariat, ce qui implique que l'**on va également avoir des communications électroniques et que l'on rentre ainsi aussi dans le champ d'application de la Directive**

[127] La Commission européenne **a également prévu des clauses contractuelles types (à insérer dans les contrats de sous-traitance, par exemple) pour ces transferts de données**. Voir à ce propos : http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_fr.htm.

[128] Cf. articles 22 à 24 de la Directive 95/46/CE.

européenne 2002/58/CE[129], qui traite plus particulièrement des traitement des données à caractère personnel dans le secteur des communications électroniques.

a. Le champ d'application de la Directive 2002/58/CE

En effet, au regard de l'article 2, d. de la directive 2002/58/CE, on entend par « **communication** » « ***toute information échangée ou acheminée*** *entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public (…)* ».

De même, comme nous l'avons vu plus haut, le Protocole Additionnel du 21 février 2008 à la Convention relative au Contrat de Transport International de Marchandises Par Route (CMR) concernant la Lettre de Voiture Electronique, définit également à son article 1 la '***lettre de voiture électronique***' comme : *« une* ***lettre de voiture émise au moyen d'une communication électronique par le transporteur, l'expéditeur ou toute autre partie intéressée*** *à l'exécution d'un contrat de transport auquel la Convention s'applique,* ***y compris les indications logiquement associées à la communication électronique sous forme de données jointes ou autrement liées à cette communication électronique au moment de son établissement ou ultérieurement de manière à en faire partie intégrante*** », ainsi qu'une '***communication électronique***' comme « ***l'information enregistrée, envoyée, reçue ou conservée par des moyens électroniques, optiques, numériques ou des moyens équivalents*** *faisant que l'information communiquée soit accessible pour être consultée ultérieurement* ».

Même si, dans le cadre de notre projet, la communication électronique ne sera pas « accessible au public » dans son sens classique[130] (en ce sens que la communication de transfert de données sera transmise du système embarqué du véhicule au serveur distant, mais cela via le réseau public de télécommunications), il importe que l'on mentionne également cette directive, car elle **apporte des définitions de fond complémentaires à la Directive 95/46/CE**[131]**, notamment en ce qui concerne la définition de plusieurs autres « acteurs-clé » qui pourraient être identifiés dans le cadre de notre projet**, comme nous le verrons ci-après.

De plus, les dispositions de cette directive *« précisent et complètent la directive 95/46/CE (…) [et] prévoient la protection des intérêts légitimes des abonnés qui sont des personnes morales »* (cf. art. 1, §2 de la directive), donc elle va au-delà de la protection offerte par la Directive 95/46/CE, qui ne protège que les intérêts des personnes physiques/individus (même si certaines lois nationales de transposition sont allées au-delà, Italie et Luxembourg, notamment).

b. Les acteurs-clé de la Directive 2002/58/CE

[129] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), *JO L 201 du 31.7.2002, p. 37–47.*

[130] En effet, selon l'article 3 de la Directive 2002/58/CE, sont concernés seulement les *« …traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques* ***accessibles au public sur les réseaux publics de communications*** *dans la Communauté (…) »* (souligné par l'auteur).

[131] Qui encadre toutes les autres situations de traitement de données à caractère personnel (en dehors du secteur des communications électroniques).

Un nouvel acteur-clé apparait ainsi dans les dispositions de la Directive 2002/58/CE pour compléter le cadre juridique en matière de vie privée au niveau européen concernant le projet qui nous concerne : l' **' utilisateur'**, qui est défini comme *« **toute personne physique utilisant un service de communications électroniques accessible au public à des fins privées ou professionnelles** sans être nécessairement abonnée à ce service »*[132].

En effet, dans le projet eCMR, il y aura plusieurs « utilisateurs » au sens de cette Directive, comme par exemple : le chauffeur du véhicule, le tiers prestataire de service qui gère le serveur et/ou le transporteur lui-même, le tiers destinataire des données (client des marchandises, transporteur, etc) ; donc il sera **utile de préciser la qualité des uns et des autres avant que tout traitement de données à caractère personnel ait lieu**.

c. Quelques définitions importantes à retenir

La Directive 2002/58/CE **vient également compléter le cadre juridique lorsque des communications électroniques sont utilisées**, ainsi elle va définir :

- ce qu'est une communication[133] (voir ci-dessus) et ce qu'est un « *courrier électronique* »[134], car dans ce projet il pourrait y avoir tant des communications de données brutes provenant des dispositifs embarqués sur le véhicule via le Stepp III vers le serveur distant (qui traitera ces données), que des courriers électroniques si, éventuellement, les entreprises décidaient que les chauffeurs envoient certaines données via courrier électronique (dans le scénario du PC embarqué, par exemple - voir point suivant), ou bien dans le cas où le « gérant » des données du serveur (cela pourrait être soit le transporteur, soit l'entreprise de services) envoie ces mêmes données à ses clients via courrier électronique.
- Cette directive définit également ce qu'on entend par « *appel* »[135], car les chauffeurs des véhicules auront éventuellement à communiquer des données (du lieu où ils se trouvent, de la livraison des marchandises, etc) également via leur téléphone mobile/GSM, pour compléter les informations déjà envoyées via le Stepp III ou bien pour en communiquer d'autres (comme leur lieu de localisation en cas de problèmes de trafic imprévus, par exemple).

La Directive 2002/58/CE donne la définition d'autres **mots-clés** qui vont être **essentiels pour déterminer si des données à caractère personnel vont être concernées dans le projet eCMR**, dont :

- les « **données de localisation** » comme étant : *« **toutes les données** traitées dans un réseau de communications électroniques **indiquant la position géographique de***

[132] Cf. Article 2, a. de la Directive 2002/58/CE – souligné par l'auteur.

[133] Et le Considérant (15) de la Directive 2002/58/CE précise que : « *Une communication peut inclure toute information consistant en une dénomination, un nombre ou une adresse, fournie par celui qui émet la communication ou celui qui utilise une connexion pour effectuer la communication.* ».

[134] Qui est *« **tout message sous forme de texte, de voix, de son ou d'image** envoyé par un réseau public de communications qui peut être stocké dans le réseau ou dans l'équipement terminal du destinataire jusqu'à ce que ce dernier le récupère »* (article 2, h. de la Directive 2002/58/CE).

[135] Cf. art. 2, e. de la Directive 2002/58/CE qui dispose que c'est « *une **connexion établie au moyen d'un service téléphonique** accessible au public **permettant une communication bidirectionnelle en temps réel*** ».

l'équipement terminal d'un utilisateur *d'un service de communications électroniques accessible au public »*[136].

Ici sont concernées surtout des **données de localisation du véhicule (et donc du travailleur, conducteur du véhicule) émises par le GPS du véhicule**, **combinées (éventuellement) avec des données de localisation obtenues par les autres dispositifs embarqués, comme la tablette du CMR** (qui est remplie suivant l'endroit où les marchandises se trouvent, donc elle donne des informations d'heure et de localisation de chargement et de déchargement de la marchandise), entre autres.

- les « **données relatives au trafic** » comme étant : *« toutes les données **traitées en vue de l'acheminement d'une communication** par un réseau de communications électroniques **ou de sa facturation** »*[137].

Il s'agit ici des données transmises au serveur distant via le Stepp III pour gérer notamment les « déficiences » techniques du système, les alertes éventuelles, etc[138].

L'article 9 de cette directive prévoit également que les données de localisation, autres que celles relatives au trafic, ne doivent être traitées « ***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*** »[139] et que ce traitement 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*** » (art. 9, §3)[140].

Ces dispositions rejoignent et complètent celles de la directive 95/46/CE concernant la durée de conservation des données à caractère personnel et les personnes responsables et habilitées à les manipuler, et va même au-delà en **introduisant la notion d'« anonymisation » des données lorsqu'il s'agit d'un traitement de données de localisation**.

---

[136] Cf. Article 2, c. de la Directive 2002/58/CE. Le Considérant (14) de cette directive complète également cette disposition en précisant que « *Par "données de localisation", on peut entendre la latitude, la longitude et l'altitude du **lieu où se trouve l'équipement terminal de l'utilisateur**, la direction du mouvement, le degré de précision quant aux informations sur la localisation, l'identification de la cellule du réseau où se situe, à un moment donné, l'équipement terminal, ou encore le moment auquel l'information sur la localisation a été enregistrée.* » Cette définition très large englobe donc tous les dispositifs embarqués dans le véhicule dans le cadre de ce projet (voir point III).

[137] Cf. Article 2, b. de la Directive 2002/58/CE, et son Considérant (15) qui dispose que « *Les données relatives au trafic peuvent inclure toute traduction de telles informations effectuée par le réseau par lequel la communication est transmise en vue d'effectuer la transmission. **Les données relatives au trafic peuvent, entre autres, comporter des données concernant le routage, la durée, le moment ou le volume d'une communication, le protocole de référence, l'emplacement des équipements terminaux de l'expéditeur ou du destinataire, le réseau de départ ou d'arrivée de la communication, ou encore le début, la fin ou la durée d'une connexion**. Elles peuvent également représenter le format dans lequel la communication a été acheminée par le réseau.* ».

[138] Voir sur ce point les derniers rapports techniques du CETIC (cités ci-dessus).

[139] En outre « *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.*** » (cf. art. 9, §1 de la Directive 2002/58/CE) – souligné par l'auteur.

[140] Souligné par l'auteur.

- Cette directive définit également la notion de « **service à valeur ajoutée** », qui comprend : *« **tout service qui exige le traitement de données relatives au trafic ou à la localisation**, à l'exclusion des données qui ne sont pas indispensables pour la transmission d'une communication ou sa facturation »*[141].

Il pourrait s'agir ici, par exemple, du travail qui serait accompli plus particulièrement par le tiers prestataires de services, ou par le transporteur lui-même, qui souhaiterait traiter les données collectées dans le but d'une meilleure gestion et/ou de contrôle des livraisons des marchandises, de l'envoi et l'émission de factures à l'égard des clients, etc.

d. Les principes à respecter en matière de communications électroniques

La Directive 2002/58/CE vient aussi **réaffirmer les principes de sécurité et de confidentialité des communications électroniques** que le « fournisseur de service de communications électroniques accessible au public » doit respecter : en effet, celui-ci doit *« **prendre les mesures d'ordre technique et organisationnel appropriées** afin de garantir la sécurité de ses services, **le cas échéant conjointement avec le fournisseur du réseau public de communications en ce qui concerne la sécurité du réseau** (…) »*[142].

Ainsi, on peut remarquer que de cette façon l'on se retrouve avec deux acteurs différents, qui pourraient être considérés comme « coresponsables » du niveau de sécurité et de confidentialité des communications en cas de problèmes:

- d'un côté, le responsable du traitement (au sens de la Directive 95/46/CE) doit respecter les principes-clé concernant les traitements de données à caractère personnel qu'il met en place et les mesures de sécurité et de confidentialité (voir point plus haut),
- et, de l'autre côté, dans les cas de communications électroniques, les fournisseurs d'internet et/ou de réseaux de téléphonie mobile sont aussi concernés par ces obligations de sécurité et de confidentialité selon les dispositions de la Directive 2002/58/CE.

Toutefois, il faut remarquer que la « non-action » de l'un ne dédouanerait pas l'autre de ses responsabilités lorsque des données à caractère personnel seraient en jeu[143].

---

[141] Cf. Article 2, g. de la Directive 2002/58/CE, et le Considérant (18) précise que : « *Les services à valeur ajoutée peuvent, par exemple, comprendre des **conseils** sur les forfaits tarifaires les plus avantageux ou **sur le guidage routier,** des informations sur l'état de la circulation, des prévisions météorologiques ou des informations touristiques.* ».

[142] Cf. articles 4 et 5 de la Directive 2002/58/CE, et surtout l'article 4, §2 qui précise que : « *Lorsqu'il existe un risque particulier de violation de la sécurité du réseau, le fournisseur d'un service de communications électroniques accessible au public **informe les abonnés** de ce risque et, si les mesures que peut prendre le fournisseur du service ne permettent pas de l'écarter, **de tout moyen éventuel d'y remédier**, y compris en en indiquant le coût probable.* ». Le Considérant (20) de la directive donne également d'autres précisions concernant cette obligation et dispose en outre que « *l'obligation qui est faite à un fournisseur de service d'informer les abonnés de certains risques en matière de sécurité **ne le dispense pas de prendre immédiatement les mesures appropriées pour remédier à tout nouveau risque imprévisible en matière de sécurité et rétablir le niveau normal de sécurité du service**, les frais en étant à sa seule charge. (…) **La sécurité s'apprécie au regard de l'article 17 de la directive 95/46/CE.*** » - souligné par l'auteur. Toutefois, dans la pratique, il est rare de voir que ces dispositions soient réellement respectées par ces acteurs.

[143] *Ibidem.* En tout dernier lieu, il appartiendrait aux tribunaux de trancher cette question.

Enfin, la Directive 2002/58/CE **prévoit également que la confidentialité des communications** via le réseau public de communications et de services de communications électroniques accessibles au public **soit garantie par l'Etat membre, ainsi que la confidentialité des données de trafic y afférentes**, ce qui se traduit par une **interdiction formelle d'écoute, d'interception ou de stockage des données de trafic et des communications** ***« sans le consentement des utilisateurs concernés*** *sauf lorsque cette personne y est légalement autorisée (…)* »[144]. Toutefois cette disposition n'empêche pas le stockage technique (au niveau du PC embarqué, du Stepp III ou du serveur) nécessaire à l'acheminement d'une communication, tel qu'il est prévu par le partenaire CETIC[145], ni l'enregistrement des données de trafic par le prestataire de services et/ou le transporteur gestionnaire du serveur *« afin de fournir la preuve d'une transaction commerciale ou de toute autre communication commerciale* »[146], sous réserve que ces données ne soient pas communiquées à des tiers « non habilités ».

Enfin, **concernant les données relatives au trafic, l'article 6 de la Directive 2002/58/CE prévoit qu'elles soient « *effacées ou rendues anonymes*** *lorsqu'elles ne sont plus nécessaires à la transmission d'une communication* » (art.6, §1), sauf si elles « *sont nécessaires pour établir les factures des abonnés et les paiements pour interconnexion peuvent être traitées* » mais alors « ***un tel traitement n'est autorisé que jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement*** »[147] (art.6, §2) ou que l'utilisateur ou l'abonné (que concernent ces données) aient donné leur consentement[148] « *afin de commercialiser ses services de communications électroniques ou de fournir des services à valeur ajoutée (…)* ***dans la mesure et pour la durée nécessaires*** *à la fourniture ou à la commercialisation de ces services* » (art.6, §3). Là encore, la durée exacte de conservation (et donc d'archivage) n'est pas spécifiée mais cette directive renvoie elle-aussi au respect des principes de proportionnalité et de nécessité.

De plus, si ces communications sont enregistrées pour servir de preuve d'une transaction commerciale (ainsi les informations du CMR servent principalement comme preuve des conditions du contrat de marchandise et de sa mise en œuvre - voir première partie) la Directive 2002/58/CE prévoit que les dispositions de la directive 95/46/CE soient applicables

---

[144] Or, par dérogation à ces dispositions, la Directive 2006/24/CE sur la conservation des données du 15 mars 2006 (et modifiant la Directive 2002/58/CE) **exige la conservation de certaines données relatives au trafic et aux données de localisation (art. 5) pendant une période pouvant aller de 6 mois à deux ans (art. 6)** *« en vue de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne »* (art. 1).

[145] Cf. page 6 du 'Rapport technique du CETIC pour le premier semestre 2009', où dans le cadre de la transmission des données, les données peuvent être stockées temporairement dans le terminal afin d'assurer le bon flux des transferts et d'éviter au maximum les pertes.

[146] Cf. article 5, §2 de la Directive 2002/58/CE et le Considérant (22) qui précise que « … ***au cours de la période de stockage la confidentialité des informations reste garantie****…* ».

[147] En principe, cette période va de 5 à 7 ans selon le droit fiscal du pays concerné. On remarquera que pour le cas précis du CMR, le droit fiscal prévoit la conservation du 3ème exemplaire du CMR pendant 7 ans à des fins de contrôle (voir point plus haut).

[148] Le "consentement" d'un utilisateur ou d'un abonné correspond au "consentement de la personne concernée" figurant à l'article 2, h. de la directive 95/46/CE (cf. art.2, f. de la Directive 2002/58/CE et Considérant (17) qui précise que : « ***Le consentement peut être donné selon toute modalité appropriée permettant à l'utilisateur d'indiquer ses souhaits librement, de manière spécifique et informée, y compris en cochant une case lorsqu'il visite un site Internet.*** » - souligné par l'auteur).

en pareil cas[149], en précisant toutefois **que les parties aux communications soient informées « *de l'enregistrement avant qu'il n'ait lieu, de la ou des raisons pour lesquelles la communication est enregistrée et de la durée du stockage de l'enregistrement* » et que cet enregistrement soit effacé « *dès que possible et, en tout état de cause, lors de l'expiration du délai légal de recours contre la transaction* »**[150].

En fait, là encore, les dispositions de la Directive 95/46/CE concernant **l'information préalable et loyale des personnes concernées** pour des traitements de données à caractère personnel les concernant, ainsi que les **temps de conservation strictement limités** de ces données, sont les **principes à retenir en matière de respect de la vie privée dans le cadre de ce projet**.

B. Les textes juridiques applicables au niveau belge

Après avoir vu les principes et acteurs-clé posés par la législation européenne, et qui s'appliquent aux flux de données à caractère personnel dans le cadre de transports impliquant plus d'un pays européen, il est nécessaire de préciser quelques dispositions du droit belge en matière de vie privée, afin de compléter le cadre juridique applicable à ce projet.

1) La Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (modifiée par la loi du 11/12/98) et l'Arrêté royal du 13 février 2001

La loi belge relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel du 8 décembre 1992[151] (ou loi « vie privée ») **transpose la Directive 95/46/CE dans le droit belge et définit les droits de la personne concernée ainsi que les devoirs du responsable du traitement**.

Comme nous l'avons vu avec la Directive 95/46/CE, la loi belge de transposition **crée une autorité nationale indépendante pour assurer le respect de la loi « vie privée » : la Commission de la protection de la vie privée**[152] (ou '**CPVP**').

Les dispositions de cette loi reprennent également les principes fondamentaux de la directive européenne, soit les **principes de : légalité, de finalité, de proportionnalité, de transparence ; ainsi que le devoir de confidentialité et de sécurité des traitements**[153].

En principe, **la loi belge est d'application** « *lorsque le traitement est effectué dans **le cadre des activités réelles et effectives** d'un établissement fixe du responsable du traitement sur le **territoire belge** ou en un lieu où la loi belge s'applique en vertu du droit international*

[149] Cf. Considérant (23) de la Directive 2002/58/CE.

[150] *Ibidem.*

[151] Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel du 8 décembre 1992, *M.B. du 18 mars 1993*. La loi « vie privée » belge a été fortement modifiée par la loi du 11 décembre 1998 et a encore fait l'objet de modifications ultérieures, notamment par la loi du 26 février 2003. Cette loi a **fait également l'objet de nombreux arrêtés d'exécution et en particulier de l'arrêté royal du 13 février 2001.**

[152] Voir site de la CPVP sur : *http://www.privacycommission.be/fr/*

[153] Ainsi, concernant les définitions et principes européens vus ci-dessus, la loi belge les reprend pratiquement mot pour mot à son article 1er, paragraphes 1 à 8.

public » et aussi « *lorsque le responsable du traitement n'est pas établi de manière permanente sur le territoire de la Communauté européenne* ***et recourt, à des fins de traitement de données à caractère personnel, à des moyens automatisés ou non, situés sur le territoire belge****, autres que ceux qui sont exclusivement utilisés à des fins de transit sur le territoire belge* » (cf. art. 3bis, 1° et 2° de la loi « vie privée ») (souligné et gras par l'auteur). Dans ce dernier cas, par exemple, le responsable du traitement doit alors désigner un représentant sur le territoire belge.

Concernant les conditions générales de licéité des traitements, en Belgique **les principes de légalité, de finalité du traitement et de qualité des données s'appliquent aussi** et sont rappelés à l'article 4, §1er de la loi de 1992, et **c'est le responsable du traitement qui doit s'assurer de leur respect** (art. 4, §2 de la loi « vie privée »).

Selon le cadre légal belge, **le Roi peut apporter des précisions à la loi pour certaines de ses dispositions** (par arrêté délibéré en Conseil des ministres, après avis de la Commission de la protection de la vie privée, pour cette loi spécifique), **d'où l'arrêté royal (AR) d'exécution du 13 février 2001.**

La loi belge reprend également les dispositions de la directive concernant les **droits de la personne concernée** (droit d'opposition, droit d'information, droit d'accès et de rectification, etc).

Toutefois, il est utile de souligner pour notre projet que le responsable du traitement est **dispensé de fournir ces informations (art. 9, §2, e.) «** ***lorsque l'enregistrement ou la communication des données à caractère personnel est effectué en vue de l'application d'une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance*** **»** : par exemple, dans le cadre des dispositions concernant la sécurité et le repos des conducteurs (voir plus loin), il est obligatoire par la loi de collecter et de traiter les données provenant de la carte du véhicule et de la carte du conducteur, même chose pour le CMR (dont les obligations d'informations – les mentions obligatoires - sont prévues par la loi), afin de s'assurer de leur respect par les principaux intéressés (qui sont informés de ces traitements dans le cadre du respect des lois concernées), donc en principe le responsable de ces traitements ne devrait pas être tenu de fournir d'informations aux personnes concernées (mais seulement en ce qui concerne les finalités envisagées par ces législations respectives).

Par contre, **en matière de mesures de confidentialité et de sécurité des traitements que le responsable du traitement doit mettre en œuvre, l'article 16 de la loi « vie privée » va au-delà des dispositions de la directive 95/46/CE, puisqu'il dispose également que** :

> *« § 1er. Lorsque le traitement est confié à un sous-traitant,* ***le responsable du traitement*** *ou, le cas échéant, son représentant en Belgique, doit :*
>
> *1°* ***choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation*** *relatives aux traitements;*
>
> *2° veiller au respect de ces mesures* ***notamment par la stipulation de mentions contractuelles;***
>
> *3°* ***fixer dans le contrat la responsabilité du sous-traitant*** *à l'égard du responsable du traitement;*
>
> *4° convenir avec le sous-traitant que celui-ci* ***n'agit que sur la seule instruction du responsable*** *du traitement* ***et est tenu par les mêmes obligations que celles auxquelles le responsable du traitement est tenu*** *en application du paragraphe 3;*

*5° **consigner par écrit ou sur un support électronique** les éléments du contrat visés aux 3° et 4° relatifs à la protection des données et les exigences portant sur les mesures visées au paragraphe 3.*

*§ 2. **Le responsable du traitement ou, le cas échéant, son représentant en Belgique, doit** :*

1° faire toute diligence pour tenir les données à jour, pour rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes, ainsi que celles obtenues ou traitées en méconnaissance des articles 4 à 8;

*2° **veiller à ce que, pour les personnes agissant sous son autorité, l'accès aux données et les possibilités de traitement soient limités à ce dont ces personnes ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités du service**[154]; (…)*

*§ 4. **Afin de garantir la sécurité des données à caractère personnel, le responsable du traitement et, le cas échéant, son représentant en Belgique, ainsi que le sous-traitant doivent prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel** contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel.*

*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**[155].*

*Sur avis de la **Commission** de la protection de la vie privée, **le Roi peut édicter des normes appropriées en matière de sécurité informatique pour toutes ou certaines catégories de traitements.** »*[156] (souligné et gras par l'auteur).

Il est important de souligner que le responsable du traitement[157] est **tenu d'effectuer une déclaration préalable à la Commission de la protection de la vie privée belge**[158], qui tient un registre public afin que chaque personne concernée puisse savoir « qui » et « pourquoi » on effectue des traitements de ses données personnelles. Toutefois, **certains traitements sont dispensés de cette déclaration** comme, par exemple, **ceux concernant « l'administration**

[154] Ce qui suppose concrètement que des mesures de sécurité organisationnelles spécifiques soient prises pour éviter que tous les employés, surtout ceux non habilités, n'accèdent aux données des personnes concernées : le responsable du traitement doit donc désigner clairement quelles personnes peuvent ou pas y accéder et les traiter, ainsi que leur niveau de responsabilité en cas de problèmes.

[155] Une analyse de l'impact des mesures de sécurité techniques à mettre en place devrait donc être réalisée préalablement à tout traitement « à risque ».

[156] **La Commission de la Protection de la vie privée belge a ainsi édicté une note** où elle reprend les mesures principales pour assurer la sécurité et la confidentialité des données à caractère personnel, voir sur : http://www.privacycommission.be/fr/static/pdf/note-s-curit--des-donn-es---caract-re-personnel.pdf , **ainsi que des mesures de référence à mettre en place en matière de sécurité** : http://www.privacycommission.be/fr/static/pdf/mesures-de-r-f-rence-vs-01.pdf

[157] Il arrive que les finalités ou les moyens d'un traitement soient déterminés conjointement par plusieurs responsables, dans ce cas-ci ils devront introduire une déclaration commune.

[158] La déclaration peut être introduite soit en complétant un formulaire papier, soit directement sur internet via le site de la Commission, qui dispose de plusieurs modèles selon les finalités poursuivies (ex. : déclaration ordinaire, déclaration de codage de données à des fins historiques, etc), voir FAQs à ce propos sur : http://www.privacycommission.be/fr/faq/aangifte/

des salaires » (cf. art. 51 de l'Arrêté Royal du 13 février 2001) **sous réserve que certaines conditions (énumérées limitativement par l'AR) soient respectées** :

- ces données doivent être **utilisées exclusivement pour la gestion des salaires**,
- elles doivent être **transmises uniquement aux personnes qui ont le droit d'en obtenir communication** ;
- **et ne pas être conservées au-delà du temps nécessaire aux finalités du traitement** (qui est de 5 ans dans le cadre de la législation relative aux documents sociaux), entre autres.

C'est **également le cas en ce qui concerne « l'administration du personnel »** (art. 52 de l'AR du 13/02/2001) **pour autant que le traitement ne se rapporte ni à des données relatives à la santé de la personne concernée, ni à des données sensibles** ou judiciaires, **ni à des données destinées à une évaluation de la personne concernée** [159] ; **ou encore la « gestion de la clientèle et des fournisseurs »** (art. 55 de l'AR du 13/02/2001) « ***pour autant*** *que pour la clientèle, aucune donnée à caractère personnel ne soit enregistrée sur base d'informations obtenues de tiers*[160] *et* ***que les données ne soient pas communiquées à des tiers*** *(sauf dans le cadre de l'application d'une disposition légale ou réglementaire ou encore aux fins de la gestion normale d'entreprise)* » (souligné et gras par l'auteur).

Il faut également souligner que cette obligation de déclaration à la CPVP ne sert pas à demander un permis ou une autorisation à effectuer un traitement de données à caractère personnel, ce n'est qu'une **déclaration qui consiste principalement en une description précise** du traitement de données envisagé (et des moyens et finalités de ce traitement), des données à caractère personnel à traiter et des personnes (ou catégories de personnes) concernées par le traitement, de l'établissement du (ou des) responsable(s) du traitement, ainsi que d'une description des mesures de sécurité organisationnelles et techniques qui vont être mises en œuvre lors de ce traitement (ces dernières ne seront pas toutefois rendues publiques dans le registre de la Commission), **afin d'assurer le respect du principe de transparence posé par la loi**. On peut ainsi consulter le registre public de la CPVP pour connaitre des déclarations déjà effectuées ou pour connaitre les détails concernant tel ou tel traitement (nom du responsable, données concernées, etc).

Toutefois, même si cette déclaration n'est pas une autorisation en soi, **elle est obligatoire** et, en matière de recours juridictionnel, **la Commission Vie Privée est compétente pour examiner les plaintes qui lui sont adressées par toute partie intéressée par un traitement de données à caractère personnel sur le territoire belge** (art. 31 de la loi « vie privée ») cependant, si ces plaintes s'avèrent recevables, la Commission a essentiellement un **rôle de médiation**.

Notons toutefois que, si une conciliation entre les parties n'est pas possible, **la Commission peut également émettre un avis motivé** sur le « caractère fondé de la plainte », qui peut être également **accompagné de recommandations à l'intention du (ou des) responsable(s) du traitement susvisés** (art. 31, §3 et 4 de la loi « vie privée ») et en adresser une copie au

[159] Or, celle-ci est une des finalités du traitement des données du CMR dans ce projet, ce qui exclut d'office la dispense de déclaration à la CPVP (il faudra donc en réaliser une).

[160] Là encore, les données enregistrées sur le CMR sont pratiquement toujours le fait de tiers (du chauffeur, de la personne qui se trouve sur les lieux de livraison de la marchandise, du service clientèle, etc), donc la dispense de déclaration ne s'appliquera pas à notre projet.

Ministère de la Justice. Elle a également le **pouvoir de dénoncer au Procureur du Roi les infractions à la loi « vie privée » dont elle a connaissance** (art. 32, §2) et elle peut soumettre au tribunal de première instance tout litige concernant l'application de la loi et de ses mesures d'exécution (art. 32, §3 de la loi « vie privée »). Une action devant les cours et tribunaux ordinaires de la part des personnes concernées est également toujours possible (le recours à la CPVP n'exclut pas cela).

En ce qui concerne les **sanctions prévues par la loi en cas de non respect des dispositions de la loi « vie privée »** (notamment en matière de sécurité et de confidentialité des traitements, par exemple), celle-ci prévoit également des **peines d'amendes** (pouvant aller de 100 euros à 20'000 euros) **à l'encontre du responsable du traitement, de son représentant en Belgique, de son préposé ou de son mandataire** (cf. art. 38 et suivants de la loi « vie privée »).

Nous verrons dans les points successifs les aspects techniques et tous les dispositifs embarqués dans le véhicule qui pourraient contenir des données à caractère personnel ou qui, par recoupement d'informations, pourraient aboutir à obtenir des données à caractère personnel au sens de la loi « vie privée » belge, et qui sont donc concernées par toutes ces dispositions.

2) La loi du 13 juin 2005 relative aux communications électroniques

La loi du 13 juin 2005[161] (ci-après loi « communications électroniques ») est aussi **intervenue pour transposer en droit belge plusieurs directives européennes[162] concernant les communications électroniques**, dont la Directive 2002/58/CE abordée ci-dessus.

Elle transpose notamment quelques **définitions juridiques** en droit belge dont, entre autres, celle de « **réseau de communication électronique** » qui s'entend par : « *les **systèmes de transmission, actifs ou passifs et, le cas échéant, les équipements de commutation ou de routage et les autres ressources qui permettent l'acheminement de signaux par câble, par***

[161] Loi du 13 juin 2005 relative aux communications électroniques, *M.B. 20.06.2005.*

[162] Ainsi cette loi transpose plusieurs directives européennes adoptées dans ce domaine, dont:

- la Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive "Cadre") (*J.O.C.E. 24 avril 2002, L 108/33*) ;
- la Directive 2002/20/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l'autorisation de réseaux et de services de communications électroniques (directive "Autorisation") (*J.O.C.E. 24 avril 2002, L 108/21*) ;
- la Directive 2002/19/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l'accès aux réseaux de communications électroniques et aux ressources associées (directive "Accès") (*J.O.C.E. 24 avril 2002, L 108/7*),
- la Directive 2002/22/CE du Parlement européen et du Conseil du 7 mars 2002 concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques (directive "Service universel") (*J.O.C.E. 24 avril 2002, L 108/51*) ;
- la Directive 2002/58/CE (celle qui nous concerne – voir points précédents)
- et la Directive 2002/77/CE de la Commission du 16 septembre 2002 relative à la concurrence dans les marchés des réseaux et des services de communications électroniques (directive "Concurrence") (*J.O.C.E. 17 septembre 2002, L 249/21*)

(voir textes sur :

http://www.bipt.be/fr/203/DocListPub/Cadre_europ%C3%A9en/DocListPub.aspx?_themeID=21).

voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques, *dans la mesure où ils sont utilisés pour la transmission de signaux autres que ceux de radiodiffusion et de télévision* » (cf. art. 2, 3° de la loi du 13/06/2005), ce qui fait que cette loi est également d'application dans le cadre de ce projet.

Cette loi reprend également la définition de ce qu'est une 'donnée de localisation' et une 'donnée de trafic' (telles que définies par la Directive 2002/58/CE), et l'article 113 de la loi « communications électroniques » **donne à l'Institut belge des services postaux et des télécommunications (l'IBPT)[163] la faculté de « *coordonner les initiatives relatives à la qualité et à la sécurité des [réseaux publics de communications électroniques et] services de communication électronique* »**. Cet Institut est aussi « *chargé de détecter, d'observer et d'analyser les problèmes de sécurité, et de fournir aux utilisateurs des informations continues en la matière* »[164].

Donc, au-delà des obligations qui incombent au responsable du traitement dans le cadre de la loi « vie privée », la loi « communications électroniques » instaure aussi une **responsabilité d'information aux fournisseurs de réseaux publics de communication électronique**, puisque l'article 113, §3, dispose que les « *entreprises fournissant des réseaux publics de communication électronique ainsi que les entreprises fournissant des services de communication électronique accessibles au public* ***doivent publier sur leur site Internet, à l'intention des utilisateurs finals****, des* ***informations comparables, adéquates et actualisées concernant la qualité du réseau et du service*** »[165], afin que l'obligation d'assurer des moyens de sécurité et de confidentialité aux traitements de données à caractère personnel via les réseaux de communications électroniques soit réellement possible.

De plus, l'article 114 de cette loi dispose que :

> *« Le* ***fournisseur*** *d'un service de communications électroniques accessible au public* ***prend les mesures d'ordre technique et organisationnel appropriées afin de garantir la sécurité de ses services****, le cas échéant* ***conjointement avec le fournisseur du réseau public*** *de communications [électroniques] en ce qui concerne la sécurité du réseau. Compte tenu de l'état de la technique et du coût de leur mise en œuvre,* ***ces mesures garantissent un degré de sécurité adapté au risque existant.*** *»* (souligné par l'auteur)[166]

Donc, dans le cas des communications électroniques transmises via le Stepp III dans le projet eCMR, non seulement toutes les transmissions de données pouvant être considérées comme étant des données à caractère personnel devront être protégées par le responsable des traitements éventuels (à déterminer au cas par cas), mais il incomberait également au fournisseur du réseau public d'internet ou de téléphonie mobile concernés une obligation de prendre des mesures d'ordre technique et organisationnel ainsi que d'information de l'utilisateur final (et de l'IBPT) en ce qui concerne la sécurité des réseaux de communications. La complexité de cette obligation et les différentes responsabilités en cas de problèmes

[163] Tel que visé à l'article 13 de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges (cf. art. 2, 1° de la loi « communications électroniques »).

[164] Ainsi inséré par article 181 de la loi du 25 avril 2007 portant des dispositions diverses (M.B. 08 mai 2007) (cf. note sous article 113 de la loi « communications électroniques).

[165] *Ibidem.*

[166] Ainsi inséré par article 182 de la loi du 25 avril 2007 portant des dispositions diverses (M.B. 08 mai 2007) (cf. note sous article 114 de la loi « communications électroniques »).

dériveront surtout des clauses du contrat de services établi entre ces fournisseurs et le(s) responsable(s) du traitement[167].

De plus, les alinéas suivants de l'article 114 de la loi précisent que :

> *« **Le fournisseur de logiciels pour la communication électronique prend également ces mesures.***[168]
>
> *Lorsqu'il existe un risque particulier d'atteinte à la sécurité de son réseau, **l'opérateur concerné informe les abonnés et l'Institut de ce risque**.*
>
> *Les opérateurs offrent gratuitement à leurs abonnés, compte tenu de l'état de la technique, les services de sécurité adéquats, afin de permettre aux utilisateurs finals d'éviter toute forme de communication électronique non souhaitée. **Les fournisseurs de logiciels pour la communication électronique y sont également obligés vis- à- vis de leurs client[169]s.***
>
> *Lorsqu'il constate une atteinte à l'intégrité de son réseau, l'**opérateur** concerné prend toutes les mesures nécessaires **afin d'informer dans les plus brefs délais les autorités, les opérateurs et les abonnés concernés**. ».*

En ce qui concerne la protection de la vie privée et des données à caractère personnel, l'article 122, §1er de la loi « communications électroniques » précise également que « *les **opérateurs supprimment les données de trafic concernant les abonnés ou les utilisateurs finals de leurs données de trafic ou rendent ces données anonymes**, dès qu'elles ne sont plus nécessaires pour la transmission de la communication (…)* », **en prévoyant toutefois au §2 une exception de stockage de certaines données**[170] **« *dans le seul but d'établir les factures des abonnés ou d'effectuer les paiements d'interconnexion* »** et précise que :

> *« Sans préjudice de l'application 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, **l'opérateur informe, avant le traitement, l'abonné ou, le cas échéant, l'utilisateur final auquel les données se rapportent** :*
>
> *1° des types de données de trafic traitées ;*
>
> *2° des objectifs précis du traitement ;*
>
> *3° de la durée du traitement.*
>
> *Le traitement des données énumérées à alinéa 1er, est **seulement autorisé jusqu'à la fin de la période de contestation de la facture ou jusqu'à la fin de la période au cours de laquelle une action peut être menée pour en obtenir le paiement.** »*[171]

---

[167] Et ce sera aux juges à déterminer les différents niveaux de responsabilité (au cas par cas) en cas de problèmes et d'éventuels litiges.

[168] Donc ici **la société qui gérerait le logiciel de traitements de données provenant du Stepp III serait également concernée par cette obligation de mettre en place des mesures d'ordre technique et organisationnel appropriées afin de garantir la sécurité du réseau**.

[169] **Nous attirons l'attention des partenaires SMOLINFO/ORDITOOL et DOCLEDGE – fournisseurs éventuels des logiciels de traitements de données dans le cadre du projet eCMR - de cette obligation légale**.

[170] Cette dérogation concerne les opérateurs uniquement, afin d'assurer une bonne gestion des paiements d'interconnexion.

[171] Les autres dispositions de l'article 122 de la loi « communications électroniques » concernent également la finalité de marketing (qu'à condition d'obtenir le consentement - même définition que celle de la loi « vie privée - de l'abonné ou, le cas échéant, de l'utilisateur final - et sous certaines conditions : cf. art. 122, §3) ; celle pour

Même si cette loi s'applique aux opérateurs et fournisseurs de services accessibles au public, on peut considérer *a fortiori* que cela vaut également pour tout accès et transmission de données à caractère personnel via un opérateur et le réseau public, puisqu'il n'existe pas de réseaux « privés » à proprement parler que le système Step III pourrait utiliser pour transmettre ses communications électroniques.

De plus, les dispositions de la loi « vie privée » s'appliquent dès lors que des données à caractère personnel sont traitées, ce qui implique qu'il faut de toute façon respecter ses dispositions : désigner un responsable du traitement, qui sera soumis à un certain nombre d'obligations et de devoirs ; informer les personnes concernées de leurs droits ; notifier au préalable tout traitement à la Commission Vie Privée, etc (voir dispositions de la loi « vie privée » citées ci-dessus).

Il faut également respecter les mesures de sécurité et de confidentialité concernant les données à caractère personnel car, outre aux dispositions de la loi « vie privée », selon l'article 123, §1er de la loi « communications électroniques » les opérateurs de réseaux mobiles « *ne peuvent traiter de données de localisation se rapportant à un abonné ou un utilisateur final que* ***lorsqu'elles ont été rendues anonymes ou que le traitement s'inscrit dans le cadre de la fourniture d'un service à données de trafic ou de localisation***. » [172] (en gras et souligné par l'auteur).

L'article 124 de la loi va même plus loin, car si l'on n'obtient pas l'autorisation (par consentement) de « *toutes les personnes directement ou indirectement concernées* » :

« *Nul ne peut :*

1° ***prendre intentionnellement connaissance de l'existence d'une information de toute nature transmise par voie de communication électronique et qui ne lui est pas destinée personnellement ;***[173]

2° ***identifier intentionnellement les personnes concernées par la transmission de l'information et son contenu ;***

3° sans préjudice de l'application des articles 122 et 123 prendre connaissance intentionnellement de données en matière de communications électroniques et relatives à une autre personne ;

4° ***modifier, supprimer, révéler, stocker ou faire un usage quelconque de l'information, de l'identification ou des données obtenues intentionnellement ou non.*** » [174] (souligné par l'auteur).

déceler des fraudes éventuelles (données communiquées qu'aux autorités compétentes en cas de délit : cf. art. 122, §4), et **sous réserve de mettre en place des mesures organisationnelles de gestion des données** (qui ne peuvent être traitées que par les personnes chargées par l'opérateur de la facturation ou de la gestion du trafic : cf. art. 122, §5).

[172] Et dans ce cas-ci le traitement est limité à ce qui est « strictement nécessaire » pour pouvoir fournir au service concerné ces données (art. 123, §4, alinéa 2 de la loi « communications électroniques »).

[173] Ce qui peut poser problème dans le domaine des relations professionnelles, puisque dans le cadre de ce projet le transporteur ou autre va être amené à prendre connaissance des informations du véhicule (et du chauffeur) transmises par voie de communication électronique.

[174] Idem : cela posera problème quant à la finalité de surveillance et de contrôle des travailleurs (les chauffeurs de camions) dont le gestionnaire du serveur va faire usage (par rapport aux données de localisation reçues via le Stepp III Falcom, par exemple).

Enfin, en Belgique, le Roi fixe par arrêté royal, après avis de la Commission de la protection de la vie privée et de l'IBPT, « *les modalités et les moyens à mettre en œuvre en vue de permettre l'identification, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications électroniques* » (art. 125, §2 de la loi « communications électroniques), ce qui exclut toute interception de ces communications par des personnes tierces « non autorisées ».

Si l'on envisage également les relations avec d'éventuels « clients » de l'entreprise (qui va gérer les données émanant des communications électroniques du Step III), l'article 128 de la loi « communications électroniques » prévoit quant à lui que :

> « *Sans préjudice de l'application 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, l'enregistrement d'une communication électronique et des données relatives au trafic qui s'y rapportent* ***réalisées dans les transactions commerciales licites comme preuve d'une transaction commerciale ou d'une autre communication professionnelle, est autorisé à condition que les parties impliquées dans la communication soient informées de l'enregistrement, des objectifs précis de ce dernier et de la durée de stockage de l'enregistrement, avant l'enregistrement****.*
>
> *Les données visées au présent article sont* ***effacées au plus tard à la fin de la période pendant laquelle la transaction peut être contestée en justice****. (…)* » (en gras et souligné par l'auteur).

Plusieurs arrêtés royaux ont été pris en vue de l'exécution de la loi du 13 juin 2005[175], néanmoins aucun ne semble concerner plus spécifiquement le traitement de données à caractère personnel lorsque des communications électroniques sont en jeu.

C. Les aspects techniques du projet[176]

Comme nous l'avons déjà mentionné, le CETIC, en accord avec les autres partenaires industriels du projet eCMR[177], a choisi d'intégrer le module « SteppIII » de Falcom dans l'architecture du système technique, et a distingué plusieurs phases importantes dans la transmission des données du véhicule au serveur distant[178]:

« 1ère phase : différents équipements embarqués dans le camion vont envoyer leurs données au kit de transmission de données, dont :

- *une* ***gateway CAN/FMS*** *»*

[175] Voir liste détaillée sur le site de l'IBPT : http://www.bipt.be/ShowContent.aspx?objectID=1892&lang=fr

[176] Nous nous permettons de reprendre certains termes et quelques figures des rapports techniques du CETIC – Rapport n°2 (janvier 2009) et n°3 (juillet 2009) – afin d'illustrer nos propos. Pour favoriser la compréhension du texte original de ce rapport par rapport aux textes du CETIC nous mettrons ces derniers entre « guillemets » et en *italique*. Nous remercions notre partenaire pour son autorisation via courriel à réutiliser certaines de ses figures dans notre propre rapport de recherche.

[177] Choix technologique de l'outil utilisé effectué en accord avec les autres partenaires Orditool/Smolinfo et Docledge.

[178] Cf. Rapport technique n°2 du CETIC de janvier 2009.

Il s'agit d'un **réseau de communication à l'intérieur du véhicule où l'on installe tous les équipements électriques** (en principe, ce sont des '*gateway*' propriétaires, c'est-à-dire que chaque constructeur de véhicule possède le sien propre).

- « *un **module GPS*** »

Qui **envoie la position géographique du camion en temps réel au transporteur** (et/ou propriétaire du véhicule)[179].

- « *un **tachymètre***. »

Aussi appelé tachygraphe, celui-ci est un **appareil de contrôle électronique qui enregistre la vitesse, le temps de conduite et d'activités** (travail, attentes, etc) **d'un véhicule de transport routier en temps réel**. En principe, ce système est basé sur un appareil enregistreur qui doit être scellé et installé par un personnel agréé et assermenté. Il doit comporter un système de stockage permanent et « inviolable » ainsi qu'une imprimante. **Les transferts de ses données se font par cartes à puces interopérables entre fabricants de système et pays**, comme nous le verrons ci-après.

- *« des capteurs (de température, humidité, événements). »*
- *« des I/O digitales ».*

Qui sont des dispositifs qui fournissent des informations d'entrée (I) et de sortie (O) sur les « évènements » produits par le camion (ex. : arrêt, démarrage, etc).

- *« Et des interfaces spécifiques.*

2ème phase : ce kit de transmission – le terminal GSM/GPRS/GPS « SteppIII » de Falcom - est relié à la plateforme de gestion des données par une liaison TCP/IP sur canal GPRS.

3ème phase : deux scénarios différents ont été prévus [par le CETIC] *: un système embarqué sans PC et un système embarqué avec PC.* »

Nous allons examiner ci-après les traitements de données (uniquement celles à caractère personnel) opérés dans le cas du deuxième scénario - le système embarqué avec PC - qui semble avoir été préféré par le partenariat du projet et qui est le plus élaboré en ce qui nous concerne[180], afin de comprendre : où sont les transferts de données, quels sont les types de données à caractère personnel transmises, et où/à qui elles sont transmises, quels sont les autres traitements effectués (etc) ?

Selon le CETIC : *« la configuration utilisant un PC embarqué fait appel au SteppIII à deux niveaux :*

- *en tant **qu'interface data fournissant les données GPS**, I/Os et accéléromètre sur l'un des ports série du module*

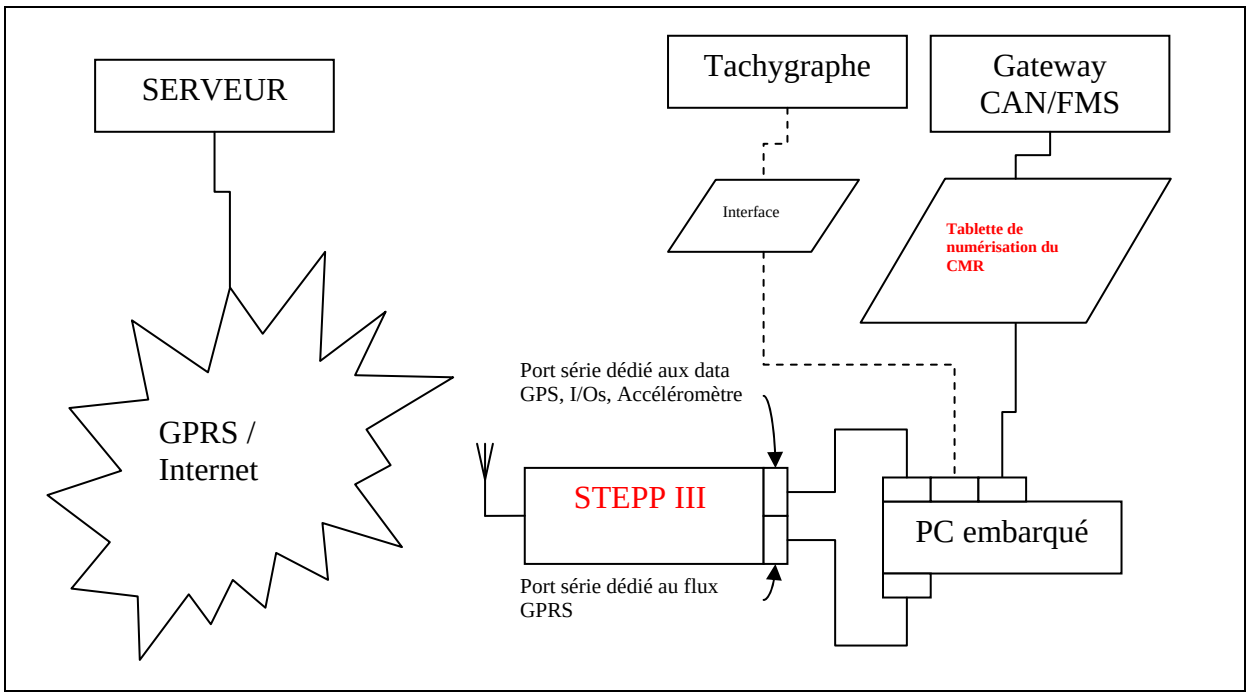
[179] GPS ou « G*lobal Positioning System* » (système de positionnement mondial ou géo-positionnement par satellite). Dans le domaine des transports, ce dispositif ne se contente pas d'être un système « passif » (en ce sens qu'il se contente de recevoir les signaux des satellites et d'en déduire la position des véhicules), car actuellement les systèmes déployés dans les véhicules adjoignent un dispositif de transmission de l'information obtenue avec le GPS qui peut fonctionner en temps réel (dans ce projet-ci il s'agit d'une liaison GPRS/internet), ceci afin de permettre aux employeurs-transporteurs de suivre leur flotte de camions en temps réel.

[180] Dans ce sens que le système embarqué de Stepp III sans PC implique que le Stepp III ne soit qu'un simple outil de transmission des données à bord du véhicule (presque rien n'est stocké en son sein, à part des données nécessaires à la gestion technique du SteppIII).

- *[et]* ***en tant qu'interface de communication vers le serveur distant via le GPRS*** *(encapsulation TCP des données série du second port série). »* [181] (souligné par l'auteur).

Dans cette dernière configuration, le PC embarqué récupèrera les données des différentes sources et utilisera le SteppIII pour communiquer avec le serveur distant (qui gérera les données reçues au moyen d'un logiciel de traitement de données).

Nous reprenons ci-après une figure[182] du CETIC afin que les flux de données soient plus évidents :



Si, au contraire, l'on ne choisissait que le (premier) scénario (où il n'y aurait pas de PC embarqué), toutes les données seraient transmises directement au serveur, par GPRS/internet, via le terminal Stepp III, qui ne serait qu'un outil de transmission de données (informations de position et données propres au camion) et de réception des commandes/ordres vers/du serveur à distance[183].

Donc, dans le (deuxième) scénario avec PC embarqué, les flux de données s'effectuent de la suivante façon :

[181] Voir page 5 du Rapport du CETIC de janvier 2009.

[182] Cf. figure 2 du Rapport technique du CETIC de janvier 2009 (avec quelques modifications par l'auteur).

Attention : selon la figure 1 du Rapport technique du CETIC de janvier 2010, nous avons également intégré le **troisième élément connecté au Stepp III : la tablette de numérisation du CMR (intégré ici en rouge à la place d'une autre interface).**

[183] Cf. point *« 2.1.1. Modélisation du flux d'information (T2.3) »* du rapport technique du CETIC de juillet 2009.

- Les différents équipements embarqués (tachygraphe, CMR via tablette électronique, etc) envoient leurs donnés au Stepp III via le PC embarqué (qui ne servirait que d'interface avec le conducteur du véhicule – sauf ajouts éventuels de fonctionnalités) ;
- Le Stepp III transfère les données au serveur de gestion de flotte via la liaison GPRS/internet ;
- Le serveur distant collecte et traite les données en tant que telles, et effectue les commandes adressées au Stepp III et au PC embarqué[184].

Comme nous l'avons déjà mentionné, **le Stepp III effectue les suivants traitements au sens de la loi « vie privée »[185] : la collecte et la transmission de données**, puisqu'il envoie tant des données qui concernent tant le véhicule que les personnes (données sur CMR, données de localisation via le GPS/GPRS) qui le conduisent ou se retrouvent en sa présence (on pourrait identifier un client via le lieu de son établissement, par exemple), entre autres.

Toutefois, **c'est au niveau du serveur distant** (qui gère l'arrivée des données du Stepp III) géré soit par le transporteur, soit par une entreprise tierce fournisseur de services à valeur ajouté, **que la plupart des traitements de données à caractère personnel envisagés dans le point suivant auront lieu**.

D. Les données à caractère personnel et les traitements de données concernés par le projet eCMR

En ce qui concerne le projet eCMR, les données à caractère personnel qui vont être concernées ici **vont découler essentiellement des données fournies par les différents systèmes embarqués dans les véhicules**, qui transmettent certaines données au serveur distant via le Stepp III.

Comme on vient de le voir, les **types d'informations pouvant être considérées comme des « données à caractère personnel » peuvent être de différentes sortes** :

- au niveau du **CMR**, on retrouve des **données à caractère personnel dans plusieurs contenus des mentions obligatoires du CMR** (soit, par ex. : le nom et l'adresse de l'expéditeur; le nom et l'adresse du transporteur; ou le nom et l'adresse du destinataire[186]) ;
- au niveau du **GPS**, les **données de localisation** transmises concernent tant la localisation du véhicule, que de son (ses) chauffeur(s) (personne physique) ou de la marchandise (lieu de chargement/déchargement qui peut être révélateur d'une adresse physique), etc.
- au niveau des autres systèmes embarqués : le **tachygraphe** peut également envoyer des **informations à caractère personnel** (par ex. temps d'arrêt/de travail pratiqués par tel ou tel chauffeur **via sa carte professionnelle**) ; les **autres capteurs du véhicule, I/O digitales et interfaces spécifiques**, révèlent également des données concernant le véhicule et la façon dont il est utilisé (donc **révèlent implicitement la façon de conduire du travailleur**), etc.

[184] *Ibidem.*

[185] Voir définition du 'traitement de données' dans la partie précédente (ou art. 2, b. de la Directive 95/46/CE).

[186] Voir point spécifique en première partie.

On peut donc établir d'ores et déjà que dans le cadre du projet eCMR, **il y aurait plusieurs traitements de données avec des finalités distinctes à envisager qui parfois peuvent se recouper** (on localise un camion pour contrôler son chauffeur, par exemple) **mais qu'il faut aborder ci-après comme des traitements différents, avec des implications et des conséquences différentes** (le contrôle du bon fonctionnement du véhicule ne devrait pas forcément mener au contrôle de la façon de conduire du chauffeur, par exemple).

Nous nous permettons d'identifier déjà ici **plusieurs finalités différentes**, qui devraient faire l'objet de plusieurs traitements de données distincts (certains pourraient être connexes), mais qui devront être précisées et définies plus spécifiquement par les personnes intéressées ultérieurement[187].

Ces finalités pourraient être :

- **soit de suivi de flotte et de marchandise,**
- **soit de localisation de véhicule et/ou de marchandise,**
- **soit de contrôle et de surveillance des travailleurs,**
- **soit de rationalisation des moyens/outils de travail** (véhicule, déplacements, etc) **qui pourrait entraîner une évaluation implicite du travailleur concerné** ;
- etc.

En soi ces différentes finalités ne sont pas « illégales » et pourraient se justifier pour plusieurs raisons (respect des législations de sécurité routière en vigueur, respect des dispositions contractuelles commerciales, respect de la législation sociale et du travail, etc), toutefois des « nuances de légitimité » des finalités de ces traitements pourraient apparaitre lorsque ce contrôle ou cette localisation, par exemple, serviraient à diminuer la liberté d'aller et de venir du chauffeur du camion, à entraver le respect de sa vie privée pendant (ou pas) son temps de travail, etc. C'est pourquoi nous avons décidé de distinguer les problématiques juridiques relatives aux relations d'emploi plus loin, dans le deuxième point (**II**) de cette partie, afin d'analyser les règles de protection de la vie privée applicables dans les relations de travail.

Pour en revenir aux informations pouvant être considérées comme des données à caractère personnel dans les traitements de données existant dans le projet eCMR (tels que décrits par les différents rapports techniques des autres partenaires[188]), **ces données proviennent principalement des suivants dispositifs embarqués dans le/à bord du véhicule** :

1) Le tachygraphe (digital)[189]

En effet, la législation en vigueur[190] prévoit qu'un tachygraphe digital soit installé sur tous les véhicules soumis au Règlement (CEE) N° 3820/85 relatif au temps de conduite et de repos[191]

[187] Il ne s'agit ici que de suppositions étant donné que ces traitements n'existent pas encore, nous nous avançons seulement sur les éventuels traitements qui pourraient exister au regard des technologies/outils utilisés.

[188] Cf. données du 'Rapport Technique Intermédiaire Semestre 4' du Coordinateur, du 'Rapport Intermédiaire du 12/04/2010' du partenariat eCMR et du 'Rapport technique pour le deuxième semestre 2009' du CETIC du 11/01/2010.

[189] Pour plus d'informations concernant le tachygraphe pouvant être utilisé par les partenaires du projet eCMR, nous renvoyons le lecteur au point 2.1.1.1.4. du dernier rapport du CETIC (cité ci-avant).

[190] Cf. Arrêté Royal du 13 juillet 1984 portant exécution du règlement (C.E.E.) n° 3821/85 du Conseil des Communautés européennes du 20 décembre 1985 concernant l'appareil de contrôle dans le domaine des transports par route, modifié par l'AR du 14 juillet 2005 (publié le 26 juillet 2005). Toutes les réglementations

tant pour les transports pour compte propre que pour les transports pour compte de tiers[192]. Il s'agit, sauf à quelques rares exceptions, des véhicules utilisés pour le transport de marchandises d'une masse maximale autorisée supérieure à 3,5 tonnes, y compris les remorques et semi-remorques.

En principe, ce dispositif a été rendu obligatoire par la loi pour remplir les suivants objectifs :

- « *renforcer la sécurité routière, car il* ***permet aux conducteurs et aux transporteurs de connaitre la vitesse de conduite suivie, les temps d'arrêts réglementaires, les temps de conduite ainsi que tous les temps de travail ou de disponibilité*** *(dont le total donnera le temps de service) ;*
- *améliorer les conditions de travail des conducteurs, car il* ***permet de veiller au respect des temps de repos quotidiens et hebdomadaires prescrits par les textes législatifs*** *;*
- *promouvoir la « loyauté » de la concurrence et* ***faciliter la gestion des entreprises de transport routier*** »[193] (souligné par l'auteur).

Le système qui doit être mis en place est, en principe, très sécurisé car il se compose du tachygraphe digital lui-même relié à un capteur de mouvements du véhicule. Ce tachygraphe est équipé d'une mémoire, d'un écran de lecture, d'un connecteur pour le téléchargement, de deux lecteurs de carte et d'une imprimante. **La mémoire de l'appareil doit conserver au moins 365 jours de données relatives au véhicule et aux conducteurs de ce véhicule, dont trois clés « secrètes » doivent assurer la sécurisation de l'enregistrement et de la conservation des données**[194].

On peut remarquer que **les cartes que l'on va utiliser pour enregistrer et lire les données de ce tachygraphe** (carte du conducteur, etc) **permettent la collecte et le traitement de toute une série de données que l'on pourra considérer « à caractère personnel »** au sens de l'article 1er, §1 de la loi du 8 décembre 1992 sur la protection des données à caractère personnel.

Si nous reprenons le tableau de synthèse de ces données citées au point 2.1.1.1.4.4 du 'Rapport Technique du CETIC de janvier 2010', nous pouvons d'ores et déjà remarquer que l'on retrouve ce type de données à plusieurs reprises, dont : l'état du travail ; l'état du chauffeur 1 et 2 ; la vitesse du véhicule (conduit par les chauffeurs) ; le numéro d'identification et le numéro d'enregistrement du véhicule (qui renvoie au propriétaire du véhicule) ; le pays d'enregistrement de la carte (idem) ; les alertes (temps de repos obligatoire) concernant le chauffeur 1 et 2 ; etc. En effet, l'enregistrement des données mentionnées ci-dessus se fait **via la transmission des informations contenues dans la puce des cartes suivantes :**

---

en vigueur en Belgique concernant le tachygraphe digital sont disponibles sur : http://www.optimumservices.org/WXTextes/Textes.htm

[191] Règlement (CEE) n° 3820/85 du Conseil du 20 décembre 1985 relatif à l'harmonisation de certaines dispositions en matière sociale dans le domaine des transports par route, *JO L 370 du 31.12.1985, p. 1–7.*

[192] Depuis le 5 août 2005, le tachygraphe digital est obligatoire dans tous les Etats membres de l'Union européenne ainsi qu'en Suisse, en Islande, en Norvège et au Liechtenstein.

[193] Source SPF Mobilité et Transports : http://www.mobilit.fgov.be/fr/index.htm (rubrique « Route » - « Temps de conduite et de repos » - « tachygraphe »).

[194] *Ibidem.*

a. La carte de conducteur[195] :

Cette **carte professionnelle et personnelle** a remplacé l'ancienne feuille d'enregistrement (disque) **et doit conserver en mémoire les prestations d'au moins les 28 derniers jours d'activité du conducteur** (conduite, repos,…), **quel que soit le véhicule qu'il ait conduit**.

Les **informations stockées** sur cette carte concernent **l'identification du conducteur[196]** (et il ne peut en avoir qu'une carte en même temps dans le véhicule); l'identification du ou des véhicules qu'il a conduit ; **les temps de conduite, de travail et de repos** (et donc son respect de la législation en vigueur) ; le type d'activité et son début et fin ; le statut de sa conduite, la distance parcourue, les anomalies de fonctionnement et les pannes éventuelles.

Elle a une **validité administrative de 5 ans et est attribuée par l'Etat de résidence du conducteur**. La carte du conducteur va donc révéler tout un ensemble de données personnelles relatives à un conducteur, « personne concernée » au sens de l'article 1, §1er de la loi « vie privée » : **ces données serviront tant à s'assurer du respect des législations en vigueur (temps de conduite et repos, etc) qu'à le localiser à un moment donné sur un véhicule donné**, par exemple. Les dispositions de la loi « vie privée » vont donc s'appliquer ici[197] et, au-delà de l'utilisation initiale de la carte prévue par la loi (carte professionnelle retraçant l'activité du conducteur), pour toute nouvelle finalité (autre que celle prévue initialement par la loi) il faudra envisager la désignation d'un responsable de traitement, déclarer ce nouveau traitement à la CPVP, informer les personnes concernées (travailleurs), etc.

Rappelons que **la collecte de ces données se fait via le tachygraphe et qu'elles sont transmises via le PC embarqué et l'interface Stepp III au serveur distant** (qui gérera également les données reçues et les utilisera éventuellement pour gérer des données sociales et/ou de contrôle du respect des législations en vigueur par le conducteur[198], par exemple). Dans le projet eCMR, un rapport « *en live* »/temps réel est prévu pour prévenir le chauffeur de la fin du temps légal de son activité de conduite, par exemple, donc il y aura une analyse des données, qui se fait via le serveur et le logiciel distants, qui pourrait avoir des incidences sur la « vie privée » des conducteurs (voir points suivants).

b. La carte d'entreprise :

Cette carte donne accès aux **données relatives aux véhicules et aux conducteurs de l'entreprise conservées dans la mémoire de l'unité du véhicule**. Elle est utilisée par le transporteur (et/ou le propriétaire du véhicule) pour permettre le **téléchargement des informations contenues dans l'unité embarquée du véhicule** et elle **permet de récupérer**

---

[195] Dont le modèle de formulaire de demande a été fixé par l'arrêté royal du 14 juillet 2005 portant exécution du Règlement (CEE) n°3821/85. Voir aussi sur : http://www.digitach.be/fr/PDF/Tacho%20FR%20Driver%20Request%201.0.pdf

[196] La carte contient aussi un numéro de carte chauffeur unique, ce qui permet d'identifier le conducteur (cf. point 2.3.1 du 'Rapport Technique Intermédiaire – Semestre 4' cité ci-dessus).

[197] Voir partie B ci-dessus.

[198] Voir Annexe 1 du 'Rapport Technique Intermédiaire – Semestre 4' du partenariat (cité ci-dessus) : qui indique que désormais il existe des tachygraphes élaborés par certains constructeurs industriels de tachygraphe qui permettent le téléchargement légal à distance en direct depuis le tachygraphe (donc est en avance sur les moyens techniques adoptés par le projet eCMR) – voir également « remarque commerciale » au point 2.2.2. du même rapport.

toutes ces données pour opérer des contrôles internes, calculer des salaires ou encore verrouiller les données en cas de vente ou de location d'un véhicule.

Une entreprise peut avoir plusieurs cartes et celles-ci ont une **validité de 5 ans**. Là encore, la carte d'entreprise est **attribuée par les Etats membres où les entreprises sont enregistrées** (en Belgique, les entreprises doivent être enregistrées auprès de la Banque Carrefour des Entreprises). Cette carte va elle aussi **contenir des données à caractère personnel**, du même type que celles mentionnées dans le point précédent **et, en recoupant ses informations avec la première carte (du conducteur), le transporteur va pouvoir émettre une fiche de paye**, entre autres, à tel ou tel conducteur ayant conduit ses véhicules : il y a donc traitement de données à caractère personnel au sens de la loi « vie privée ».

De plus, **il faut souligner que cette « mémoire » de données à caractère personnel échappe au contrôle des conducteurs** (personnes concernées), puisqu'elles se rapportent essentiellement aux données conservées dans la mémoire de l'unité du véhicule, qui est lui sous le contrôle du propriétaire du véhicule. Donc, là encore, la loi « vie privée » devra s'appliquer à tout traitement de données ultérieur (non prévu par la législation initiale imposant la carte d'entreprise).

c. La carte d'atelier :

Cette carte-ci permet l'initialisation, l'étalonnage et le calibrage de l'appareil ainsi que d'autres interventions techniques, ce qui est réalisé uniquement par des centres agréés, qui vont garantir l'intégrité et la sécurité du système.

Elle a une **fonction essentiellement de contrôle du tachygraphe lui-même et des différentes interventions techniques subies par l'appareil et/ou le véhicule**.

La loi « vie privée » ne devrait donc pas s'appliquer, à moins qu'un fichier ou une base de données contenant des données à caractère personnel (associant la carte à un véhicule appartenant à un transporteur[199], par exemple, ou à un travailleur) soit réalisée par ces centres agréés, mais ce n'est pas sa finalité originelle.

d. La carte du contrôleur :

Cette dernière carte **permet aux agents mandatés d'avoir accès aux données contenues dans la mémoire de l'unité du véhicule et dans les cartes de conducteur et/ou de les télécharger**. Des autorités de contrôle spéciales doivent disposer d'un matériel informatique spécifique pour récupérer l'ensemble de ces données.

Là encore, des données à caractère personnel sont en cause, et elles peuvent impliquer plusieurs « personnes concernées » au sens de la loi « vie privée » : les conducteurs, mais aussi les transporteurs et/ou propriétaires des véhicules utilisés.

En principe, **les données contenues dans la mémoire de l'unité du véhicule, des cartes de conducteur et des cartes d'atelier doivent être régulièrement téléchargées par les**

[199] Mais il faut souligner que la loi belge ne protège que les données des personnes physiques, individus, et non celles des sociétés, personnes morales, en tant que telles. Attention, ceci n'est toutefois pas le cas dans tous les pays européens : ainsi au Luxembourg, ou en Italie, par exemple, les lois « vie privée » incluent cette protection, alors même que la directive 95/46/CE ne le prévoyait pas à l'origine, il faudra en tenir compte si des flux de données à caractère personnel circulent entre la Belgique et ces pays.

entreprises afin de constituer une banque de données permettant ces contrôles. Ces bases de données peuvent constituer également un outil de gestion de flotte pour les entreprises.

A cette fin, et pour faciliter le contrôle et la gestion de ces cartes, une interopérabilité totale devrait être assurée à une large échelle, puisque toutes les cartes devraient pouvoir être utilisées dans tous les appareils quelle qu'en soit la marque et tous les appareils devraient accepter toutes les cartes. En ce sens, il existe des obligations spécifiques à l'égard des données destinées pour le contrôle en entreprise enregistrées par le tachygraphe digital[200], dont la délivrance (de toutes ces cartes) doit se faire via le service DIGITACH en Belgique[201].

Par ailleurs, le service belge de DIGITACH[202] est relié au système européen TACHONET (*Telematics Network for the Exchange of Information Concerning the Issuing of Tachograph Cards*)[203] qui est un réseau télématique qui permet l'échange d'informations concernant les tachygraphes délivrés par chaque Etat membre.

Toutefois, comme l'a fait remarquer notre partenaire CETIC[204], en pratique, il n'y aurait que trois constructeurs qui proposent des tachygraphes numériques homologués conformément aux directives européennes, même si la majorité des données obligatoires devant être émises par les tachygraphes se retrouvent dans tous les trois modèles[205].

Concernant les conditions de licéité que la législation « vie privée » impose, au regard de l'article 5 de la loi belge de 1992 (applicable au niveau national) ainsi que de l'article 7 de la Directive européenne 95/46/CE[206] (qui a été transposée par tous les Etats membres de l'Union Européenne), la légalité des traitements prévus à l'origine de l'introduction de l'obligation du tachygraphe et de ces cartes devrait être assurée puisque leur existence est prévue par une législation en vigueur.

On peut citer comme exemple la loi du 21 décembre 2006[207], qui avalise l'utilisation d'équipements embarqués interopérables, dont le tachygraphe, et qui prévoit à son article 4 que :

> *« Le traitement des données à caractère personnel nécessaires au fonctionnement du service européen de télépéage s'effectue en conformité avec les normes protégeant les libertés et les droits fondamentaux des personnes, y compris leur vie privée, et dans le respect des dispositions de la loi du 8 décembre 1992 relative à la protection de la vie*

---

[200] Voir document de l'ITLB – DIGITACH là-dessus sur : http://www.digitach.be/fr/PDF/downloaddatafr.pdf

[201] Voir conditions d'obtention et de délivrance des cartes sur : http://www.digitach.be/fr/frameset.htm

[202] L'ASBL «Institut Transport Routier et Logistique Belgique» (ITLB)) a été mandatée par l'Etat belge pour exécuter, par délégation et sous le contrôle du SPF Mobilité et Transports, la mission d'autorité publique consistant à organiser et à exploiter le système de gestion et de délivrance de toutes les types de cartes tachygraphiques associées au tachygraphe digital : un service interne – en l'occurrence le **SERVICE DIGITACH** - a été créé à cette fin (voir plus d'informations sur : http://www.digitach.be/fr/frameset.htm).

[203] Voir site européen sur : http://ec.europa.eu/idabc/en/document/2283/5926. « Tachonet » est un réseau d'échange entre les autorités nationales qui ont la responsabilité de la délivrance des cartes afin de bien s'assurer notamment qu'un conducteur ne possèdera pas plusieurs cartes.

[204] Voir dernier Rapport Technique cité avant, aux points 2.1.1.1.4 (pp. 6 et suiv.).

[205] Ibidem.

[206] En effet, l'article 5, c) précise que *« Le traitement de données à caractère personnel ne peut être effectué que dans l'un des cas suivants : (…) c) lorsqu'il est nécessaire au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une loi, d'un décret ou d'une ordonnance; (…) »*.

[207] Loi transposant la directive 2004/52/CE du Parlement européen et du Conseil du 29 avril 2004 concernant l'interopérabilité des systèmes de télépéage routier dans la Communauté, *M.B. du 29 décembre 2006.*

privée à l'égard des traitements de données à caractère personnel et de la loi du 13 juin 2005 relative aux communications électroniques. ».

De plus, on peut dire que d'autres dispositions légales sont également en jeu, puisqu'il s'agit ici d'un **secteur professionnel particulier où d'autres législations** (de sécurité routière, de respect des temps de conduite et de repos, etc) **rentrent également en compte et dont on se doit d'assurer la proportionnalité des différents intérêts en jeu** (respect de la vie privée *versus* le contrôle du respect de ces autres règles, garantes du bon fonctionnement du parc routier et de la santé et sécurité des chauffeurs routiers, par exemple) [208].

On peut citer également, parmi ces autres règles, les **dispositions du Règlement (CEE) 561/2006 relatif aux temps de conduite et de repos[209] dans le transport par route** : celles-ci sont **d'application sur tous déplacements effectués dans leur totalité ou en partie sur le réseau routier ouvert au public**, par des véhicules en charge ou à vide, destinés au transport de marchandises par des véhicules dont la masse maximale autorisée, y compris celle des remorques ou des semi-remorques, dépasse les 3,5 tonnes; et au transport de personnes par des véhicules prévus à cet effet et qui sont construits ou aménagés de façon permanente pour le transport de plus de 9 personnes, conducteur compris.

Ce règlement **prévoit**, entre autres, **le respect d'une durée de *'conduite journalière prédéfinie'***, celle-ci étant définie comme *« étant la durée de conduite totale accumulée entre la fin d'un temps de repos journalier et le début du temps de repos journalier suivant ou entre un temps de repos journalier et un temps de repos hebdomadaire »*. En principe, cette durée ne peut pas dépasser 9 heures, toutefois, deux fois par semaine, la durée de conduite journalière peut être prolongée jusqu'à 10 heures maximum[210]. De plus, le temps de conduite hebdomadaire ne peut être supérieur à 56 heures. **Ce règlement encadre également les périodes[211] et les interruptions de conduite[212], ainsi que les temps de repos journaliers** (qui peuvent être normaux[213] ou réduits[214]) **que les chauffeurs (et l'entreprise qui les engagent) doivent respecter.**

De plus, ce règlement **prévoit également tous les enregistrements à présenter lors d'un contrôle routier : ceux-ci concernent tant la carte du conducteur que les disques tachygraphes analogiques et les « *print-outs* » du tachygraphe digital, et ils visent les**

[208] Nous ne nous voulons pas exhaustifs concernant ces autres réglementations, ce secteur d'activité étant assez complexe au niveau réglementaire.

[209] Cf. A.R. du 9 avril 2007 d'application du Règlement 561/2006 en Belgique.

[210] Sur base du règlement social, un chauffeur pourrait prester deux périodes de conduites journalières par jour calendrier à condition de respecter les interruptions et les périodes de repos journalières et hebdomadaires réglementaires.

[211] Qui est la durée de conduite cumulée entre le moment ou le conducteur se met au volant après un temps de repos ou une pause et le moment où il observe une pause ou un temps de repos. Le temps de conduite peut être continu ou fragmenté. Après 4 heures et demie de conduite, le conducteur doit respecter une interruption d'au moins 45 minutes, à moins qu'il n'entame une période de repos.

[212] Une interruption de conduite est définie comme *« toute période durant laquelle le conducteur ne peut conduire ni effectuer d'autres tâches et qui est uniquement destinée au repos »*.

[213] Soit toute période de repos d'au moins 11 heures par période de 24 heures ; soit le temps de repos journalier normal peut être pris en deux tranches, dont la première doit être une période ininterrompue d'au moins 3 heures et la deuxième une période ininterrompue d'au moins 9 heures.

[214] Le temps de repos journalier normal d'au moins 11 heures peut être réduit à condition de respecter les conditions suivantes: le temps de repos journalier réduit s'élève à au moins 9 heures et un conducteur ne peut prendre plus de trois temps de repos journaliers réduits entre deux temps de repos hebdomadaires.

activités du chauffeur et du véhicule du jour même ainsi que des 28 jours calendrier précédents (disques). On peut donc dire qu'il s'agit ici du traitement légal « originel » des données à caractère personnel contenues par le tachygraphe et les relatives cartes d'enregistrement des données, tel que prévu spécifiquement dans le cadre de la règlementation du tachygraphe.

Toutefois, nous avons vu que **le tachygraphe peut conserver techniquement les données pendant 12 mois, ce qui veut dire que l'on pourrait recouper les informations provenant du tachygraphe avec les cartes conducteurs introduites pendant cette période, et donc obtenir des traitements de données à caractère personnel dont la conservation pourrait être considérée comme « disproportionnée »[215] par un juge**, puisque cette loi n'impose l'obligation que de connaitre les données des 28 jours précédents un contrôle/téléchargement. **Il appartient donc aux personnes ayant un accès autorisé à ces données de ne pas les utiliser à des finalités ultérieures non compatibles avec la finalité initiale** (de contrôle, par exemple) des traitements de données à caractère personnel qui auraient été préalablement déclarés[216].

2) Le CMR (données transmises par la tablette de numérisation)

Comme nous l'avons déjà étudié dans la première partie de ce rapport[217], le chauffeur du véhicule doit avoir également en sa possession la lettre de voiture ou CMR qui accompagne toute marchandise.

Ce CMR va contenir plusieurs données à caractère personnel : que ce soit celles **du/des conducteur/s** qui ont transporté une marchandise donnée (à laquelle tel ou tel CMR correspond) ; celles du **travailleur responsable de l'entreprise de transport** (qui a signé le CMR initial, au moment de la commande, par exemple) ; celles de la **personne qui va réceptionner la marchandise** (que ce soit le client ou une entreprise tierce - intermédiaire), puisque c'est cette dernière signature qui va « conclure » les obligations légales du CMR (voir détails dans la première partie) ; etc.

La loi « vie privé » va donc trouver à s'appliquer ici : pour ce qui est des données concernant un CMR émis et traité en Belgique, ce sera la loi de 1992 qui s'appliquera, toutefois si l'on rentre dans le cadre d'un transport européen, ce seront les dispositions de la Directive européenne 95/46/CE telles qu'elles auront été transposées par les lois nationales des Etats membres qui s'appliqueront (ainsi, comme nous l'avons dit, certains Etats protègent

---

[215] En effet, tant la loi « vie privée » que la Directive 95/46/CE parlent d'une durée de conservation *« n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement (…) »* (cf. article 4, §1er, 5° de la loi de 1992 et article 6, §1, e) de la Directive 95/46/CE).

[216] Cf. article 4, §1er de la loi de 1992 (et article 6, 1. b) de la Directive 95/46/CE) qui dispose que :

« Les données à caractère personnel doivent être :

1° traitées loyalement et licitement;

2° collectées pour des finalités déterminées, explicites et légitimes, et ***ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables****. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible lorsqu'il est effectué conformément aux conditions fixées par le Roi, après avis de la Commission de la protection de la vie privée; (…) »* (souligné par l'auteur).

[217] Voir « Rapport de recherche du CRID n°1 » - Annexe 1 au Rapport d'activité n°1 (juillet 2008).

également les données concernant les personnes morales, donc il faudra en tenir compte en cas de flux transfrontaliers avec ces pays-là).

Au regard des conditions à respecter dans la législation « vie privée » (principes de licéité et légitimité des traitements, de proportionnalité, du respect de la finalité initiale du traitement, déclaration préalable à l'autorité indépendante de contrôle, etc), il ne devrait pas y avoir de différences majeures entre les différentes lois nationales de transposition. Dans le doute, il y a lieu de se référer aux dispositions de la Directive 95/46/CE.

En matière de **durée de conservation des données que le CMR contient** (et qui renvoient tant à la marchandise, qu'aux différents acteurs en jeu – chauffeur du véhicule, entreprise de transport, client, entreprise tierce intermédiaire de services, etc), **la loi sur le CMR[218] prévoit que le troisième exemplaire des lettres de voiture (le second exemplaire en ce qui concerne les lettres de voiture pour déménagements) doive être conservé par l'entreprise, au moins pendant les 5 ans[219] qui suivent la date du transport et qu'il soit classé par ordre chronologique, d'une manière permettant un contrôle aisé par les agents chargés du contrôle.** Ceci oblige donc les responsables des traitements de données à caractère personnel à prendre en compte les dispositions de la loi « vie privée » pendant toute la durée de cette conservation et de **s'assurer à la fin de cette obligation que toutes ces données soit effacées ou tout du moins « anonymisées »** (si l'entreprise devait conserver ces données pour des besoins de statistiques historiques internes, par exemple).

Selon la loi sur le CMR, **ces exemplaires peuvent être conservés sur « *tout support d'information pour autant que la visualisation et l'impression de l'intégralité du document puissent être aisément opérées* »[220], ce qui implique que cet archivage puisse être sous format papier ou même électronique, pour autant que ces conditions soient respectées.**

En cas de sous-traitance technique de cette conservation (entreprises assurant l'archivage numérique, par exemple) **la loi « vie privée » impose aux responsables du traitement (ainsi qu'à ses sous-traitants** techniques également) **de mettre en place des mesures supplémentaires de « sécurité et de confidentialité des traitements »**[221], que ce soit tant au niveau technique (selon l'état de l'art en vigueur dans le secteur) qu'au niveau organisationnel (seules des personnes habilitées peuvent y accéder), **et d'assurer la « qualité des données »[222] tout au long de cette conservation** (exactes et, si possible, mises à jour[223]).

---

[218] Voir première partie de ce rapport.

[219] L'article 60 du Code TVA étend toutefois cette obligation à 7 ans (en vue de contrôles fiscaux).

[220] Cf. site http://www.mobilit.fgov.be/fr/route/goods/ .

[221] Cf. dispositions de l'article 16, §1er de la loi de 1992 (voir points ci-dessus).

[222] En effet, ce même article prévoit, à son §2, que :

« Le responsable du traitement ou, le cas échéant, son représentant en Belgique, doit :

*1° **faire toute diligence pour tenir les données à jour, pour rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes**, ainsi que celles obtenues ou traitées en méconnaissance des articles 4 à 8;*

*2° **veiller à ce que, pour les personnes agissant sous son autorité, l'accès aux données et les possibilités de traitement soient limités à ce dont ces personnes ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités du service**;*

*3° **informer les personnes agissant sous son autorité des dispositions de la présente loi et de ses arrêtés d'exécution**, ainsi que de toute prescription pertinente, relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel;*

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*** »[224] (souligné par l'auteur).

3) Autres dispositifs embarqués pouvant contenir des données à caractère personnel

a. Le module GPS :

Comme nous l'avons déjà mentionné, la Directive européenne 2002/58/CE[225] concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications[226] électroniques garantit cette protection pour ce qui est des réseaux publics de communications électroniques (que ce soient les réseaux mobiles numériques, internet, etc) de la Communauté. Si l'on se plaçait dans le secteur des communications électroniques « non publics » (par exemple, un réseau intranet à une entreprise), c'est alors la Directive 95/46/CE qui s'appliquerait. La première est toutefois intéressante à citer ici puisque la Directive 2002/58/CE vient définir certains concepts-clé, comme les données de trafic et/ou de localisation (voir partie précédente).

Etant donné que le projet eCMR va utiliser les réseaux publics GPRS/TCP (protocole internet) pour la transmission des données, ces deux dispositions législatives (transposées en Belgique par la loi de 1992 et par la loi de 2005, comme nous l'avons vu auparavant) s'appliquent.

Concernant les **données que le module GPS délivre, qui sont clairement des « *données de localisation* » des véhicules (et donc aussi des personnes/conducteurs qui les conduisent**, « personnes concernées » au sens de la Directive 95/46/CE et d'« utilisateurs » au sens de la Directive 2002/58/CE), on peut considérer que le module GPS du véhicule transmet la position géographique du véhicule, qui renvoie à un moment donné de travail du conducteur. Il s'agira donc d'une donnée à caractère personnel puisque le recoupement des différentes informations (avec la carte du conducteur présente sur le tachygraphe à l'heure GPS donnée, par exemple) nous donnera avec certitude le nom du ou des chauffeurs des véhicules concernés. On rentre ici dans le champ d'application de la législation « vie privée », dont le point précédent nous a démontré toutes ses implications juridiques concrètes.

Les responsables du traitement de ces données (normalement le gestionnaire du serveur à distance – le transporteur ou une entreprise tierce prestataire de services), devront donc remplir toute la série d'obligations imposées tant par la Directive 95/46/CE (s'ils évoluent dans le réseau routier européen, par exemple) que la loi belge de 1992 (pour les responsables

---

*4° **s'assurer de la conformité des programmes servant au traitement automatisé des données à caractère personnel avec les termes de la déclaration visée à l'article 17 ainsi que de la régularité de leur application**.* » (en gras et souligné par l'auteur).

[223] Cf. article 4, §1er, 4° de la loi de 1992.

[224] Voir point spécifique auparavant.

[225] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), *O L 201 du 31.7.2002, p. 37–47.*

[226] Cf. définition d'une « communication » à l'article 2, d) et le Considérant (15) de la Directive 2002/58/CE.

résidant en Belgique), ainsi que par la Directive 2002/58/CE transposée dans la loi belge du 13 juin 2005 relative aux communications électroniques[227].

b. Le PC embarqué :

Comme tout matériel informatique, celui-ci va disposer d'une adresse IP[228], qui est le numéro qui identifie chaque ordinateur connecté à Internet, ou plus généralement et précisément, l'interface avec le réseau de tout matériel informatique (routeur, serveur) connecté à un réseau informatique utilisant l'Internet Protocol. Selon l'Avis 1/2009229 du groupe d'experts européens en protection des données à caractère personnel, appelé aussi Groupe « Article 29 »[230], **une adresse IP est une considérée comme étant une donnée à caractère personnel,** ***« à moins que les fournisseurs de services «soient en mesure de préciser avec une certitude absolue que les données correspondent à des utilisateurs non identifiables »*** donc *« par mesure de sécurité, ils devront traiter toutes les informations IP comme des données à caractère personnel»*.

Concernant le projet eCMR, le PC embarqué est l'interface avec tous les équipements embarqués du véhicule afin de transmettre les données de ces équipements (GPS, tablette numérique du CMR, tachygraphe, interface CAN/FMS) via le Stepp III au serveur distant : il révèle donc aussi beaucoup de données de localisation via ces outils là, et donc là encore des données à caractère personnel.

Plusieurs traitements selon les dispositions de la loi « vie privée » sont déjà identifiés : la collecte des informations ; leur transmission ; éventuellement leur manipulation et/ou effacement, verrouillage, etc ; une certaine conservation (nécessaire pour des raisons techniques), etc. Il s'agira par la suite de voir pour quelles finalités ces traitements auront lieu et de suivre toutes les étapes prévues par la législation « vie privée » (telles que mentionnées plus haut).

c. Le terminal Stepp III

Le « Falcom Stepp III » est un **dispositif de repérage configurable à puce**, dont il est possible de l'adapter entièrement aux besoins des utilisateurs. Il peut également fonctionner de manière autonome (sans nécessité de PC embarqué) et est capable d'interagir directement avec un PC/serveur distant en utilisant les capteurs du véhicule.

Ce qui nous intéresse pour ce projet, c'est qu'il **ne permet pas le stockage des données** (ou en tout cas celui-ci n'est limité qu'à quelques bytes de façon temporaire) : il ne fait que générer et récolter les informations des autres dispositifs, et les transmettre au serveur distant. Cette **transmission des informations se fait à l'aide du protocole TCP supporté par la**

[227] Voir développements de ces obligations au début de notre deuxième partie ci-dessous.

[228] *Internet Protocol.*

[229] Avis 1/2009 concernant les propositions modifiant la directive 2002/58/CE sur la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques»), WP 159 adopté le 10 février 2009, Groupe « Article 29 » sur la Protection des Données.

[230] Le Groupe de Travail « Article 29 » sur la protection des données a été créé en vertu de l'article 29 de la Directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la Directive 95/46/CE et à l'article 15 de la Directive 2002/58/CE.

liaison GPRS entre le terminal Stepp III et le serveur de gestion de flotte : ce terminal transmet ainsi les informations de position, des données propres au camion et peut recevoir les commandes directement du serveur distant[231].

Là encore, cette transmission des données **génère une sorte d'identification propre à chaque terminal Stepp III** (appelée « socket TCP »[232]) ce qui permet de retracer un véhicule donné à un moment donné (et donc son conducteur, par le recoupement d'informations), nous rentrons donc dans le champ d'application de la loi belge « vie privée » de 1992 et de la Directive 95/46/CE. De plus, le Stepp III **effectue également des transmissions de « *données de trafic* »**, définies là encore par la Directive 2002/58/CE comme étant « *toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation* »[233].

Comme nous l'avons déjà dit, le terminal Stepp III a pour fonction de collecter différentes données provenant de plusieurs sources (tachygraphe, tablette du CMR, et autres équipements embarqués), et de les transmettre via GPRS/internet à un serveur (ou PC) distant, qui lui aura en place des logiciels qui aideront au recoupement des différentes informations afin de fournir un service de valeur ajouté aux transporteurs et autres clients éventuels. Ces données proviennent pour la plupart de dispositifs embarqués qui existent déjà à bord des véhicules et qui sont déjà encadrés par différentes lois (sur la sécurité routière, etc), mais toutes les données gérées par le SteppIII ne vont pas pouvoir être considérées comme étant des données à caractère personnel (comme par exemple les données provenant des capteurs d'humidité, etc) en tant que telles.

Tout peut être communiqué en temps réel via le Stepp III au serveur à distance, mais étant donné que la transmission d'un trop gros paquet de données pourrait entraîner des pertes, le partenaire CETIC[234] a décidé de couper les communications « en paquets » (fichiers fragmentés) pour assurer leur transmission. Dans ce type de schéma, **les conducteurs des véhicules sont « passifs » sur le système** : ils ne peuvent ni agir sur les fonctionnalités du Stepp III (outil pratiquement inviolable), ni le commander (les commandes se font à distance, par le serveur). Il n'y a que sur le PC embarqué (s'il y en a un) qu'ils pourraient avoir un certain pouvoir d'action, mais il faut savoir que les données transmises via le Stepp III peuvent l'être même sans l'intervention de ce PC (qui, pratiquement, ne va servir que d'interface de communication entre le transporteur et son chauffeur/conducteur).

Le serveur distant (qui pourra être géré tant par le transporteur, que par une entreprise tierce prestataire de services pour les transporteurs ou/et ses clients) va donc recouper les informations provenant de plusieurs dispositifs embarqués, ce qui va permettre d'autres traitements de données à caractère personnel (avec les finalités potentielles déjà mentionnées).

---

[231] Cf. Rapport technique du CETIC de juillet 2009, p. 5 et suivantes.

[232] Ibidem (p. 6) qui dit que : « *Lorsqu'un terminal se connecte au serveur de gestion de flotte, ce dernier crée un « socket TCP ». Il s'agit d'un canal de communication dédié à chaque terminal caractérisé par un certain nombre de paramètres : adresse et port source, adresse et port destination… Chaque « socket TCP » créé dispose d'un numéro identifiant pour l'associer au terminal correspondant* … ». Ce qui prouve bien qu'il y a des données identifiantes des terminaux qui font que le gestionnaire du serveur à distance va savoir à tout moment quel est le véhicule qui lui envoie des informations et l'associer à une personne identifiable facilement, le conducteur, par ailleurs.

[233] Cf. article 2, b) de la directive.

[234] *Ibidem.*

Pour conclure sur les différents systèmes examinés ci-dessus, on peut noter qu'on peut envisager plusieurs traitements de données à caractère personnel au sens de l'article 1er, §2 de la loi de 1992[235] puisque pratiquement tous les types de traitements prévus par la loi sont présents : en effet, dans le projet eCMR, on va tant **collecter** les données à caractère personnel émises par le tachygraphe, que celles provenant des différentes cartes énumérées ci-dessus via le tachygraphe, les données émanant de la tablette numérique du CMR (qui contient les coordonnées de l'entreprise transporteur, du client de la marchandise, éventuellement d'une entreprise tierce ; les coordonnées du chauffeur et celles de toute personne qui viendrait à signer le CMR dans le cadre de ses fonctions), **que les enregistrer, utiliser, communiquer, analyser,** etc.

Donc, comme on l'a souvent mentionné, **on rentre bien dans le champ d'application de la loi « vie privée » et l'on devra mettre en place toutes les conditions prévues par la loi, soit** :

- **désigner un (ou des) responsable(s) pour les différents traitements envisagés** s'il existe plusieurs finalités et qu'elles ne sont pas compatibles entre elles,
- effectuer une **déclaration préalable à la CPVP**,
- **informer correctement toutes les personnes concernées** (travailleurs, clients, partenaires commerciaux, etc),
- **mettre en place des mesures effectives de sécurité et de confidentialité des données** (tant au niveau technique qu'organisationnel),
- **mettre en place des outils pour assurer le respect des droits des personnes concernées** (droit d'accès, de rectification, d'opposition, etc), et ainsi de suite.

[235] Cette définition est également contenue à l'article 2, b) de la Directive européenne 95/46/CE précitée.

II/ Les principaux textes juridiques concernant la protection de la vie privée dans la relation d'emploi:

Au-delà des données nécessaires à assurer le bon déroulement du service de transport de marchandises, ainsi que le respect d'un certain nombre de législations spécifiques au secteur du transport routier, **les données à caractère personnel qui vont être traitées dans le cadre du projet eCMR pourraient poser problème car elles pourraient être aussi collectées et traitées pour une finalité plus problématique : celle de la « surveillance et du contrôle des travailleurs »**.

On va donc voir dans cette partie quels sont les textes législatifs à respecter quand des relations de travail existent, que ce soit au niveau belge **(C)** (pour les transports à l'intérieur des frontières nationales) qu'européen **(B)** et international **(A)** (puisque la grande majorité des transports de marchandises pourront avoir lieu transfrontières), ainsi que les implications juridiques (obligations des uns, droits et devoirs des autres, responsabilités, etc) dans le cadre du projet eCMR. Dans un dernier point, nous aborderons également l'avis émis par le Contrôleur Européen pour la Protection des Données (CEPD) concernant la future directive dans le secteur des « transports intelligents » **(D)**.

A. Les textes juridiques applicables au niveau international pour le respect de la « vie privée » dans les relations d'emploi

1) La Recommandation n° R (89) 2 du Conseil de l'Europe sur la protection des données à caractère personnel utilisées à des fins d'emploi[236]

Cette Recommandation **vise les Etats membres du Conseil de l'Europe**[237], qui s'engagent à *« s'assurer que les principes [qui y sont] contenus soient reflétés dans la mise en œuvre des législations nationales relatives à la protection des données dans le secteur de l'emploi (…) »*.

Les principes dégagés par ce texte **s'appliquent à la collecte et à l'utilisation de données à caractère personnel à des fins d'emploi dans les secteurs public et privé**, tant aux données traitées automatiquement qu'aux *« autres informations sur les employés détenues par les employeurs dans la mesure où ces informations sont nécessaires pour rendre intelligibles les données traitées automatiquement »*[238].

Cette Recommandation présente **plusieurs intérêts** en ce qui nous concerne :

---

[236] Recommandation n° R (89) 2 du Comité des Ministres aux Etats Membres sur la protection des données à caractère personnel utilisées à des fins d'emploi, adoptée par le Comité des Ministres le 18 janvier 1989 lors de la 423e réunion des Délégués des Ministres, Conseil de l'Europe, 1989.

[237] Créé le 5 mai 1949, le Conseil de l'Europe a une dimension paneuropéenne et a pour objectif *« de favoriser en Europe un espace démocratique et juridique commun, organisé autour de la Convention européenne des droits de l'homme et d'autres textes de référence sur la protection de l'individu »*. Actuellement, il comporte 47 pays membres, dont la Belgique.

[238] La Recommandation laisse le champ libre à chaque Etat membre *« d'étendre les principes énoncés à tous les traitements manuels »*. Ainsi, l'Etat Irlandais s'est réservé la possibilité de limiter le champ d'application de cette recommandation uniquement aux données automatisées, par exemple.

- tout d'abord, elle **définit l'expression « *à des fins d'emploi* »** comme : *« les rapports entre employés et employeurs relatifs au recrutement des employés, à l'exécution du contrat de travail, à la gestion, y compris les obligations découlant de la loi ou de conventions collectives, ainsi que la planification et l'organisation du travail »*.

En effet, dans le projet qui nous concerne, les données qui seront collectées par le kit de transmission seront nécessaires tant à l'exécution du contrat de travail des chauffeurs routiers avec leur employeur, qu'à l'exécution des dispositions contractuelles des transporteurs et/ou entreprises intermédiaires avec leurs clients. Ces données pourront également concerner la planification et l'organisation du travail des conducteurs, puisque la lettre de voiture permet de savoir à quel moment est effectué le chargement, le déchargement de la marchandise, etc, et ainsi permettre à l'employeur des chauffeurs d'organiser la répartition des camions et/ou des marchandises selon les résultats obtenus.

- ensuite, la recommandation du Conseil de l'Europe, par analogie avec la notion de « *personne concernée* » de la Convention 108[239], **introduit le principe du respect de la vie privée et de la dignité humaine des « employés »**, qui *« devrait être préservé lors de la collecte et de l'utilisation de données à caractère personnel à des fins d'emploi »*.

En effet, malgré que l'on se retrouve dans un **domaine à la frontière entre le droit du travail et le droit général**, le premier consacrant le **« *lien de subordination* » comme la principale caractéristique de la relation d'emploi** (en ce sens que l'employé/travailleur est subordonné à l'autorité de son employeur et de ce fait doit obéir à ses ordres sur le lieu de travail), cette **Recommandation va atténuer ce lien car il consacre *« la possibilité [d'avoir] des relations sociales et individuelles sur le lieu de travail »*.** L'existence de cette possibilité est indispensable pour comprendre qu'au-delà de la relation de travail, subordonnée par nature, **le travailleur aura aussi un droit au respect de sa vie privée** et que, en tant que tel, il pourra refuser de donner des informations personnelles le concernant à son employeur et/ou tout du moins limiter son pouvoir d'ingérence et d'action dans sa vie privée.

- Cette Recommandation, de nouveau par analogie avec la Convention 108, **consacre également le droit d'information et de consultation des employés *« préalablement à l'introduction ou à la modification de systèmes automatisés pour la collecte et l'utilisation de données à caractère personnel concernant les employés »***, tout en **laissant le soin aux législations et aux conventions collectives nationales de régler cet aspect au niveau national**.

En ce qui concerne le projet eCMR, ce droit va s'appliquer également *« à l'introduction ou à la modification de procédés techniques destinés à contrôler les mouvements[240] ou la productivité des employés »*, dont l'accord des employés ***« devrait être recherché avant [leur] introduction »*, si la procédure de consultation venait à révéler une possibilité d'atteinte au droit au respect de la vie privée et de la dignité humaine des employés**, *« à moins que d'autres garanties appropriées ne soient prévues par la législation ou la pratique nationales »*.

- La Recommandation R (89)2 **réitère également les principes suivants**:

[239] Cf. Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 (dite « Convention 108 »), citée ci-dessus.

[240] Ce que les méthodes classiques de « géolocalisation » par GPRS permettent de faire.

- **information de l'employé** si les données à caractère personnel viennent de sources en dehors des rapports de travail ;
- les **données collectées doivent être pertinentes et non excessives, nécessaires** (par ex., lors d'une procédure de recrutement) ;
- **l'enregistrement des données n'est possible que s'il est réalisé à des fins d'emploi** ;
- et les **données devront être exactes, mises à jour si nécessaire, et *« reproduire fidèlement la situation de l'employé »***.

Selon les termes employés **on exclut donc toute possibilité ultérieure de « profilage »[241] de l'employé par tel ou tel procédé d'encodage et d'enregistrement des données**. **De plus, si les données sont *« appréciatives relatives à la productivité ou à la potentialité des employés »* elles devront être fondées sur des *« évaluations équitables et loyales »*.** On devra donc tenir compte de la façon dont ces données vont être enregistrées par les outils technologiques utilisés, afin de voir si leur collecte permet une évaluation ultérieure de la façon de travailler du chauffeur routier, par exemple.

- Ce texte **réaffirme le principe de finalité** de la collecte des données à caractère personnel, **qui ne pourra être réalisé qu'*« à des fins d'emploi »* exclusivement**, afin d'éviter toute utilisation ultérieure des mêmes données à des fins différentes et non compatibles avec le traitement initial.

Néanmoins, si cela devait se produire, il **réaffirme le besoin de prendre *« des mesures appropriées pour éviter que ces données ne soient mal interprétées dans un contexte différent et pour assurer qu'elles ne soient pas utilisées de manière incompatible avec le but initial »*, surtout en cas de *« mise en relation de fichiers »***[242].

En ce qui concerne le **délai de conservation** des données, là encore par analogie avec la Convention 108, on se réfère à la **notion de *« période raisonnable »***[243].

Récemment[244], un conseiller juridique de la **Commission pour la protection de la vie privée belge** a fait mention de la « jurisprudence/doctrine » de la CPVP (avis rendus par la CPVP) en la matière et qui est **d'admettre des délais de conservation des données différents selon les finalités poursuivies par ces traitements[245] et selon des niveaux de risques différents**.

---

[241] Voir à ce sujet la récente Recommandation adoptée par le Conseil de l'Europe en la matière : « *Draft recommendation on the protection of individuals with regard to automatic processing of personal data in the context of profiling* », Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data [ETS 108] (T-PD), Strasbourg, 3 juin 2010.

[242] Ce qui pourrait être le cas lors de l'enregistrement des données du CMR : de la simple vérification de l'heure de déchargement de la marchandise on pourrait, par exemple, utiliser cette information afin de mesurer la rapidité du travailleur en question sur une période donnée, afin de mesurer son rendement en comparaison avec d'autres travailleurs pour le même type de travail.

[243] Cf. article 5 de la Convention sur la « qualité des données ».

[244] Lors d'un colloque JURITIC du 25 juin 2010, organisé par le CRID/FUNDP sur le « Profilage électronique et protection de la vie privée » (www.juritic.be/).

[245] Par ailleurs, la CNIL (autorité française) admet des délais de conservation de données de (géo)localisation à des fins de gestion des salariés assez courts (2 mois) et pour les usages professionnels c'est admis jusqu'à 3 mois, ensuite le responsable du traitement doit s'assurer de leur « anonymisation » (*ibidem*).

- **En cas de communication externe des données**, on recommande que celle-ci n'ait lieu **que pour *« les besoins des fonctions officielles des organismes publics »*** [246] **et *« dans les limites des obligations légales de l'employeur*** *ou conformément à d'autres dispositions du droit interne »*.

Ceci limitera fortement la possibilité de communiquer ces données à des personnes privées, non qualifiées pour les obtenir, comme d'éventuels tiers à la relation d'emploi (ainsi on ne pourrait pas communiquer des informations concernant le respect de la législation des temps de travail par un chauffeur donné à un client tiers non qualifié pour les obtenir, par exemple).

- Quant aux **données sensibles**[247], elles ne peuvent être **collectées que *« dans des cas particuliers, dans les limites prévues par le droit interne et conformément aux garanties appropriées y figurant »*, sinon *« le consentement exprès et éclairé des employés »* est requis.**
- Enfin, même si l'on se trouve dans une relation de travail, subordonnée, où en principe l'employeur se retrouve dans une position hiérarchique par rapport à ses employés, cette recommandation dispose que **l'employeur se doit de respecter le principe de mise à disposition des informations sur les données à caractère personnel détenues par lui, afin que l'employé puisse faire valoir ses droits sur ses données personnelles** (accès, rectification, contestation, effacement, etc)[248].

2) Le 'Projet de Recueil de directives pratiques sur la protection des données personnelles des travailleurs' de l'OIT[249]

Il s'agit de la **première initiative internationale** destinée à *« fournir des orientations sur la protection des données personnelles des travailleurs »*, **adoptée le 7 octobre 1996** par un

[246] Ceci pourrait être le cas, par exemple, du devoir de communication de certaines données de localisation des employés aux services douaniers et/ou de police, dans le cadre de leurs missions de contrôle et de surveillance des infractions (au code de la route, aux règles d'hygiène et de sécurité des marchandises transportées, etc).

[247] Par données « sensibles » ou « catégories particulières de données » on entend les *« données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, les données relatives à la vie sexuelle ou à des condamnations pénales, visées à l'article 6 de la Convention [108] (…) »*. Cf. point 10.1. de la Recommandation R (89) 2 (ainsi que les dispositions de la Directive 95/46/CE citées plus haut).

[248] Cf. aussi l'article 8 de la Convention 108 où :

*« **Toute personne doit pouvoir:***

***a. connaître l'existence d'un fichier automatisé de données à caractère personnel, ses finalités principales, ainsi que l'identité et la résidence habituelle ou le principal établissement du maître du fichier**;*

b. obtenir à des intervalles raisonnables et sans délais ou frais excessifs la confirmation de l'existence ou non dans le fichier automatisé, de données à caractère personnel la concernant ainsi que la communication de ces données sous une forme intelligible;

c. obtenir, le cas échéant, la rectification de ces données ou leur effacement lorsqu'elles ont été traitées en violation des dispositions du droit interne donnant effet aux principes de base énoncés dans les articles 5 et 6 de la présente Convention;

*d. **disposer d'un recours** s'il n'est pas donné suite à une demande de confirmation ou, le cas échéant, de communication, de rectification ou d'effacement, visée aux paragraphes b et c du présent article. »*. (souligné par l'auteur).

[249] Projet de Recueil de directives pratiques sur la protection des données personnelles des travailleurs, Bureau international du Travail, Organisation internationale du Travail (OIT), Genève, 1995.

groupe de 24 experts indépendants originaires de 20 pays membres de l'Organisation Internationale du Travail (OIT).

Les directives proposées n'ont **pas un caractère contraignant**, mais ce Recueil est supposé être pris en compte par les pays membres de l'OIT dans leur *« élaboration de lois, règlements, conventions collectives, codes du travail, lignes directrices et dispositions concrètes concernant la collecte, le stockage, la diffusion et le contrôle des données concernant les travailleurs »*.

Selon les principes généraux dégagés par ces experts, le projet de recueil stipule que ***« le traitement des données personnelles des travailleurs devrait se limiter à des fins touchant directement la relation d'emploi »*** **et réaffirme le principe de finalité** (tel qu'il a été exprimé par la Convention 108 et la Recommandation R (89) 2 du Conseil de l'Europe).

De plus, ils soulignent le fait que **toute personne *« ayant accès aux données personnelles des travailleurs devrait être tenue à une obligation de confidentialité »*** et rappellent les **droits dont bénéficient les travailleurs** en tant que 'personne concernée', **ainsi que l'interdiction de collecte des données personnelles dites sensibles**, sauf si *« ces données concernent directement la relation d'emploi et si la législation nationale les y autorise »* (gras et souligné par l'auteur).

De même, ils rappellent la **nécessité d'obtenir l'autorisation écrite des travailleurs en cas de communication des données personnelles à des tiers, sauf cas restrictifs, et d'une information correcte des travailleurs par leurs employeurs avant que tout traitement ne soit mis en place**.

On peut donc conclure que tant au niveau international, que paneuropéen, les principes liés au respect de la vie privée des travailleurs sont directement liés à ceux des individus 'personnes concernées', tels que prévus dans les règlementations citées ci-après.

B. Les textes juridiques applicables au niveau communautaire

On ne fera que renvoyer au ***point I*** de la deuxième partie de ce rapport, concernant la Directive 95/46/CE et la Directive 2002/58/CE : toutes les dispositions citées s'appliquent aussi dans ce cas-ci, même si les finalités du traitement à caractère personnel sont différentes, étant donné que ces directives ont une portée générale en matière de respect de la vie privée.

1) La Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

Cette Directive impose donc le **respect de quelques principes-clés[250] en droit européen**, qui vont se retrouver dans la plupart des législations nationales des Etats membres, et qui sont (bref rappel car partie envisagée plus haut) :

- **Principe de légalité** du traitement de données (collecte loyale et licite).
- **Principe de finalité** (les données doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement et de manière incompatible avec ces finalités).

[250] Cf. article 6 et suivants de la Directive.

- **Principe de proportionnalité et de nécessité** (données adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées ; exactes et, si nécessaire, mises à jour ; et conservées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités).
- **Principe de légitimité des traitements** de données (la personne concernée doit avoir donné « indubitablement » son consentement, ou le traitement est nécessaire à l'exécution d'un contrat ou de mesures précontractuelles, ou il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis, etc[251]).
- **Devoir de confidentialité et de sécurité des traitements par le 'responsable du traitement', qui doit mettre en œuvre des *« mesures techniques et organisationnelles appropriées »***[252] (il doit également s'assurer que tous ses éventuels sous-traitants[253] respectent bien cela sous son autorité et sur instruction seulement[254]).
- Et **principe de transparence**, c'est-à-dire :
    - **devoir d'information de la personne concernée** (droits de la personne concernée : accès, opposition, rectification, …) ;
    - et **obligation de notification à l'autorité de contrôle indépendante**[255].

Comme on l'a vu précédemment, **les seuls instruments internationaux concernant la protection des données à caractère personnel des travailleurs ont repris ces principes pour les adapter à la relation d'emploi**, et ainsi **l'employeur s'est vu reconnaître la qualité de « responsable du traitement »**[256] au sens de la Directive 95/46/CE.

C. Le cadre légal belge en matière de respect de la vie privée dans les relations d'emploi

Les principes de la loi « vie privée » belge ont été déjà expliqués plus haut, donc nous nous contentons de la citer pour rappel.

1) La Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel

La loi du 8 décembre 1992 (ou « loi vie privée») **définit les droits et devoirs de la personne concernée ainsi que les obligations du responsable du traitement**, elle **crée un organe de contrôle indépendant** (la Commission de la protection de la vie privée – ou **CPVP**[257]), et **reprend les principes fondamentaux des Directives européennes (légalité, finalité, proportionnalité, transparence, confidentialité et sécurité**, etc).

[251] Voir toutes les conditions de légitimité prévues à l'article 7 de la Directive95/46/CE.

[252] Cf. articles 16 et 17 de la Directive 95/46/CE.

[253] Au sens de l'article 2, e) de la Directive 95/46/CE.

[254] En vertu des articles 16 et 17 de la Directive également.

[255] Cf. article 18 de la Directive : chaque Etat membre a donc instauré une autorité de contrôle au niveau de la protection des données.

[256] Voir définition de l'article 2, d) de la Directive 95/46/CE.

[257] Site sur : *http://www.privacycommission.be/fr/*

2) Autres textes juridiques belges pertinents en matière de protection de la vie privée des travailleurs:

Outre la loi « vie privée » de 1992, en ce qui concerne le contrôle et la surveillance des travailleurs, il existe deux conventions collectives de travail, élaborées sous l'égide du Conseil National du Travail[258], qui règlementent les relations d'emploi en Belgique (et qui ont été rendues obligatoires par arrêté royal), et qui sont :

a. La Convention collective de travail n° 68[259]

Il s'agit, d'une part, de la **Convention collective de travail n° 68 du 16 juin 1998 relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu de travail** (ci-après CCT n°68), qui rappelle les dispositions en matière de respect de la vie privée internationales et européennes (cf. Convention 108, Recommandation n° R(89)2, Directive 95/46/CE et Recueil de directives pratiques sur la protection des données personnelles des travailleurs de l'OIT, citées ci-dessus) ainsi que le « ***droit au respect de la vie privée inscrit explicitement dans l'article 22 de la Constitution Belge*** ».

Cette Convention rappelle en outre un certain nombre de principes régissant le droit du travail, dont l'article 16, al. 1er de la loi du 3 juillet 1978[260], qui stipule que « *l'employeur et le travailleur se doivent le respect et des égards mutuels* ». C'est dans ce cadre-ci que s'inscrit la rédaction de la CCT n°68 puisque **les partenaires sociaux ont estimé que, étant donné les répercussions sur la vie privée du travailleur que la surveillance par caméras sur le lieu de travail peut avoir, « *il fallait arrêter les conditions d'admissibilité et d'installation* » de cette surveillance pour offrir des garanties suffisantes en matière de respect de la vie privée des travailleurs**.

Cette Convention **définit également ce qu'il faut entendre par surveillance par caméras sur le lieu de travail, dans quelles conditions cette surveillance est autorisée et quelles prescriptions il y a lieu de respecter en la matière,** en confirmant et **en concrétisant les principes de la loi « vie privée »** (citée ci-dessus) dont notamment : le **principe de finalité**, le **principe de proportionnalité** et **l'obligation d'information préalable par rapport au lieu de travail**, que les données à caractère personnel (images comprenant des données personnelles identifiables) résultant de la surveillance par caméras soient conservées ou non.

Ainsi, la CCT n°68 donne une **définition de 'surveillance par caméras'** comme étant « *tout système de surveillance comportant une ou plusieurs caméras et* ***visant à surveiller certains endroits ou certaines activités sur le lieu de travail à partir d'un point qui s'en trouve géographiquement éloigné*** *dans le* ***but ou non de conserver les images dont il assure la collecte et la transmission*** » (art. 2 de la CCT). Par analogie, on peut assimiler à cette surveillance celle effectuée par tous les dispositifs embarqués dans les véhicules dans le secteur du transport routier, utilisant parfois par ailleurs ces dispositifs en les combinant avec

[258] En effet, en droit du travail belge, les organisations de travailleurs et d'employeurs représentées au Conseil national du Travail peuvent décider de conclure une convention collective de travail afin de régler telle ou telle matière par la voie conventionnelle.

[259] Convention collective de travail n° 68 du 16 juin 1998 relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu de travail (ratifiée par l'AR du 20 septembre 1998, paru au MB du 2 octobre 1998).

[260] Cf. loi du 3 juillet 1978 relative aux contrats de travail (*M.B. du 22/08/1978*).

une caméra de surveillance (installée dans le cockpit du conducteur et/ou à l'intérieur de la remorque, surtout dans les transports de matières dangereuses ou à grande valeur). On est donc ici dans un **cas de « télésurveillance » des travailleurs**.

Afin que cette surveillance puisse être admise, les articles 4 à 11 de la **CCT n°68** fixent un **certain nombre de conditions**, dont :

- le **principe de finalité** (art. 4 de la CCT), qui doit être défini « ***clairement et explicitement par l'employeur*** ». De plus, **la surveillance n'est autorisée que lorsque l'une des finalités (limitatives) suivantes est poursuivie**, soit :

1° la **sécurité et la santé** (des travailleurs et/ou sur le lieu de travail[261]) ;

2° la **protection des biens de l'entreprise** ;

3° le **contrôle du processus de production** (qui peut **porter tant sur les machines que sur les travailleurs**, mais pour ces derniers celui-ci ne peut avoir pour but que « *l'évaluation et l'amélioration de l'organisation du travail* ») ;

Pour ces trois premières finalités la surveillance par caméras peut être **permanente ou temporaire** (toutefois, dans le cas du contrôle du processus de production, **la surveillance permanente ne peut porter que sur les machines**)[262].

4° le **contrôle du travail du travailleur** (mais « *la poursuite de cette finalité ne peut avoir pour conséquence que les décisions et évaluations de l'employeur se fondent exclusivement sur les données collectées par voie de surveillance par caméras* »[263] et sous réserve des dispositions de l'art. 9, §2 de la CCT[264]).

Or, **ce contrôle ne doit pas avoir pour but de filmer en permanence le travailleur** : donc, sur le lieu de travail, en principe, la surveillance par caméras ne peut être que temporaire (ainsi que pour le contrôle du processus de production qui porte sur les travailleurs).

Par ailleurs, les commentaires sous les articles de la CCT spécifient que l'on puisse utiliser des caméras à des fins de formation (s'il ne s'agit pas de surveillance) et qu'en cas de « *surveillance secrète par caméras* » les dispositions du Code pénal et du Code de procédure pénale s'appliquent[265]. Et **une surveillance par caméras permanente sur les lieux de travail n'est autorisée que « *dans la mesure où le but n'est pas de viser le travailleur* »**.

---

[261] Respect des législations en vigueur dans ces matières (voir parties précédentes pour le secteur routier).

[262] Cf. article 6 de la CCT n°68.

[263] Ce qui implique que l'employeur doive justifier éventuellement une décision de renvoi d'un travailleur par d'autres éléments que ceux rapportés par les caméras (ex. : en cas de vol, la preuve par l'image doit être complétée par la constatation du vol lui-même par un agent de la police).

[264] Qui dispose que : « *Lorsque la surveillance par caméras a pour* ***objet le contrôle des prestations de travail, et plus particulièrement le mesurage et le contrôle en vue de déterminer la rémunération ou a des implications sur les droits et obligations du personnel*** *de surveillance,* ***l'employeur fournit cette information*** *dans le cadre de la procédure fixée à l'article 11 et suivants de la loi du 8 avril 1965 instituant les règlements de travail.* », c'est-à-dire que « ***le travailleur peut prendre connaissance en permanence et sans intermédiaire*** *– sans préjudice du droit à l'assistance de son délégué syndical –* ***du règlement de travail et de ses modifications*** », dont l'employeur doit lui remettre une copie (cf. commentaires sous art. 9).

[265] En effet, en principe, la preuve obtenue par des « moyens illégaux » n'était pas admise par les tribunaux, toutefois un arrêt récent, dit arrêt « *Antigoon* » (cf. Cour de Cassation, 14 octobre 2003), a admis la « preuve illégale » étant donné le caractère sérieux de l'abus à dénoncer. Voir à ce propos l'article de : LEONARD T. et

- le **principe de proportionnalité** (art. 7 de la CCT) : en effet, selon les dispositions de cet article, un « *employeur ne peut utiliser la surveillance par caméras d'une manière incompatible avec la **finalité expressément décrite*** » et cette surveillance « *doit être **adéquate, pertinente et non excessive** au regard de cette finalité* » (donc renvoi exprès aux dispositions de la loi « vie privée »).

Ainsi, si la surveillance par caméras devait entrainer une « *ingérence dans la vie privée du travailleur* », l'article 8, §2 de la CCT dispose que « *cette ingérence **doit être réduite à un minimum*** » et qu'il y a lieu de respecter les suivantes procédures : **la procédure de consultation** (s'il apparait que la surveillance puisse avoir des implications sur la vie privée des travailleurs le conseil d'entreprise, ou à défaut le comité pour la prévention et la protection au travail, doit examiner les mesures qu'il y a lieu de prendre pour réduire cette ingérence au minimum ; ou cela doit se faire par un **commun accord entre l'employeur et la délégation syndicale**[266]**) et l'évaluation régulière des systèmes de surveillance utilisés** (par le conseil d'entreprise ou le comité pour la prévention et la protection au travail, afin de faire des propositions en vue de revoir ces systèmes en fonction des développements technologiques qui peuvent proposer des systèmes moins intrusifs)[267].

Par ailleurs, la CCT met en place également **d'autres conditions de procédure afin d'accroitre la transparence dans cette matière et de permettre un « dialogue » entre les différentes parties** (art. 9 et suiv.), dont :

- **l'obligation d'information préalable du conseil d'entreprise** (ou, à défaut, du comité pour la prévention et la protection au travail, ou de la délégation syndicale, ou encore des travailleurs) « *sur tous les aspects de la surveillance par caméras* » ;
- et **l'obligation d'information des travailleurs « *sur tous les aspects de la surveillance par caméras* »** sur : la finalité poursuivie ; le fait que des images soient ou non conservées ; le nombre et l'emplacement de la ou des caméras ; et la ou les périodes concernées pendant lesquelles la ou les caméras fonctionnent.

En outre, selon l'article 13 de la CCT, l'employeur doit *« **traiter les images collectées de bonne foi et en conformité avec la finalité décrite*** » ainsi que s'assurer de la « *compatibilité »* de tout usage ultérieur avec la finalité initiale « *et prendre toutes les mesures pour éviter, vu le contexte, les erreurs d'interprétation* ».

Enfin, la CCT n°68 **rappelle les droits des travailleurs en tant que « personnes concernées » au sens de la loi « vie privée** » (cf. art. 10, 12 et 13 de cette loi) et que le fait que pour exercer ces droits « *ils ont le droit de se faire assister par leur délégué syndical* »[268] (selon les règles en vigueur en droit du travail).

ROSIER K., *La jurisprudence « Antigoon » face à la protection des données : salvatrice ou dangereuse ?*, Editorial de la RDTI., qui constate que : « *L'arrêt « Antigoon » marque en effet un tournant décisif dans la jurisprudence de la Cour en ce qu'il consacre l'autorisation de principe d'avoir égard à des preuves recueillies illicitement sauf exceptions définies par la Cour : lorsque le respect de certaines conditions de forme est légalement prescrit à peine de nullité ; lorsque l'irrégularité commise entache la crédibilité de la preuve ; lorsque l'usage de cette preuve est contraire au droit à un procès équitable.* ». Toutefois cette jurisprudence est fortement contestée tant par la doctrine que par d'autres arrêts des juridictions civiles et du travail (voir références dans article précité).

[266] Cf. article 10 de la CCT n°68.

[267] Cf. art. 11 de la CCT.

[268] Cf. art. 14 de la CCT n°68.

b. La Convention Collective de Travail n°81[269]

D'autre part, **la Convention Collective de Travail n°81 du 26 avril 2002 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau** (ci-après CCT n°81) **a réitéré les principes énoncés par la CCT n°68**.

Cette CCT est également intervenue pour s'assurer le respect de la législation « vie privée » car les *« **modes de contrôle souvent inhérents à la gestion même du système informatique se sont développés** afin par exemple d'assurer le bon fonctionnement du réseau (…) [or] le contrôle de données de communication électroniques transmises ou reçues par un travailleur et transitant par le réseau de l'entreprise, est potentiellement ouvert à l'employeur* ». On retrouve là encore, par analogie, le cas qui nous concerne dans le projet eCMR, puisque toutes les communications électroniques effectuées par les conducteurs, dont la plupart via le SteppIII (donc sans qu'aucun contrôle direct ne puisse être effectué par le travailleur), vont être « scannées » et analysées par le logiciel du serveur distant, géré soit par leur employeur, soit par son sous-traitant technique (comme une entreprise intermédiaire de services, par ex.), et entrainer des conséquences pour le respect de leur vie privée sur leur « lieu de travail » (le véhicule, dans ce cas-ci).

Là encore, la CCT n°81 réaffirme le principe selon lequel lorsque ce contrôle porte sur des données à caractère personnel il « *doit pouvoir être concilié avec les normes fondamentales qui garantissent le droit de toute personne au respect de sa vie privée* ». Les partenaires sociaux ont donc décidé d'intervenir encore une fois via **l'adoption d'une convention de travail afin de « *préciser ces normes fondamentales de manière à s'assurer de leur applicabilité effective dans l'entreprise* »**[270].

Toutefois, soulignons que cette CCT **n'intervient que pour garantir le droit à la vie privée du travailleur « *lorsque sur le lieu de son travail, des données de communication électroniques sont collectées dans le but de les contrôler et dans ce cadre d'en assurer le traitement de manière à les attribuer à un travailleur* »**[271]. En effet, elle ne réglemente ni l'accès, ni l'utilisation par le travailleur des moyens de communication électroniques en réseau au sein de l'entreprise[272] (comme l'accès à l'internet, l'utilisation du courriel pour des besoins professionnels ou privés, etc) car « *la fixation de ces règles d'accès et/ou d'utilisation est liée aux prérogatives de l'employeur* ».

Malgré les dispositions générales de cette CCT, dans le sens où elle s'applique à des relations d'emploi quel que soit le secteur d'activité visé, la CCT n° 81 précise que « ***ces normes***

---

[269] Convention collective de travail n° 81 du 26 avril 2002 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau (ratifiée par l'AR du 21 juin 2002, paru au MB du 29 juin 2002).

[270] Cf. introduction à la CCT n°81. Un rappel des normes internationales et européennes (Recueil de directives pratiques de l'OIT ; art. 8 de la CEDH ; Directive 95/46/CE) a été également réalisé, ainsi qu'un rappel et la réaffirmation de l'adhésion de cette CCT au cadre légal belge en matière de vie privée (art. 22 de la Constitution ; loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques dont l'article 109ter D vise la protection du secret des télécommunications ; et surtout loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel) (voir partie précédente).

[271] Et **que des données personnelles identifiables soient conservées** (cf. préambule de la CCT n°81).

[272] Cf. article 1er, §2 de la CCT n°81.

pourront, en tant qu'elles constituent un dispositif de base, être précisées, complétées et/ou modalisées au niveau du secteur et/ou de l'entreprise en fonction de leurs spécificités »[273] (souligné par l'auteur). Elle constitue par ailleurs un « engagement » pour toutes les parties prenantes à la relation de travail à ce que :

- d'une part, les travailleurs « *reconnaissent le principe selon lequel* ***l'employeur dispose d'un droit de contrôle sur l'outil de travail et sur l'utilisation de cet outil par le travailleur dans le cadre de l'exécution de ses obligations contractuelles****, y compris lorsque cette utilisation relève de la sphère privée, compte tenu des modalités d'application prévues par la convention* » ;
- et de l'autre, les employeurs « ***respectent le droit des travailleurs à la protection de leur vie privée dans le cadre de la relation de travail*** *et des droits et obligations que celle-ci implique pour chacune des parties.* » (cf. article 3 de la CCT) (souligné par l'auteur).

Cette convention définit également à son article 2 ce qu'elle entend par '*données de communication électroniques en réseau*' et qui sont : « *les données relatives aux communications électroniques transitant par réseau,* ***entendues au sens large*** *et indépendamment du support par lequel elles sont transmises ou reçues par un travailleur dans le cadre de la relation de travail* » (elle entend ainsi définir un cadre suffisamment large **pour englober l'ensemble des technologies en réseau tant interne qu'externe, et ce indépendamment du support auquel elles recourent**[274]). Peuvent ainsi être visés les ordinateurs, les GSM, tous les dispositifs permettant des communications électroniques (comme le SteppIII de Falcom dans le projet eCMR), etc.

Puis la CCT n°81 **impose également le respect** (cf. art. 4 de la CCT) :

- **du principe de finalité** (art. 5) : c'est-à-dire que l'employeur ne peut exercer un contrôle des données de communication électroniques en réseau, via une procédure directe ou indirecte (caractère déterminé en fonction de la finalité poursuivie), que s'il poursuit **certaines finalités limitées (énumérées exhaustivement par l'article 5 de la CCT)**[275], dont :

1° la prévention des faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui (comme par ex. le piratage informatique ou bien la consultation de sites incitant à la discrimination ou autres);

2° la **protection des intérêts économiques, commerciaux et financiers de l'entreprise auxquels est attaché un caractère de confidentialité** ainsi que la lutte contre les pratiques contraires[276] (comme par ex. la divulgation de fichiers et la violation de secrets d'affaires y compris la recherche et le développement);

---

[273] Ce qui est aussi la position « officieuse » de la CPVP belge (voir point suivant).

[274] Cf. commentaire sous article 2 de la CCT.

[275] Toutefois, **aucune distinction n'est opérée par cette CCT selon que le contrôle poursuivi ait ou non un caractère permanent**, étant donné qu'il est apparu que cette distinction risquait d'être artificielle étant donné que « *la fonction de contrôle est quasi indissociable des systèmes de réseau véhiculant des données de communication électroniques* » (cf. introduction de la CCT n°81).

[276] Qui pourrait être invoqué dans le cadre d'une surveillance des chauffeurs routiers lorsqu'ils sont responsables de la livraison de marchandises, par exemple.

3° la **sécurité et/ou le bon fonctionnement technique des systèmes informatiques en réseau de l'entreprise**, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'entreprise ;

Toutefois, il y a lieu de **respecter une phase dite de « sonnette d'alarme »** ici et qui *« vise essentiellement à informer les travailleurs d'une anomalie et les avertir d'une individualisation en cas de récurrence* ». En effet, si l'on attribuait à un travailleur une « *anomalie d'utilisation des moyens de communication* », **par application de la procédure d'individualisation, ce travailleur devrait être invité à un entretien préalablement à l'adoption de toute décision ou évaluation susceptible de l'affecter individuellement** (procédure à caractère contradictoire, dans le sens où ainsi le travailleur pourra s'expliquer lors de cet entretien sur l'utilisation « anormale » réalisée par lui, tout en se faisant assister par son délégué syndical s'il le souhaite).

D'autre part, lorsque l'objet et le contenu des données de communications électroniques en réseau ont un **caractère professionnel non contesté par le travailleur « *l'employeur pourra les consulter sans autre procédure* »** afin d'assurer le bon fonctionnement de l'entreprise[277]. Ce qui n'est pas le cas lorsque « *notamment par une mention en ce sens dans l'objet qui définira ainsi l'étendue du contrôle de l'employeur, la nature privée du contenu de ces données est invoquée* » : dans ce cas, la procédure d'individualisation joue pour les données dont il est question mais leur contenu ne pourra pas être consulté.

4° le **respect de la bonne foi des principes et règles d'utilisation des technologies en réseau fixés dans l'entreprise** (qui renvoie tant au règlement intérieur qu'à une quelconque « *privacy policy* » - politique interne concernant la vie privée – établie par l'entreprise).

En outre, l'employeur doit définir clairement et de manière explicite la ou les finalités d'un tel contrôle (art. 5, §2), tout en ayant la possibilité d'utiliser des contrôles à des fins de formation (s'il ne s'agit pas de surveillance). Toutefois, en cas de « *surveillance secrète des données de communication électroniques en réseau* » les dispositions du Code pénal et du Code de procédure pénale s'appliquent[278].

- **du principe de proportionnalité** : **le contrôle doit** donc **revêtir dans tous les cas un caractère « *adéquat, pertinent, et non excessif* » au regard de la ou des finalités poursuivies**, donc **il ne doit pas y avoir d'ingérence dans la vie privée du travailleur** (cf. art. 6 de la CTT), tout comme il est déjà prévu par la loi « vie privée » (voir plus haut). Si toutefois cela devait se produire « *cette ingérence doit être réduite à un minimum »* (art. 6, §2).
- **du principe de transparence** : la convention prévoit l'obligation de **mettre en place des procédures d'information et de consultation des travailleurs lors de**

[277] Ainsi, dans le projet eCMR, en principe le contenu des données de communication transmises au serveur distant ont un caractère strictement professionnel si la finalité du traitement est par exemple la gestion de la flotte des véhicules, la gestion de la marchandise et de la clientèle et/ou le contrôle des législations en vigueur dans le secteur routier (dont le transporteur est aussi responsable de son application).

[278] Voir commentaire sur l'arrêt « Antigoon » réalisé pour la CCT n°68. Toutefois, il y a lieu de préciser qu'en cas de suspicion d'abus et/ou d'actes illicites par les travailleurs, l'employeur n'a pas un pouvoir de « police » et doit en principe contacter les autorités judiciaires autorisées par la loi afin de mettre en œuvre de telles pratiques d'interception de communications (au regard du principe de respect de la confidentialité des communications électroniques, tel que définit dans la partie sur la loi « communications électroniques »).

l'installation du système de contrôle, dont un **système d'information collective**[279] (information du conseil d'entreprise ou, à défaut, du comité pour la prévention et la protection au travail ou, à défaut, de la délégation syndicale ou, à défaut, des travailleurs) **et individuelle « *sur tous les aspects du contrôle* »** (information du personnel via des panneaux d'information mais aussi via des courriers individuels ou des avenants au contrat de travail, par exemple[280], **ou même par mention sur écran de messages à l'allumage du poste de travail et/ou lors de l'activation de certains programmes**[281]) et cela « *quelle que soit la finalité poursuivie* ».

Ainsi, d'une part, **cette information individuelle et collective doit porter** :

- **sur la politique de contrôle (ainsi que les prérogatives de l'employeur et du personnel de surveillance)** ;
- sur la ou les **finalités poursuivies** ;
- sur le **fait que des données personnelles soient ou non conservées, le lieu et la durée de conservation**[282] ;
- et sur le **caractère permanent ou non du contrôle** (art. 9, §1er).

Alors que, d'autre part, **concernant l'information individuelle**, celle-ci **doit porter également sur** :

- l'**utilisation de l'outil mis à disposition des travailleurs pour l'exécution de leur travail** (en ce compris les limites à l'utilisation fonctionnelle) ;
- les **droits, devoirs, obligations des travailleurs et les interdictions éventuelles** prévues dans l'utilisation des moyens de communication électronique ;
- **et les sanctions prévues au règlement de travail en cas de manquement** (art. 9, §2).

Là encore, la CCT n°81 stipule qu'une **évaluation régulière des systèmes de contrôle** doit être réalisée (soit par le conseil d'entreprise, soit par le comité pour la prévention et la protection au travail, soit avec la délégation syndicale) de façon à ce que des moyens plus innovants soient proposés afin de « *mieux atteindre* ***l'objectif de non ingérence ou d'ingérence minimale dans la vie privée dans la vie privée des travailleurs*** » (cf. introduction et art. 10 de la CCT).

Ces trois mêmes principes doivent également être respectés au moment où les données de communication électroniques collectées en vue d'un contrôle sont traitées de manière à les attribuer à une personne identifiée ou identifiable, qui est une phase dite « *d'individualisation*

---

[279] « *Sur le plan collectif, l'accent est mis sur les* ***dispositions conventionnelles en vigueur en matière d'information des représentants des travailleurs****, en faisant explicitement référence aux procédures prévues par la convention collective de travail n° 9 du 9 mars 1972 coordonnant les accords nationaux et les conventions collectives de travail relatifs aux conseils d'entreprise.* » (cf. introduction et article 7 de la CCT).

[280] Via un support laissé au choix de l'employeur ***« pour autant que l'information fournie soit effective, compréhensible et mise à jour*** » (la qualité de l'information est donc essentielle afin d'assurer un consentement éclairé de la part du travailleur) (cf. art. 8 de la CCT).

[281] **Cette dernière façon de faire nous semble la plus propice à mettre en œuvre dans le cadre du projet eCMR : lorsque le travailleur allumerait le PC embarqué, par ex., un message pourrait s'afficher lui indiquant tous les dispositifs de contrôle des communications électroniques effectuées par le serveur distant.**

[282] On renvoie ici le lecteur aux dispositions de la loi « vie privée » étudiées dans la partie antérieure.

des données de communication électroniques »[283] (art. 11 de la CCT). Cependant, la CTT rappelle que **« *seules les données de communication électroniques pourront être individualisées* » et non leur contenu** (sauf aux parties habilitées à en prendre connaissance et après accord du travailleur).

Cette individualisation se fait **en fonction de la finalité que poursuit le contrôle installé par l'employeur et il peut s'agir** :

- **soit d'une procédure directe** (uniquement si l'on est dans le cadre des trois premières finalités visées ci-dessus par l'article 5, §1er, 1°, 2° et 3°)[284] ;
- **soit au moyen d'une procédure indirecte** (si l'on est **dans le cadre de la quatrième finalité, c.à.d. le contrôle des travailleurs** – art. 5, §1er, 4°) : donc l'employeur devra inviter le travailleur visé à un entretien, préalablement à toute décision ou évaluation susceptible d'affecter individuellement le travailleur (sauf en cas de suspension de l'exécution du contrat de travail pour quelque cause que ce soit)[285]. Celle-ci doit en principe revêtir un « *caractère de rappel ou de mise au point des principes et règles fixées dans l'entreprise de manière à éviter la survenance d'une nouvelle anomalie de même nature* »[286] (sauf dispositions contraires prévues par le règlement interne de l'entreprise ou le caractère grave de la faute commise, ici les dispositions du droit du travail s'appliqueront de plein droit).

c. L'Avis n°12/2005 du 7 septembre 2005 de la Commission pour la Protection de la Vie Privée[287]

En ce qui concerne la surveillance des travailleurs, justement par l'utilisation d'un système de monitoring associé au système de navigation GPS sur des véhicules de service, **la Commission pour la Protection de la Vie Privée (CPVP) a été amené à rendre un avis le 7 septembre 2005 sur une proposition de loi** qui **s'inspirait de l'esprit de la convention collective nº 68** du 16 juin 1998 relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu de travail[288] et qui entendait « ***fixer les bases d'une utilisation appropriée des systèmes de monitoring associés aux systèmes de***

[283] Entendue comme *« l'opération consistant à traiter des données de communication électroniques en réseau collectées lors d'un contrôle installé par l'employeur en vue de les attribuer à un travailleur identifié ou identifiable. »* (définition donnée par l'art. 12 de la CCT n°81).

[284] En pratique, les éventuelles anomalies peuvent être constatées par la consultation périodique des données de communication électroniques en réseau collectées dans l'entreprise ou par toute source d'information, et cette individualisation directe a pour but de permettre à l'employeur qui constate une anomalie de procéder à une individualisation des données afin de retracer l'identité de la ou des personnes responsables (cf. commentaire sous art. 15 de la CCT). Dans le projet eCMR, la plupart du temps les anomalies au bon fonctionnement des dispositifs embarqués vont pouvoir se faire via cette procédure d'individualisation directe.

[285] Cf. articles 15, 16 et 17 de la CCT n° 81.

[286] Cf. commentaire sous art. 16.

[287] Commission pour la protection de la vie privée, Avis n°12/2005 du 7 septembre 2005, réf. SA2 / A / 2005 / 013, concernant 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'.

[288] Convention qui a été rendue obligatoire par l'arrêté royal du 20 septembre 1998 (Moniteur belge du 2 octobre 1998).

***navigation GPS installés sur les véhicules de service**, tant dans les entreprises privées, que dans les entreprises publiques autonomes et le secteur public.* »[289].

Cette proposition introduisait notamment **l'obligation de ne pouvoir mettre en place une telle surveillance « *qu'après accord des commissions paritaires ad hoc**, du comité commun à l'ensemble des services publics, ou des organes compétents en vertu du régime des relations collectives de travail.* » (cf. art. 3 de la proposition).

Ainsi, **la CPVP dans son avis a rappelé** les suivants principes :

1) D'une part, elle estime, **qu'il ne lui est « *pas possible d'émettre un seul grand avis sur l'impact des nouvelles technologies** (GSM, courriel,…) sur la vie privée car la problématique lui semble trop étendue »*, mais qu'elle reste *« à disposition pour continuer [à se prononcer là-dessus] à l'avenir* »[290]. D'autre part, elle ne voit **pas la nécessité de modifier la loi générale « vie privée » pour inclure des règles spécifiques concernant tel ou tel secteur/domaine** puisque, selon elle, « ***la loi du 8 décembre 1992 revêt une portée générale dans le domaine de la protection de la vie privée lors du traitement de données relatives à une personne physique** et, à l'instar d'une loi générale, formule des principes applicables à tous les fichiers de données à caractère personnel au sens de cette loi* »[291].

2) **L'obligation de déclaration à la Commission et le devoir d'information préalable des travailleurs (avant tout traitement de cette nature) :** à cet égard, la CPVP rappelle que **l'accord entre partenaires sociaux** (évoqué par l'article 3 de la proposition de loi visée par l'avis) **devrait porter sur plusieurs points** :

    - **la finalité** (du traitement de données à caractère personnel), en ce sens que « *tout traitement de données à caractère personnel, **tel qu'un système permettant de rechercher la localisation précise des membres du personnel**, **doit répondre à des finalités déterminées, explicites et légitimes qui en justifient l'installation et l'utilisation*** » ;

Ainsi, cet accord doit également définir « ***explicitement la finalité de la surveillance*** » (en la reprenant si possible par écrit dans l'accord lui-même), **en tenant compte de :**

- **la sécurité du travailleur ;**
- **la protection du véhicule de service** (afin de permettre l'échange d'informations utiles à une éventuelle intervention de la police ou des secours, par ex.) ;

---

[289] Cf. 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 (Déposée par M. Philippe Mahoux) du 18 février 2005.

[290] Dans une rencontre informelle avec un membre de la CPVP, on nous a par ailleurs indiqué que la CPVP était ouverte à une « autorégulation » par le secteur routier et de la logistique ainsi que sur l'élaboration d'une sorte de « code de bonne conduite » en matière d'utilisation des nouvelles technologies (via les systèmes embarqués) pour la surveillance et le contrôle des travailleurs dans ce secteur spécifique. **Nous invitons le partenariat à y réfléchir dans le cadre de discussions ayant lieu dans leur secteur d'activité spécifique** (via le Cluster Logistique wallon, par exemple).

[291] Ainsi que le Conseil d'Etat l'avait déjà fait dans son *Avis du 19 juillet 1994, section de législation, première chambre des vacations, sur un projet d'arrêté royal « organisant la communication de données sociales à caractère personnel entre institutions de sécurité sociale »* (cité par l'avis de la CPVP).

- **des « besoins professionnels bien définis » concernant le transport et la logistique** (comme la gestion du parc automobile, par ex.) ;
- **et du pouvoir d'exercer un contrôle[292] sur le travail de l'employé.**

    - **L'admissibilité** (cf. art. 5 de la loi « vie privée ») : la CPVP rappelle que **les traitements de données à caractère personnel ne peuvent être effectués que dans un « *nombre limité de cas, parmi lesquels notamment le cas où le consentement ressort à l'intéressé, en l'occurrence le travailleur* »**[293] (souligné par l'auteur).

A ce propos, la proposition de loi va plus loin que la loi générale, puisqu'elle impose l'accord des syndicats afin de contribuer à la « *transparence du traitement, à un meilleur équilibre entre les droits des travailleurs et l'employeur et au caractère libre de l'accord du travailleur individuel* », toutefois la CPVP rappelle que **cet accord des syndicats « *ne peut pas remplacer le consentement [du travailleur]* *en tant que tel* »** donc il faut que « ***l'accord du syndicat soit enrichi du consentement individuel des travailleurs*** »[294] (souligné et gras par l'auteur).

- La **proportionnalité** : celle-ci ne peut être **jugée qu'au regard des finalités** « *de telle sorte que ces dernières doivent d'abord être clairement définies* » **afin d'évaluer la proportionnalité du traitement en lui-même ainsi que de chaque donnée traitée**.

Ainsi, au regard de ce principe, **la CPVP n'admet qu'un contrôle « ponctuel » (donc non permanent) et seulement *« si des indices font soupçonner des abus de la part de certains employés »*** (donc tout contrôle en dehors des heures de travail est exclu) ou « ***s'il est effectué dans l'intérêt de la sécurité du travailleur*** » : elle considère donc **qu'un contrôle permanent** *« avec lecture systématique des données enregistrées par le système de localisation* » doive être **considéré comme « *disproportionné* »**, **mais admet** qu'il puisse être envisagé **« *pour des raisons de sécurité, dans un contexte spécifique* »** (comme par exemple dans le cadre d'un transport de matières dangereuses ou de fonds).

Par ailleurs, la CPVP admet également qu'il puisse exister « *certaines hypothèses dans lesquelles **un contrôle plus régulier pourrait être justifié s'il est directement lié à la nature des tâches à accomplir par l'employé**, et plus précisément afin d'optimiser la gestion des déplacements de véhicules professionnels* », dans ces cas-là elle permettrait « *des contrôles tout au long de la journée de travail (…) **mais sans que le suivi des véhicules soit continu*** ». Par rapport à cela, la Commission propose alors que « *dans les cas où **cela s'avère faisable**, la **solution optimale** consisterait à **permettre à l'employé d'activer et de désactiver le***

[292] Selon les Développements précédant la proposition de loi ***« il s'agirait (uniquement) de surveiller le personnel, afin de contrôler l'utilisation professionnelle du véhicule de service et l'application honnête du régime de travail*** » (cité par l'avis, p. 4) (souligné par l'auteur). Ce qui réduit la marge de manœuvre du responsable de traitement concernant de tels traitements ayant pour finalité une surveillance « excessive » du travailleur.

[293] Une analyse approfondie mériterait d'être faite concernant la réalité d'un « consentement libre et éclairé » des travailleurs, puisque ceux-ci sont soumis aux aléas du marché du travail et à la « bonne volonté » de leurs employeurs, surtout dans un secteur aussi précaire que le transport routier où le droit du travail général souffre de nombreuses spécificités/exceptions (régime spécial concernant les salaires, les horaires de travail, les heures supplémentaires, etc).

[294] Cf. loi « vie privée » mais également l'article 123 de la loi « communication électroniques » (citées ci-dessus).

système de façon ponctuelle, selon les nécessités de sa localisation *(par exemple, à l'arrivée et au départ de chaque lieu où il doit se rendre). Le* ***système devrait*** *en tout état de cause pouvoir* ***être désactivé lors de l'utilisation du véhicule en dehors des heures de travail****.* » (souligné et gras par l'auteur).

- **La transparence et l'information** (cf. art. 9 de la loi « vie privée ») : en effet, dans le cas où un traitement ayant une finalité de contrôle devrait être mis en place, la CPVP rappelle que dans ce cas-là **le(s) responsable(s) du traitement devrait(ent) prévoir une** ***« information détaillée au profit des personnes dont les données sont traitées****, en particulier* ***qui est soumis à un contrôle****,* ***dans quelle mesure un contrôle est effectué****,* ***la nature des abus qui peuvent donner lieu à un contrôle****,* *la* ***durée des contrôles****,* *la* ***procédure qui sera suivie après le contrôle.*** *»* (souligné par l'auteur).

De plus, chaque type de traitement de données à caractère personnel ayant pour finalité la surveillance et le contrôle des travailleurs doit faire l'objet d'une **demande de contrôle préalable à la Commission** car il s'agit de **traitements dits « sensibles »**, et la CPVP devra examiner au cas par cas chaque demande en ce sens.

En outre, ainsi que la CPVP le rappelle dans son avis, « ***l'employeur*** *qui procède à l'installation et à l'utilisation d'un tel système de surveillance* ***doit en outre veiller*** *à toute une série d'autres mesures (…) [comme]* ***garantir la sécurité et la confidentialité du traitement****,* ***respecter les droits des personnes concernées en matière d'accès et, le cas échéant, de rectification de leurs données à caractère personnel****.* » (souligné par l'auteur).

On peut donc dire qu'il y a encore une **relative insécurité juridique dans ce domaine**, et notre recommandation aux éventuels futurs responsables de ce type de traitements est de bien respecter l'obligation de déclaration préalable à la Commission afin d'obtenir un avis favorable au traitement ou, à défaut, des recommandations concrètes pour mettre en œuvre un tel traitement au sein de son entreprise.

D. L'avis du Contrôleur Européen pour la Protection des Données concernant la protection de la vie privée dans le secteur des « transports intelligents »

Depuis l'année 2008, la Commission européenne s'est également penchée sur la problématique des ICT dans les « transports intelligents »[295], ainsi un '**Plan d'action pour le déploiement de systèmes de transport intelligents en Europe'**[296], puis une '**proposition de Directive 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**

[295] Pour toutes les informations voir sur site de la Commission européenne : http://ec.europa.eu/transport/its/road/action_plan/action_plan_en.htm# (en anglais).

[296] Communication de la Commission, *Plan d'action pour le déploiement de systèmes de transport intelligents en Europe, COM(2008) 886 final*, Bruxelles le 16.12.2008.

transport'[297]**,** ont été tour à tour élaborés afin de chercher à réglementer la matière en collaboration avec les acteurs du secteur du transport au niveau européen[298].

1) Sur le 'Plan d'action pour le déploiement de systèmes de transport intelligents en Europe'

Ce Plan d'action est intervenu afin que « *le potentiel des systèmes de transport intelligents soit pleinement exploité et favorise l'émergence de résultats tangibles* » (notamment en matière de sécurité routière, de gestion de la « congestion » routière[299], de réduction de la pollution et d'économie de l'énergie). Pour le secteur qui nous occupe dans le projet eCMR, soit en matière de transport routier des marchandises, **ces systèmes de transport intelligents sont notamment employés pour la gestion et le contrôle du trafic, pour la gestion des télépéages et pour la navigation routière**.

C'est pourquoi le plan d'action visait à la **mise en place d'une feuille de route pour six domaines d'actions prioritaires** se fondant sur une série d'initiatives déjà en cours à la Commission européenne (dont le plan d'action pour la logistique du transport de marchandises, le plan d'action sur la mobilité urbaine, le déploiement de Galileo, le paquet «*écologisation des transports*», l'initiative *i2010* sur les véhicules intelligents, l'initiative *eSafety*, le 7e programme-cadre pour la recherche et le développement technologique, l'initiative *eCall*, les plateformes technologiques européennes et leurs programmes stratégiques de recherche, ou l'initiative *CARS 21*[300]), et qui sont :

1) L'utilisation optimale des données relatives aux routes, au trafic et aux itinéraires
2) La continuité des services STI de gestion du trafic et des marchandises dans les corridors de transport européens et dans les agglomérations urbaines
3) La sécurité et la sûreté routière :
4) L'intégration des véhicules dans l'infrastructure de Transports
5) La sécurité et la protection des données et les questions de responsabilité
6) Et la coopération et la coordination des STI européens

[297] 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, *COM(2008) 887 final, 2008/0263 (COD),* Bruxelles, le 16.12.2008.

[298] Même si déjà depuis les années 1980 certaines initiatives avaient commencé à se mettre en place en étant centrées sur certains aspects précis, notamment sur les transports non polluants et économes en énergie, la congestion routière, la gestion du trafic, la sécurité routière, la sûreté des transports commerciaux ou la mobilité urbaine. Leur mise en œuvre étant souvent non coordonnée et morcelée selon les pays européens, l'Union européenne a commencé à s'y intéresser petit à petit pour finalement aboutir à ces amorces de « législation » européenne, ceci afin d'éviter que « *les STI ne finissent par composer un assemblage disparate d'applications et de services et pour garantir la continuité géographique, l'interopérabilité des services et des systèmes et la normalisation* ».

[299] Comme il est souligné dans ce document « *Des services d'information en temps réel sur la circulation routière et les déplacements (RTTI), qui, de plus en plus, sont combinés à la navigation par satellite, sont désormais proposés de source privée et publique et favorisent la mobilité.* ».

[300] Pour des références complètes concernant ces actions se référer au texte du Plan d'action (p. 8).

Toutefois la Commission européenne précise que « ***La mise en place d'un cadre qui vise à réaliser ces actions et qui précise les procédures et les spécifications concernées nécessitera la mobilisation des États membres et d'autres parties prenantes.***[301] *(…) ce plan d'action aidera à coordonner les ressources et les instruments disponibles afin d'apporter une forte valeur ajoutée à l'Union européenne.* ». La plus-value de ce plan d'action est qu'il a été élaboré sur la base de contributions obtenues grâce à une **large consultation des parties prenantes du secteur** (recueillies par des entretiens avec le secteur privé et public, des ateliers, un questionnaire internet, ainsi qu'à partir de discussions ciblées au sein de forums), d'où la stratégie qui en a émergé.

2) Sur la proposition de 'Directive 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'

Etant donné que l'adoption des systèmes de transport intelligents dans le domaine du transport routier n'a pas été aussi rapide qu'escompté par la Commission européenne et que le déploiement des services restait, d'une manière générale, fragmentaire, dont *« il en résulte une multiplicité de solutions nationales, régionales et locales, sans harmonisation claire, qui met en péril l'intégrité du marché unique.* », la Commission a décidé d'aller plus loin et de rédiger une **proposition de directive** suivant les résultats déjà obtenus. L'objectif général de cette proposition étant d'établir un « *cadre pour accélérer et coordonner le déploiement et l'utilisation des systèmes de transport intelligents dans le domaine du transport routier, notamment les interfaces avec d'autres modes de transport, en vue de favoriser l'émergence, dans l'Union européenne, d'un transport des marchandises et des passagers plus efficace, plus respectueux de l'environnement et plus fiable.* »[302]. Les objectifs spécifiques de cette directive sont notamment : l'accroissement de l'interopérabilité des systèmes, la fourniture d'un accès ininterrompu, la continuité des services et la mise en place d'un mécanisme de coopération efficace entre toutes les parties prenantes.

L'intérêt majeur de cette directive pour la poursuite de notre projet est qu'elle proposera des définitions communes à des notions comme « *systèmes de transports intelligents* (STI) », « *interopérabilité* », « *prestataire de services STI* », « *dispositif nomade* », « *plateforme* » (…)[303]. Ces notions devront être reprises par les Etats membres dans leurs lois nationales de transposition, afin que la qualité de ces données, leur fiabilité et mise à jour régulière, leur échange, etc, soient assurés (art. 3 de la proposition) ; alors que la Commission aura un rôle plus spécifique pour le déploiement et l'utilisation dans quelques domaines prioritaires, dont la gestion des « *données relatives aux routes, à la circulation et aux déplacement* », dans la « *continuité des services STI de gestion de la circulation et du fret dans les couloirs de transport européens(…)* », en ce qui concerne « *la sécurité et la sûreté routières* » et dans « *l'intégration du véhicule dans l'infrastructure de transport* »[304] (et qui se feront

[301] Souligné par l'auteur.

[302] Conformément au principe de subsidiarité, la Commission européenne a estimé que l'adoption d'une directive-cadre était le « *meilleur moyen d'atteindre l'objectif poursuivi* ».

[303] Voir article 2 de la proposition de directive.

[304] Dont les principes et les éléments essentiels sont visés aux Annexes I et III de la directive. Nous invitons les partenaires du projet eCMR à les lire puisqu'ils sont essentiels au bon déploiement du dispositif choisi par ce projet (Annexe II essentiellement).

certainement par voie de Règlement). Cette directive fait également appel à la nécessité de certification du matériel et des logiciels STI liés à l'infrastructure routière (art. 5), pour des raisons d'efficacité (énergétique), de sûreté et de sécurité, ou de protection de l'environnement.

En ce qui concerne les **règles relatives au respect de la vie privée, à la sécurité et à la réutilisation des informations, l'article 6** de cette directive (version de la proposition) dispose que :

> « *1. Les États membres veillent à ce que le traitement des données à caractère personnel dans le cadre de l'exploitation des STI* ***soit conforme aux règles communautaires protégeant les libertés et les droits fondamentaux des individus, en particulier les directives 95/46/CE et 2002/58/CE.***
>
> *2. En particulier, les États membres veillent à ce que les données et les enregistrements des STI soient protégés contre toute utilisation abusive, notamment les accès non autorisés, les modifications ou les pertes.*
>
> *3. La directive 2003/98/CE [concernant la réutilisation des informations émanant du secteur public] s'applique.* »

Cette directive prévoit également la **création d'un comité**, dénommé « *Comité européen des STI (EIC)* », **et d'un 'Groupe consultatif européen sur les STI'**, qui la conseillera « *sur les aspects techniques et commerciaux du déploiement et de l'utilisation des STI dans la Communauté* » (il devra être composé de « *représentants à haut niveau de prestataires de services STI, d'associations d'utilisateurs, d'opérateurs de transport et d'exploitants d'installations, du secteur manufacturier, de partenaires sociaux, d'associations professionnelles,…* »)[305]. Le texte prévoit également que les Etats membres soumettent régulièrement un « *rapport circonstancié sur leurs activités et projets nationaux concernant les domaines prioritaires* », et qu'ils établissent un plan d'action national quinquennal (avec des rapports annuels sur l'état d'avancement).

3) Recommandations du Contrôleur Européen en ce qui concerne le respect de la vie privée

Dans le cadre des compétences que le Règlement 45/2001/CE306 attribue au Contrôleur Européen pour la protection des données (CEPD)[307,] celui-ci a émis un avis[308] se penchant sur les aspects « vie privée » que l'utilisation des systèmes de transport intelligents implique,

[305] Cf. article 8 et 9 de la proposition de directive.

[306] Règlement (CE) n° 45/2001 du Parlement Européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, *J.O.U.E. L 8 du 12.01.2001* (pp. 1 à 22).

[307] Le Règlement (CE) n° 45/2001 définit les mêmes droits et obligations que la Directive 95/46/CE, mais au niveau des institutions et des organes européens. Il institue également le CEPD en tant qu'autorité de contrôle indépendante qui a pour mission de garantir le respect dudit règlement.

[308] 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, (2010/C 47/02), J.O.U.E, C 47 du 25.2.2010 (p.6-16).

étant donné que la plupart des véhicules aujourd'hui utilisent ces systèmes afin de tracer les véhicules, les marchandises et même les individus, par le biais des systèmes de géolocalisation notamment.

Cet avis, adopté en juillet 2009, portait surtout sur le texte de la proposition d'un plan de déploiement de la Commission européenne pour les systèmes de transport intelligents (STI) en Europe en vue d'accélérer et de coordonner leur déploiement dans les transports routiers et leur relation avec d'autres modes de transport, et sur la proposition de directive. Son intervention se justifiait, selon le CEPD, *« étant donné que* ***ce déploiement a des implications importantes en termes de protection de la vie privées, notamment parce que ces systèmes permettent de suivre un véhicule et de recueillir un large éventail de données relatives aux habitudes de conduite des usagers européens de la route*** ».

Dans cet avis, le CEPD relève que la protection des données a été prise en compte dans le projet de cadre juridique et qu'elle est également présentée comme une condition générale pour le déploiement des STI. Toutefois, il **souligne dans son avis que la proposition est trop générale pour répondre de façon appropriée aux questions de vie privée et de protection des données soulevées par le déploiement des STI dans les États membres**.

En particulier, il estime que **le cadre juridique ne définit pas clairement** :

- quand l'exécution des services STI entraînera la collecte et le traitement de données personnelles,
- quelles sont les finalités et les modalités selon lesquelles des traitements de données pourront avoir lieu,
- ou qui sera responsable du respect des obligations en matière de protection des données.

Or, étant donné qu'il existe un risque que **le manque de clarté du cadre juridique proposé conduise à une « *incertitude élevée, à une fragmentation et à des incohérences en raison de différents niveaux de protection des données en Europe* »**[309] le CEPD a rendu le suivant avis en **formulant les recommandations suivantes**:

1° la nécessité d'une clarification des responsabilités: en effet, selon le CEPD il est **essentiel de clarifier les rôles des différents acteurs impliqués dans les STI afin de déterminer qui a la responsabilité de s'assurer que les systèmes fonctionnent correctement** du point de vue de la protection des données (qui est le responsable du traitement ?);

2° il faudra des garanties supplémentaires lors de l'utilisation des technologies de localisation: notamment des **mesures de protection appropriées** (précisions sur les circonstances spécifiques pour lesquelles les mouvements d'un véhicule seront suivis et **limitation stricte** de l'utilisation de systèmes de localisation **à ce qui est nécessaire,** notamment) **doivent être mises en œuvre par les responsables du traitement** qui fournissent des services STI **pour que l'utilisation des technologies de localisation ne soit pas intrusive (ou le moins intrusif possible) en termes de vie privée**;

3° le CEPD rappelle le principe de la "*privacy by design*" (c'est-à-dire le respect de la vie privée dès l'élaboration des outils techniques) et recommande **d'envisager la vie**

[309] Souligné par l'auteur.

privée et la protection des données à un stade précoce de la conception des STI afin de définir l'architecture, le fonctionnement et la gestion des systèmes.

En effet, selon lui, la protection de la vie privée et les exigences de sécurité doivent déjà être incorporées dans les normes, les meilleures pratiques, les spécifications techniques et les systèmes.

Nous appuyons tout à fait cette démarche en suggérant au partenariat qu'il mène une réflexion approfondie sur l'architecture du système embarqué (Stepp III de Falcom) de collecte et de transfert de données vers le serveur distant, ainsi que du(des) logiciel(s) de traitement des données (surtout si les finalités de ces traitements servent surtout au contrôle et à la surveillance des travailleurs). D'ailleurs, la garantie d'une bonne politique de vie privée (privacy policy) incorporée dans ce service sera un avantage commercial de vente à des futurs clients, en plus de respecter la réglementation en vigueur dans la matière (voir parties ci-dessous).

4) Evolutions dans le secteur

Nous attirons l'attention du partenariat sur le fait que **le dernier 6 juillet 2010 le texte de la directive[310] a été approuvé en deuxième lecture par le Parlement européen**[311], **donc le cadre légal dans ce secteur risque fortement de changer** dans les prochains mois/années. En vertu de cette directive, la Commission doit, dans les sept années à venir, adopter des spécifications (fonctionnelles, techniques, organisationnelles ou relatives à la prestation de services) afin de permettre la compatibilité, l'interopérabilité et la continuité des solutions STI à travers l'Europe. **La Commission va en outre créer un groupe consultatif européen sur les STI**, qui réunira les représentants des parties concernées et aura pour rôle de conseiller la Commission sur les aspects commerciaux et techniques de la mise en œuvre et du déploiement des systèmes de transport intelligents dans l'Union européenne[312].

Nous invitons nos partenaires industriels à se faire connaître auprès des autorités nationales du secteur afin de contribuer à la mise en place de ces systèmes (tout en proposant le dispositif concerné par le projet eCMR).

---

[310] Désormais appelée : "*Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport*" (suivre évolutions sur: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2010-0258&language=EN).

[311] Ainsi, M. Siim Kallas, vice-président de la Commission européenne chargé des transports, a déclaré: «*Cette directive est un instrument important pour une mise en œuvre coordonnée des STI en Europe. Elle permettra de progresser énormément vers le déploiement et l'utilisation de services STI intéropérables et fluides, tout en laissant aux États membres la liberté de décider dans quels systèmes investir. Le vote d'aujourd'hui facilitera le développement d'une mobilité intégrée et compétitive plus efficace, plus sûre et plus durable en Europe.*" (voir Communiqué de presse sur: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/891&format=HTML&aged=0&language=FR&guiLanguage=fr).

[312] Les prochaines étapes après cela vont être : les États membres auront 18 mois pour transposer la directive en droit interne après sa publication au Journal officiel de l'Union Européenne, puis d'ici fin 2010 le comité européen STI et le groupe consultatif européen STI devront être institués, et d'ici fin 2011 la Commission annonce qu'elle adoptera un programme de travail et les États membres sont invité à publier un premier rapport sur leurs activités nationales (pour plus d'informations, consulter régulièrement le site : http://ec.europa.eu/transport/its/).

Bibliographie

Avis/Décisions :

Commission pour la protection de la vie privée, avis n° 11/2004 du 4 octobre 2004, n° 14, N. Réf. : 10 / A / 2004 / 011, http://www.privacycommission.be/fr/docs/Commission/2004/avis_11_2004.pdf

Commission pour la protection de la vie privée, Avis n°12/2005 du 7 septembre 2005, réf. SA2 / A / 2005 / 013, *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* http://www.privacycommission.be/fr/docs/Commission/2005/avis_12_2005.pdf

Contrôleur Européen pour la protection des données, Avis du 22 juillet 2009 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, JO C 47, 25.02.2009, p. 6, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_FR.pdf

Décision 2004/915/CE du 27 décembre 2004, modifiant la décision 2001/497/CE en ce qui concerne l'introduction d'un ensemble alternatif de clauses contractuelles types pour le transfert de données à caractère personnel vers de pays tiers, Journal officiel L 385 du 29.12.2004, http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=fr&type_doc=Decision&an_doc=2004&nu_doc=915

Groupe « Article 29 » sur la Protection des Données, *Avis 4/2007 sur le concept de données à caractère personnel*, WP 136 adopté le 20 juin 2007, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_fr.pdf

Groupe « Article 29 » sur la Protection des Données, *Avis 1/2009 concernant les propositions modifiant la directive 2002/58/CE sur la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques»),* WP 159 adopté le 10 février 2009, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp159_fr.pdf

Groupe « Article 29 » sur la Protection des Données, *Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant »*, WP 169 adopté le 16 février 2010, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_fr.pdf

Conventions collectives :

Convention collective de travail n° 68 du 16 juin 1998 relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu de travail *(ratifiée*

par l'AR du 20 septembre 1998 paru au M.B. du 2 octobre 1998), http://www.cnt-nar.be/F1I.htm

Convention collective de travail n° 81 du 26 avril 2002 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau *(ratifiée par l'AR du 21 juin 2002, paru au MB du 29 juin 2002)*, http://www.cnt-nar.be/F1I.htm

Doctrine :

LÉONARD, Thierry ; ROSIER, Karen. *La jurisprudence « Antigoon » face à la protection des données: salvatrice ou dangereuse ?*, Revue du Droit des Technologies de l'Information, 2009, n° 36. - pp. 5-10, http://www.rdti.be/editorial/edit36.html

LETACQ F., IDIT, *« Comparaison CMR et droit interne : Tableau comparatif des régimes français et CMR du contrat de transport routier de marchandises »*, http://www.idit.asso.fr/docenligne/documents/comparaison_cmr.pdf?PHPSESSID=e5cdad1062601f8c5b9c90884af82a50

MORENO O., *La géolocalisation des travailleurs*, DroitBelge.Net - Actualités - 22 décembre 2005, http://www.droitbelge.be/news_detail.asp?id=297

RAY J.-E., *Géolocalisation, données personnelles et droit du travail*, Dr.soc., 2004, p. 1081

Législation belge :

Arrêté Royal du 13 juillet 1984 portant exécution du règlement (C.E.E.) n° 3821/85 du Conseil des Communautés européennes du 20 décembre 1985 concernant l'appareil de contrôle dans le domaine des transports par route, modifié par l'AR du 14 juillet 2005 (publié le 26 juillet 2005), http://www.ejustice.just.fgov.be/cgi_loi/arch_a1.pl?=&sql=%28text+contains+%28%27%27%29%29&rech=1&language=fr&tri=dd+AS+RANK&numero=1&table_name=loi&F=&cn=1984071333&caller=archive&fromtab=loi&la=F&ver_arch=002#fiche

Arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B. 13 mars 2001*, http://www.privacycommission.be/fr/static/pdf/wetgeving/ar_vie_privee.pdf

Arrêté Royal relatif au transport de choses par route du 7 MAI 2002, rubrique « Route - Transport de marchandises - Transport pour compte de tiers - Lois et textes réglementaires » disponible sur : http://www.mobilit.fgov.be/fr/index.htm

Arrêté Ministériel pris en exécution de l'arrêté royal du 7 mai 2002 relatif au transport de choses par route du 8 MAI 2002 (tel que modifié par l'Arrêté Ministériel du 5 février 2007), rubrique « Route - Transport de marchandises - Transport pour compte de tiers - Lois et textes réglementaires » disponible sur : http://www.mobilit.fgov.be/fr/index.htm

Loi du 3 juillet 1978 relative aux contrats de travail, *M.B. du 22 août 1978* (mise à jour au 27/10/2009), http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1978070301&table_name=loi

Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B. 18 mars 1993 (version consolidée 01/08/2007)*, http://www.privacycommission.be/fr/static/pdf/wetgeving/loi_vie_privee.pdf

Loi du 10 juin 1998 modifiant la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, *M.B. 22 septembre 1998*, http://reflex.raadvst-consetat.be/reflex/pdf/Mbbs/1998/09/22/57338.pdf

Loi du 3 mai 1999 relative au transport de choses par route, rubrique « Route - Transport de marchandises - Transport pour compte de tiers - Lois et textes réglementaires », *M.B. du 30/06/1999, p. 24507*, http://reflex.raadvst-consetat.be/reflex/pdf/Mbbs/1999/06/30/62496.pdf

Loi du 13 juin 2005 relative aux communications électroniques, *M.B. 20.06.2005, http://www.juridat.be/cgi_loi/loi_F.pl?cn=2005061332*

Loi du 21 décembre 2006 transposant la directive 2004/52/CE du Parlement européen et du Conseil du 29 avril 2004 concernant l'interopérabilité des systèmes de télépéage routier dans la Communauté, *M.B. du 29 décembre 2006*, http://www.staatsbladclip.be/moniteur/lois/2006/12/29/loi-2006014293.html

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 (Déposée par M. Philippe Mahoux), 3-1044/1 3-1044/1, Sénat de Belgique, SESSION DE 2004-2005, 18 FÉVRIER 2005, http://www.philippe-mahoux.be/020_vie_politique.php?doc=1257

Législation internationale et européenne :

Communication de la Commission, *Plan d'action pour le déploiement de systèmes de transport intelligents en Europe*, COM(2008) 886 final, Bruxelles le 16.12.2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0886:FIN:FR:HTML

Convention sur la circulation routière, signée à Genève le 19 Septembre 1949, Nations Unies (ONU), *Recueil des Traités*, vol. 125, p. 3

Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales, signée à Rome le 4 novembre 1950, Conseil de l'Europe, http://conventions.coe.int/Treaty/fr/Treaties/Html/005.htm

Convention relative au Contrat de Transport International de Marchandises par Route (CMR) et Protocole de Signature, signée à Genève le 19 Mai 1956, Nations Unies (ONU), http://www.unece.org/trans/conventn/cmr_f.pdf

Convention sur la circulation routière, Vienne, 8 Novembre 1968, Nations Unies, (version consolidée 2006), http://www.unece.org/trans/conventn/Conv_road_traffic_FR.pdf et http://www.unece.org/trans/conventn/Agreement_road_traffic_FR.pdf

Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 (dite « Convention 108 »), Strasbourg, http://conventions.coe.int/Treaty/fr/Treaties/Html/108.htm

Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, *JO L 281 du 23.11.1995, p. 31–50*, http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=31995L0046&model=guichett&lg=fr

Directive 2002/58/CE du Parlement européen et du Conseil, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, *Journal officiel n° L 201 du 31/07/2002 p. 0037 – 0047*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:FR:HTML

Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, *JO L 105 du 13.4.2006, p. 54–63*, *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:FR:NOT*

Document informel N° 12, COMMISSION ECONOMIQUE POUR L'EUROPE, COMITE DES TRANSPORTS INTERIEURS, Soixante-douzième session, ONU, Genève, 23-25 février 2010, *Adoption de la liste des principales décisions prises par le Comité à sa soixante-douzième session*, *http://www.unece.org/trans/doc/2010/itc/ITC-72-inf12f.pdf*

Draft recommendation on the protection of individuals with regard to automatic processing of personal data in the context of profiling, COUNCIL OF EUROPE, Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data [ETS 108] (T-PD), Strasbourg, 3 juin 2010, http://www.coe.int/t/dghl/standardsetting/DataProtection/TPD%20documents/T-PD-BUR_2009_02rev6_en_Fin%20_2.pdf

Projet de Recueil de directives pratiques sur la protection des données personnelles des travailleurs, Bureau international du Travail, Organisation internationale du Travail (OIT), Genève, 1995, http://www.ilo.org/global/About_the_ILO/Media_and_public_information/Press_releases/lang--fr/WCMS_008116/index.htm#n

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, COM(2008) 887 final, 2008/0263 (COD), Bruxelles, le 16.12.2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0887:FIN:FR:HTML

Protocole du 5 juillet 1978 à la Convention relative au contrat de transport international de marchandises par route (CMR), signé à Genève, Nations Unies (ONU), http://www.unece.org/trans/conventn/CMR_prot_f.pdf

Protocole additionnel à la CMR du 17-19 octobre 2006 concernant l'harmonisation des prescriptions applicables aux opérations de transport international par route et facilitation de ces opérations, Conseil Economique et Social de l'ONU (Commission Economique pour L'Europe, Comité des Transports Intérieurs, Groupe de travail des transports routiers, Centième session), Genève, 17-19 octobre 2006 (Point 5 de l'ordre du jour provisoire), http://www.unece.org/trans/doc/2006/sc1/ECE-TRANS-SC1-2006-01f.pdf

Protocole Additionnel du 21 février 2008 à la Convention relative au Contrat de Transport International de Marchandises Par Route (CMR) concernant la Lettre de Voiture Electronique, Conseil Economique et Social de l'ONU (Commission Economique pour L'Europe, Comité des Transports Intérieurs, 70ème session), Genève, 19 – 21 Février 2008, Nations Unies (ONU), http://www.unece.org/trans/doc/2008/sc1/ECE-TRANS-2008-CRP-01a1f.pdf

Recommandation n° R (89) 2 du Comité des Ministres aux Etats Membres sur la protection des données à caractère personnel utilisées à des fins d'emploi, adoptée par le Comité des Ministres le 18 janvier 1989, lors de la 423e réunion des Délégués des Ministres, Conseil de l'Europe, 1989, http://www.coe.int/t/f/affaires_juridiques/coop%E9ration_juridique/protection_des_donn%E9es/documents/instruments%20juridiques%20internationaux/1Rec(89)2_FR.pdf

Règlement (CEE) n° 11 du 27 juin 1960 concernant la suppression de discriminations en matière de prix et conditions de transport, pris en exécution de l'article 79, paragraphe 3, du traité instituant la Communauté économique européenne, http://admi.net/eur/loi/leg_euro/fr_360R0011.html

Règlement (CEE) n° 3820/85 du Conseil du 20 décembre 1985 relatif à l'harmonisation de certaines dispositions en matière sociale dans le domaine des transports par route, J.O. L 370 du 31.12.1985, p. 1–7, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31985R3820:FR:NOTRèglement (CEE) n° 881/92 du Conseil du 26 mars 1992, concernant l'accès au marché des transports de marchandises par route dans la Communauté exécutés au départ ou à destination du territoire d'un État membre, ou traversant le territoire d'un ou de plusieurs États membres, J.O. L 95 du 9.4.1992, p. 1–7, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31992R0881:FR:NOT

Règlement (CEE) n° 3118/93 du Conseil, du 25 octobre 1993, fixant les conditions de l'admission de transporteurs non-résidents aux transports nationaux de marchandises par route dans un État membre, J.O. L 279 du 12.11.1993, p. 1–16, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31993R3118:FR:NOT

Règlement (CE) n° 45/2001 du Parlement Européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, J.O.U.E. L 8 du 12.01.2001, p. 1-22, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/DataProt/Legislation/Reg_45-2001_FR.pdf