Advies nr 31/2012 van 12 september 2012

Betreft: Adviesaanvraag betreffende het voorontwerp van wet tot creatie van het kader voor het invoeren van intelligente vervoerssystemen ("ITS-kaderwet") (CO-A-2012-023)

De Commissie voor de bescherming van de persoonlijke levenssfeer;

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna WVP), inzonderheid artikel 29;

Gelet op het verzoek om advies van de Staatssecretaris voor Mobiliteit ontvangen op 21/05/2012;

Gelet op het verslag van de heer De Schutter;

Brengt op 12 september 2012 het volgend advies uit:

I. ONDERWERP EN CONTEXT VAN HET ADVIES

1. De Staatssecretaris voor Mobiliteit vraagt het advies van de Commissie over het voorontwerp van wet tot omzetting van de Richtlijn 2010/40/EU van het Europees Parlement en de Raad van 7 juli 2010 betreffende het kader voor het invoeren van intelligente vervoerssystemen op het gebied van wegvervoer en voor interfaces met andere vervoerswijzen; hierna "het voorontwerp van wet".

2. Dit voorontwerp van wet kadert in een ruimere Europese context waaronder een Actieplan van de Europese Commissie[1] (hierna "ITS Actieplan), de richtlijn 2010/40/EU (hierna "ITS-richtlijn") en eerdere relevante standpunten van Europese en andere buitenlandse overheden, waaronder
   - een advies van de Europese toezichthouder voor gegevensbescherming (hierna "EDPS") [2;]
   - adviezen van Groep Gegevensbescherming artikel 29 (m.b.t. een geharmoniseerde pan-Europese dienst voor noodoproepen vanuit voertuigen, genaamd "eCall", gebaseerd op het gemeenschappelijke Europese alarmnummer 112)[3] en betreffende geolocatie op slimme mobiele apparaten[4];
   Eerder was er ook een advies van de Groep van Berlijn[5]

3. Omdat ook sprake is van een gewestaangelegenheid[6] zal op regionaal niveau ook sprake zijn van omzetting van de ITS-richtlijn. Een Vlaams voorontwerp van Decreet[7] is inmiddels aangenomen dat tot doel heeft om de ITS-richtlijn op Vlaams niveau om te zetten. De Commissie vernam dat dit ontwerp voor officieel advies zou worden voorgelegd aan de Vlaamse Toezichtcommissie. Zij pleegde dienaangaande overleg met de Vlaamse Toezichtcommissie teneinde te komen tot een wederzijds afgetoetst standpunt.

4. De Europese Commissie (DG MOVE) verzocht een privaat consortium[8] om een studie te verrichten over gegevensbescherming, waarvan de publicatie wordt verwacht in september. De eerste bevindingen uit deze studie werden toegelicht op een workshop op 13 juni 2012. Geviseerde ITS applicaties in deze studie zijn de digitale tachograaf, e-Call, rekeningrijden (Road user Charging), e-Ticketing bij openbaar vervoer, betaling van parkeerdiensten, verzekeringen gebaseerd op het rijgedrag ("Pay-As-You-Drive"), snelheidscontrole per traject (Section Speed Control), vlootbeheer (Fleet monitoring), het verwerken van

---

[1] Actieplan van de Europese Commissie dd. 16 december 2008 voor de invoering van intelligente vervoerssystemen in Europa, COM(2008) 886 def., gepubliceerd op http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0886:FIN:NL:PDF
[2] Zie het Advies van de Europese Toezichthouder voor gegevensbescherming betreffende de mededeling van de Commissie over een actieplan voor de invoering van intelligente vervoerssystemen in Europa en het bijbehorende voorstel voor een richtlijn van het Europees Parlement en de Raad tot vaststelling van het kader voor het toepassen van intelligente vervoerssystemen op het gebied van wegvervoer en voor raakvlakken met andere vervoerswijzen van 22 Juli 2009, PB, C 47/6 van 25 februari 2010, gepubliceerd op http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_NL.pdf
[3] Zie het werkdocument WP 125 van 26 september 2006 betreffende de gevolgen van het eCall-initiatief vanuit het oogpunt van bescherming van gegevens en van de persoonlijke levenssfeer, gepubliceerd op http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp125_nl.pdf
[4] Zie het document WP 185 over geolocatiediensten op slimme mobiele apparaten gepubliceerd op http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_nl.pdf
[5] Working Paper van 4-5 april 2011 m.b.t. Event Data Recorders (EDR) on Vehicles Privacy and data protection issues for governments and manufacturers, gepubliceerd op http://www.datenschutz-berlin.de/attachments/795/675.42.10.pdf?1308146250
[6] Vervoer is voornamelijk een gewestbevoegdheid.
[7] Betreffende het kader voor het invoeren van intelligente vervoerssystemen op het gebeid van wegvervoer en voor interfaces met andere vervoerswijzen
[8] Onder leiding van de Nederlandse onderneming Rapp Trans

verkeersgegevens (Traffic Data Collection) en samenwerkende systemen (Cooperative systems van types zoals C2C, C2I en I2C[9]).

5. Het doel van de ITS-richtlijn is omschreven als "(het waarborgen van) *het gecoördineerd en coherent invoeren van interoperabele intelligente vervoersystemen in de hele Unie*"[10].

6. "Intelligente vervoerssystemen" (hierna "ITS") *"zijn geavanceerde toepassingen die, zonder intelligentie als zodanig te belichamen, gericht zijn op het aanbieden van innovatieve diensten inzake verschillende vervoerswijzen en verkeersbeheer en die uiteenlopende gebruikers in staat stellen zich beter te informeren en veiliger, meer gecoördineerd en „slimmer" gebruik te maken van vervoersnetwerken"*[11]. Hierbij zijn *"zijn telecommunicatie, elektronica en informatietechnologieën met verkeerstechniek geïntegreerd met het oog op het plannen, ontwerpen, exploiteren, onderhouden en beheren van vervoerssystemen. Door informatie- en communicatietechnologie toe te passen op de sector van het wegvervoer en de interfaces daarvan met andere vervoerswijzen wordt een aanzienlijke bijdrage geleverd aan het verbeteren van de milieuprestaties, van de efficiëntie, met inbegrip van energie-efficiëntie, van de veiligheid van het wegvervoer, met inbegrip van het vervoer van gevaarlijke goederen, van de openbare veiligheid en van de mobiliteit van passagiers en goederen, terwijl tegelijkertijd het functioneren van de interne markt en meer concurrentiekracht en een grotere werkgelegenheid worden gewaarborgd. (…)."*[12]

7. ITS worden reeds sinds enkele jaren op steeds kleinere schaal in verscheidene vervoersprojecten uitgerold en ontwikkeld op Europees vlak of in de lidstaten, waaronder luchtvervoer (SESAR[13]), binnenvaart (RIS[14]), vervoer per spoor (ERTMS[15]) en via openbare vervoersmaatschappijen (MOBIB, NAVIGO[16]), scheepvaart (grote projecten en systemen zoals VTMIS[17], AIS[18], LRIT[19]), en wegvervoer (eToll[20] en eCall[21]).

---

[9] Waarbij de I staat voor de wagen (car) en de I voor infrastructuur
[10] Overweging 23 van de ITS-richtlijn;.
[11] Overweging 3 van de ITS-richtlijn;
[12] Overweging 4 van de ITS-richtlijn;
[13] http://www.sesarju.eu/
[14] http://ris.vlaanderen.be/html_nl/wat_is_ris/wat_algemeen.html
[15] http://ec.europa.eu/transport/rail/interoperability/ertms/ertms_en.htm
[16] http://www.cnil.fr/en/la-cnil/actu-cnil/article/article/2eme-controle-des-passes-anonymes-navigo/?tx_ttnews%5BbackPid%5D=91&cHash=1126ea84e899268aa04dd05017940670
[17] Vessel Traffic Management Information System. http://www.transport-research.info/web/projects/project_details.cfm?id=101
[18] Automatic Identification System of afgekort AIS is een systeem gebaseerd op transponder-technologie waarmee de veiligheid van scheepvaart op zeeën en het binnenwater verhoogd wordt. Het is bedoeld om overzicht en informatie te bieden via interactie tussen de schepen onderling en met instanties aan de wal. Het is in 2003 voor de zeevaart ingevoerd. Op het binnenwater gebruikt men Inland-AIS en is het een aanvulling op het bestaande verkeersmanagement van verkeersposten
[19] long-range identification and tracking (LRIT)
[20] Elektronische tolheffing of rekeningrijden
[21] Zie punt 3 van het advies van de EDPS dat verwijst naar het Actieplan van de Europese Commissie. Zie voormeld Werkdocument van de groep 29 betreffende eCall.

8. Het gaat hierbij om deels openbare, deels commerciële diensten (bijv. real-time verkeersinformatie, eFreight, eCall[22], eToll, reserveren van parkeerplaatsen[23] en het nieuwe type digitale tachograaf met ITS interface[24]), waarbij diverse actoren actief zijn ter promotie van ITS (bvb autoverzekeringsmaatschappijen, autoverhuurbedrijven[25],…). Vooral de commerciële diensten zijn de laatste jaren in opkomst omdat steeds meer voertuigen worden uitgerust met satellietnavigatie en mobiele communicatietechnologie (draadloze netwerken en internetverbinding), waardoor het mogelijk is om verkeersgegevens in te winnen zonder gebruik van de wegkantsystemen die worden beheerd door de wegbeheerders[26].

9. Volgens de groep van Berlijn[27] zal deze technologische trend ervoor zorgen dat de slimme voertuigen (net zoals slimme meters) op termijn een onderdeel zullen vormen van het zogenaamde "Internet of Things". Nieuwe concepten en trends zoals "connected cars" ("slimme en sociale" wagens) en "samenwerkende mobiliteit" passen in dit kader via de verbinding via internet, GPS en lokale netwerken. Dit zal nieuwe diensten of toepassingen ("Apps") doen ontstaan die de veiligheid verbeteren, voor minder files en vervuiling zorgen én het persoonlijke comfort verhogen[28]. Ook batterijbeheer voor elektrische wagens, motormanagement, muziek op aanvraag in de wagen[29], en marketingdiensten gebaseerd op context en connectiviteit ontstaan. Er zijn echter ook nadelen verbonden aan de toenemende profilering van de betrokkenen via de toenemende risico's die potentieel eigen zijn aan toenemende gegevensverwerking (bvb hacking van het openen van de deuren op afstand, en het alarmsysteem van de wagen onklaar maken[30], beveiligingsinbreuken, afbakenen van doelwitten voor misdrijven,…).

---

[22] Zie http://www.nxp.com/wcm_documents/news/meet-nxp/shows-and-events/ecall/presentations/eCall_trial_end_release.pdf

[23] Zie punt 8 van het advies van de EDPS.

[24] Zie randnummer 5 van het Advies van 5 oktober 2011 van de Europese Toezichthouder voor gegevensbescherming betreffende het voorstel voor een verordening van het Europees Parlement en de Raad tot wijziging van Verordening (EEG) nr. 3821/85 van de Raad betreffende het controleapparaat in het wegvervoer en tot wijziging van Verordening (EG) nr. 561/2006 van het Europees Parlement en de Raad, PB C 37/6 van 10 februari 2012, gepubliceerd op http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:037:0006:0013:NL:PDF

[25] Zie pagina 5 van voormeld Werkdocument WP 125 betreffende e-Call van de Groep 29.

[26] Zie http://www.rapptrans.nl/nl/its_pr_verkeers_reizigersinformatie.php

[27] Zie randnummer 2 van voormelde working paper van de Groep van Berlijn.

[28] Zie http://www.tue.nl/?id=17796

[29] Zie bvb de "MOG App" ondersteund door de nieuwe modellen van diverse autofabrikanten (http://www.fastcompany.com/1839441/mog-and-ford-voice-control-music-technology-for-cars en http://www.fastcompany.com/1805641/why-cars-the-worlds-worst-mobile-devices-are-hurting-music-services-like-spotify-pandora)

[30] http://www.businessweek.com/articles/2012-06-07/is-detroit-buying-verizon-s-lte-connected-car-vision

10. Ook in België is het meest concrete en zichtbare project voor het grote publiek wellicht Mobib, naast een proefproject van rekeningrijden in Leuven[31] en het gebruik van "fleetlogger" systemen in de dienstwagens van de politiediensten, en bij huurwagens en professioneel transport. De resultaten van de test in Leuven bewijzen volgens stakeholders dat 'intelligente mobiliteit' sturend werkt, doordat in overeenstemming met het mobiliteitsbeleid van de stad er minder sluipverkeer was en men meer in de dalperiodes reed.[32].

II. ALGEMENE VOORBESCHOUWING IN VERBAND MET DE TAAK VAN ADVIESVERLENING BIJ EEN ABSTRACT KARAKTER VAN DE ITS_RICHTLIJN EN HET VOORONTWERP

11. De Commissie ziet haar wettelijke adviestaak bemoeilijkt door de zeer algemene , abstracte opzet van de ITS Richtlijn die het Voorontwerp wenst om te zetten. De ITS-Richtlijn en het voorontwerp bieden onvoldoende verduidelijking over welke concrete ITS systemen en toepassingen worden geviseerd door Europa voor welke doelstellingen, hoewel een aantal van deze systemen toch reeds zijn gekend door Europa, want reeds zijn uitgerold of klaar om te worden uitgerold[33].

12. Europa verplicht de lidstaten om "de nodige wettelijke en bestuursrechtelijke bepalingen" te verrichten om te voldoen aan de ITS Richtlijn binnen een zeer korte omzettingstermijn (27 februari 2012)[34]. Anderzijds vereisen zowel de Europese[35] als de nationale regels inzake privacybescherming[36] dat de nationale wetgever duidelijke, concrete wetgeving dient op te stellen op het niveau van de omschrijving van de concrete inmengingen in de persoonlijke levenssfeer in het algemeen en de verwerkingen van persoonsgegevens in het bijzonder. Het ITS Actieplan van de Europese Commissie bevatte analoge vaagheden als de ITS Richtlijn en kreeg reeds de kritiek van de EDPS[37] op bepaalde punten zeer (te) abstract te zijn.

---

[31] sinds september 2011 via samenwerking tussen IBM, NXP, Mobistar, Touring en stad Leuven
[32] Bron http://www.its.be/Default.aspx?alias=www.its.be/tinc
[33] Zie randnummer 7 hiervoor.
[34] Zie artikel 18 van de ITS-Richtlijn
[35] Zie de rechtspraak van het EHRM over vereiste van voorzienbaarheid onder artikel 8 EVRM, o.m. in EHRM 4 mei 2000, Rotaru , § 52:
[36] Zie de rechtspraak van het grondwettelijk Hof inzake artikel 22 Grondwet
[37] Zie punt 5 en 14 van het voormelde advies van 22 juli 2009. 5. "(…) De specifieke doeleinden waarvoor ITS op deze gebieden zullen worden gebruikt, zijn evenwel niet duidelijk (…)". *"De EDPS wijst er evenwel op dat het voorgestelde wetgevingskader te breed en te algemeen is om de problemen inzake privacy en gegevensbescherming waartoe de invoering van ITS in de lidstaten aanleiding geeft, adequaat te kunnen aanpakken."*

13. Gelet op het belang van ITS systemen en applicaties voor onze maatschappij en de impact die het gebruik van geolocatietechnologie kan hebben op de vrijheid van zich anoniem te verplaatsen acht de Commissie het niet opportuun om zich te beperken tot het verlenen van een zeer kort en abstract advies in deze materie.

14. Om de wetgever maximaal te helpen bij het voorzien van een passende algemene legistieke omkadering inzake privacy- en gegevensbescherming bij het omzetten van de ITS-Richtlijn voegt de Commissie een concreet tekstvoorstel in bijlage bij dit advies, dat rekening houdt met de diverse opmerkingen in dit advies en een precedent op Europees vlak, met name in de energiesector.

15. Gelet op het regionaal karakter van de materie[38] en teneinde de eenheid van reglementering aangaande de vereiste waarborgen inzake ITS in België te bewaken naar de diverse actoren toe, is de Commissie voorstander van het afsluiten van samenwerkingsakkoorden tussen de federale overheid en de regionale overheden in deze materie. Zij wijst op de normatieve kracht van dergelijke akkoorden, en op het feit dat het afsluiten voor dergelijke akkoorden ook verplicht zal zijn gelet op de dwingende bepalingen van de bijzondere Wet tot hervorming der instellingen van 8 augustus 1980[39].

16. De Commissie en de Vlaamse Toezichtcommissie hebben, mede hierdoor, nauw samengewerkt. Het is voor de burger van een gewest of land immers moeilijk denkbaar dat de bescherming van persoonsgegevens zou gaan verschillen van het ene gewest tegenover het andere.

17. Dit geldt ook voor de burgers van de Europese Unie. De Commissie is derhalve eveneens voorstander van een Europees tekstvoorstel in deze materie, daar de ITS Richtlijn al bij al te vaag blijft op het gebied van dataprotectie, zoals de EDPS reeds opmerkte[40].

III. INHOUD VAN HET VOORONTWERP

A. Doeleinde van het voorontwerp

18. Het voorontwerp van wet heeft een dubbel doel (artikel 2 voorontwerp). Enerzijds wordt voorzien in een omzetting van de ITS-richtlijn[41]. Anderzijds wil de wetgever een kaderwet creëren *"die ter zake enerzijds de algemene principes uiteenzet en anderzijds verdere*

[38] Zie randnummer 3.
[39] Zie artikel 92 bis, §2, a) van de bijzondere Wet tot hervorming der instellingen van 8 augustus 1980
[40] Zie het voormelde advies van 22 juli 2009.
[41] Algemene toelichting bij het voorontwerp van wet.

aanpassings- en uitvoeringsbepalingen toevertrouwt aan de Koning. Daarnaast is het nuttig om het kader voor een effectieve samenwerking rond en opvolging van de intelligente transportsystemen te organiseren. Naast de verschillende federale overheidsdiensten zijn hierbij immers nog verschillende andere actoren betrokken."[42]

19. Hiertoe worden volgende maatregelen ingevoerd:
    - Invoering van relevante definities betreffende ITS (Hoofdstuk II, artikel 3);
    - toepassingsgebied van de wet op ITS toepassingen en ITS diensten (hoofdstuk III, artikel 4);
    - de afbakening van prioritaire ontwikkelings- en toepassingsgebieden (hoofdstuk IV, artikelen 5 tem 6);
    - bescherming van grondrechten (Hoofdstuk V, artikel 7);
    - aansprakelijkheidsregeling (Hoofdstuk VI, artikel 8);
    - Machtiging aan de Koning om federale wetten aan te vullen, op te heffen of te vervangen om ze in overeenstemming te brengen met de vereisten inzake ITS (Hoofdstuk VII, artikel 9 tem 11);
    - (uitvoering van) samenwerking inzake ITS door federale overheid (Hoofdstuk VIII, artikel 12);
    - Uitvoerings- en slotbepalingen (Hoofdstuk IX, artikelen 13 tem 15).

20. Vooral de Hoofdstukken V en VII (artikelen 7 en 9 tem 11) blijken van belang voor de toepassing van de WVP.

21. Het artikel 7 luidt als volgt :

    "§1. Geen bepaling van deze wet doet afbreuk aan de wettelijke en reglementaire beschermingsmechanismen inzake verwerking van persoonsgegevens, beveiliging en hergebruik van informatie.
    §2. Ingeval van conflict en/of tegenstrijdigheid tussen de in §1 bedoelde gelijktijdig toepasselijke wetgevende beschermingsmechanismen wordt in het kader van ITS steeds voorrang gegeven aan de wetgevende bepalingen die de ITS gebruiker ter zake de ruimste rechtsbescherming bieden"

[42] Algemene toelichting bij het voorontwerp van wet.

B. Verwerkte gegevens

22. Het voorontwerp biedt onvoldoende zicht op de vraag welke persoonsgegevens zullen (kunnen) worden verwerkt in de beoogde ITS systemen. Een verwijzing naar dataminimalisering is niet aanwezig in het voorontwerp.

23. De overweging 12 bij de ITS Richtlijn stelt *"Bij ITS- toepassingen dienen onder meer de beginselen van doelbeperking en gegevensminimalisering te worden toegepast op ITS-toepassingen."*

24. Artikel 10.3 van de ITS Richtlijn legt uit wat wordt bedoeld met "gegevensminimalisering" door te stellen dat persoonsgegevens alleen worden verwerkt *"indien dergelijke verwerking noodzakelijk is voor de ITS-toepassingen en –diensten."* (zie hierna randnummer 53).

25. Het is reeds duidelijk dat ITS betrekking kan hebben op de meest uiteenlopende persoonsgegevens die zullen afhangen van (de architectuur van) het concrete systeem en de mogelijke applicaties. De vraag welke granulariteit van de gegevens wordt verwerkt, hetzij door keuze van de gebruiker, hetzij standaard ingebouwd in het systeem (of eventueel gebruikt naargelang de applicatie) zal ook een impact hebben.

26. Toepassing van het vaak genoemde beginsel van gegevensbescherming door ontwerp (ook ingebouwde privacy of "privacy by design" genoemd[43]) is op dat vlak een aandachtspunt dat de wetgever had kunnen aanhalen, uiteraard rekening houdend met de tenuitvoerleggingskosten van elk systeem en project.

27. De Commissie plaatst anderzijds toch een voorbehoud bij het lanceren van het "beginsel" van gegevens- of dataminimalisering dat als dusdanig niet in de Richtlijn 95/46/EG vermeld staat. Zij is van oordeel dat de wetgever voorzichtig dient te zijn bij het lanceren van nieuwe "beginselen" en acht dat het niet expliciet vermelden van dataminimalisering in het voorontwerp geen probleem hoeft te zijn. Een toepassing van het proportionaliteitsbeginsel is volgens de Commissie reeds voldoende (zie hierna onder punt F).

28. De Commissie wijst er wel op dat elk concreet systeem en elke toepassing wel specifieke vragen zal oproepen qua proportionaliteit (zie hierna), die steeds geval per geval zullen moeten worden beoordeeld. De Commissie wenst dat zij hierbij steeds haar wettelijk voorziene rol als onafhankelijk adviseur en toezichthouder ten volle kan spelen (artikelen 29 en volgende WVP). Zij verzoekt derhalve dat de ITS-kaderwet expliciet voorziet dat haar

[43] Zie voor een definitie het tekstvoorstel in bijlage bij dit advies, en punt III.1 van het advies van 22 juli 2009 van de EDPS.

advies verplicht moet worden aangevraagd voor elk publiek of privaat ITS systeem of project via hetwelk (gevoelige) persoonsgegevens in de zin van artikel 6, 7 of 8 WVP worden verwerkt, wanneer uit de toepassing of diensten een besluit volgt waaraan voor een persoon rechtsgevolgen verbonden zijn of een besluit dat hem in aanmerkelijke mate treft, of dat bestemd is om bepaalde aspecten van zijn persoonlijkheid te evalueren, of waarbij persoonsgegevens worden verwerkt zonder de (vrije en specifieke) toestemming van de betrokkene.

29. De Commissie wijst er verder op dat de verwerking van locatiegegevens bijzonder delicaat is en reeds wettelijk geregeld is[44]: *"Aangezien de locatiegegevens naar de identificatie van een natuurlijk persoon op een bepaalde plek verwijzen, is de verwerking van de persoonsgegevens bijzonder delicaat, omdat die verwerking een schending van de individuele vrijheden met zich kan brengen (de vrijheid om anoniem te komen en te gaan, het recht op het respect voor de persoonlijke en familiale levenssfeer, ...)"*[45].

30. Bij het opnemen van gebeurtenissen in voertuigen voor veiligheidssystemen (zgn. "Event Data Recorder" of "EDR") kunnen bvb gegevens worden verwerkt zoals de technische status van het voertuig (brandstofverbruik,…); het ogenblik van een ongeval en het dynamische gedrag van de bestuurder (bvb druk remolie bij het begin en het einde van het remmen, snelheid van het voertuig ook tijdens het afremmen, snelheid van de motor, al dan niet gebruik van veiligheidsgordels, toerental percentage,…).

31. De Commissie wijst er op dat de verwerking van dergelijke gegevens een verwerking van profielgegevens kan uitmaken die het gedrag van een betrokkene op gedetailleerde wijze in kaart kunnen brengen. De betrokken aanbieders van dergelijke ITS systemen en diensten dienen maatregelen te nemen tot bescherming van de betrokkenen tegen dergelijke inkijkoperaties, zoals reeds vastgelegd in het Europese recht[46].

---

[44] Zie hierna bij de verwijzingen naar de artikelen 122 en 123 van de wet van 13 juni 2005 betreffende de elektronische communicatie.

[45] Senaat, Toelichting bij het Wetgevingsstuk nr. 3-1856/1 betreffende het Wetsvoorstel tot wijziging van de wet van 13 juni 2005 betreffende de elektronische communicatie, teneinde de persoonlijke levenssfeer beter te beschermen in het kader van de op locatiegegevens gebaseerde diensten of de locatiediensten via mobiele telefoon, gepubliceerd op http://www.senate.be/www/?MIval=/publications/viewPub&COLL=S&LEG=3&NR=1856&PUID=50335286&LANG=nl. ,

[46] Zie de Aanbeveling CM/Rec(2010)13 van 23 november 2010 van de Raad van Ministers over de bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens in de context van profilering, gepubliceerd op https://wcd.coe.int/wcd/ViewDoc.jsp?Ref=CM/Rec(2010)13&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864. Zie de explanatory memorandum gepubliceerd op https://wcd.coe.int/wcd/ViewDoc.jsp?id=1693029&Site=CM

IV. ALGEMEEN ONDERZOEK

A. Toepasselijkheid van de WVP

32. *Intelligente vervoerssystemen zijn gebaseerd op het verzamelen, verwerken en uitwisselen van zeer diverse gegevens, zowel uit publieke als particuliere bronnen; en zijn dan ook data-intensief"*[47], aldus de EDPS. De invoering van ITS zal, volgens de EDPS, *"in ruime mate berusten op geolocatietechnologieën, zoals technologieën voor plaatsbepaling via satelliet, en contactloze technologieën, zoals RFID, die de levering van diverse openbare en/of commerciële locatiegebaseerde diensten (bijv. real-time verkeersinformatie, eFreight, eCall, eToll, reserveren van parkeerplaatsen) zullen vergemakkelijken. Sommige van de gegevens die door middel van ITS zullen worden verwerkt, zijn gebundeld — zoals gegevens betreffende het verkeer, ongevallen en opportuniteiten — en hebben geen betrekking op individuele personen, terwijl andere gegevens verband houden met geïdentificeerde of identificeerbare personen en derhalve worden aangemerkt als persoonsgegevens in de zin van artikel 2, onder a), van Richtlijn 95/46/EG".*

33. De Groep 29 en de Commissie hebben reeds een aantal adviezen uitgebracht die betrekking hebben op relevante technologieën zoals geolocatie[48], RFID[49], ….

34. Het voorontwerp van wet betreft derhalve verwerkingen van persoonsgegevens en valt daarmee binnen het toepassingsveld van de Richtlijn 95/46/EG en de WVP. Dit betekent dat de diverse verantwoordelijken voor de verwerking een aantal principes van de WVP zullen moeten naleven (zie hierna).

B. Toepasselijkheid van de Wet elektronische Communicatie

35. Bepaalde vormen van ITS maken gebruik van een openbaar telecommunicatienetwerk[50], waarbij de Wet van 13 Juni 2005 betreffende de elektronische communicatie van toepassing kan zijn op dergelijke systemen en toepassingen. Toch is het toepassingsgebied van de Wet

---

[47] Zie punt 8 van voormeld advies van de EDPS

[48] Zie het advies 12 / 2005 van 7 september 2005 betreffende het Wetsvoorstel tot regeling van het toezicht op werknemers door middel van een monitoringsysteem verbonden met het GPS-navigatiesysteem van dienstwagens, overeenkomstig de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van de persoonsgegevens, gepubliceerd op http://www.privacycommission.be/sites/privacycommission/files/documents/advies_12_2005_0.pdf.
Zie het advies WP 185 van de Groep 29 van 16 mei 2011 over geolocatiediensten op slimme mobiele apparaten, gepublcieerd op http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_nl.pdf

[49] Advies uit eigen beweging 27/2009 van 14 oktober 2009 inzake RFID, gepubliceerd op http://www.privacycommission.be/sites/privacycommission/files/documents/advies_27_2009_0.pdf
Zie het advies van de Groep 29 WP 180 van 11 februari 2011 betreffende het herziene voorstel van de industrie voor een effectbeoordelingskader wat betreft de bescherming van de persoonlijke levenssfeer en persoonsgegevens bij RFID-toepassingen, gepubliceerd op http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_nl.pdf

[50] Zie punt 2 "Hoe werkt eCall" in voormeld werkdocument WP 125 van de Groep 29.

van 13 juni 2005 beperkt tot de publieke elektronische communicatienetwerken en-diensten, waardoor de bescherming van de Wet van 13 Juni 2005 vaak niet van toepassing zal zijn. Dit is het geval als actoren die geolocatiediensten aanbieden geen operator zijn (bvb fabrikanten van GPS systemen) en als het gaat om locatiediensten en -applicaties die op basis van een combinatie van basisstation-, Wifi- en gps-gegevens worden aangeboden (zogenaamde "diensten van de informatiemaatschappij" zijn geen "elektronische communicatiediensten"[51] en worden dus niet beschermd door de Wet van 13 juni 2005). Indien de Wet van 13 juni 2005 niet van toepassing is, blijven de beschermingsmaatregelen van de WVP echter van kracht.

C. Onderzoek van artikel 7 van de ITS-kaderwet

36. De Commissie acht het niet voldoende om in artikel 7 van de ITS-kaderwet te stellen " *Geen bepaling van deze wet doet afbreuk aan de wettelijke en reglementaire beschermingsmechanismen inzake verwerking van persoonsgegevens, beveiliging en hergebruik van informatie (…)".* Niet alleen moeten de ITS-kaderwet maar ook de ITS-systemen, toepassingen en –diensten conform de (elektronische-) privacywetgeving zijn. Artikel 10 van de ITS-richtlijn stelt trouwens dat *"de verwerking van persoonsgegevens in de context van de exploitatie van ITS-toepassingen en –diensten"* (moet worden) *"uitgevoerd overeenkomstig de uniale regelgeving ter bescherming van de fundamentele rechten en vrijheden van het individu, met name de Richtlijn 95/46/EG en Richtlijn 2002/58/EG.* "

37. De Commissie stelt toch vast dat de ITS-richtlijn duidelijk en expliciet de toepasselijkheid van de Richtlijn 2002/58/EG bevestigt[52], waar het voorontwerp van wet dergelijke duidelijke verwijzing niet bevat. In de Memorie van Toelichting m.b.t. artikel 7 van het voorontwerp lezen we enkel *"In §1 wordt het door artikel 10 van de ITS-richtiijn vereiste minimumbeschermingsniveau inzake verwerking van persoonsgegevens, beveiliging en hergebruik van informatie gegarandeerd."*

38. Bij analogie naar de ITS-richtlijn verzoekt de Commissie de wetgever duidelijker de verwijzing naar de WVP en de reglementering inzake elektronische communicatie op te nemen in de Memorie van Toelichting en in artikel 10 van het voorontwerp van wet.

---

[51] Zie punt 4.2.1. van het advies 13/2011 over geolocatiediensten op slimme mobiele apparaten gepubliceerd op http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_nl.pdf

[52] Zie overweging 12 en 13 van de ITS-richtlijn, en artikel 10 van de ITS-richtlijn.

D. Het beginsel van een gerechtvaardigde verwerking

39. Artikel 5 van de WVP vermeldt vijf gevallen waaronder een verwerking van persoonsgegevens mag worden verricht.

40. De EDPS stelde[53] *"Het is niet duidelijk wanneer de verwerking van persoonsgegevens van start zal gaan als de ITS-apparatuur eenmaal in een voertuig is ingebouwd, en op welke rechtsgrondslag de verwerking zal plaatsvinden. De operatoren kunnen zich voor de gegevensverwerking op verschillende rechtsgrondslagen baseren, onder meer de ondubbelzinnige toestemming van de gebruikers, een overeenkomst of een juridische verplichting die de verantwoordelijke voor de verwerking moet nakomen. De rechtsgrondslag waarop de verwerking van gegevens via ITS plaatsvindt, moet worden geharmoniseerd om te waarborgen dat de systemen in geheel Europa werken en dat de gebruikers geen nadeel ondervinden van verschillen in de manier waarop de verwerking per lidstaat gebeurt."*

41. Meer aandacht gaat intussen op Europees vlak naar het voorhanden zijn van de juiste legitimiteitsbasis voor elke applicatie[54].

42. In zoverre het gaat om verwerkingen van persoonsgegevens die kunnen worden gekaderd onder artikel 12, dit wil zeggen de (uitvoering van) samenwerking inzake ITS door federale overheid, kan worden verwezen naar artikel 5 e) WVP (de vervulling van een taak van openbaar belang of een taak die deel uitmaakt van de uitoefening van het openbaar gezag, die aan de verantwoordelijke voor de verwerking werd opgedragen).

43. Niet alle systemen en toepassingen zullen evenwel verplicht worden uitgerold. Commerciële, niet-verplichte toepassingen door derden vergen een andere legitimiteitsbasis zoals toestemming van de betrokkene (artikel 5 a) WVP), de noodzaak om een overeenkomst uit te voeren (artikel 5 b) WVP), of een situatie waarbij er sprake is van een afgewogen belang (artikel 5 f) WVP).

44. In een aantal gevallen zal de toestemming van de abonnee reeds wettelijk vereist zijn, zoals bij ITS systemen en applicaties die locatiegegevens[55] verwerken via openbare telecommunicatienetwerken, door een elektronische communicatiedienst van een operator ("hotspot applicaties" in de wagen). Een groot aantal ITS toepassingen zullen hier niet onder vallen als "dienst van de informatiemaatschappij".

---

[53] Zie randnummer 16 van het advies van de EDPS.
[54] Element van de in randnummer 3 vermelde studie die 10 ITS toepassingen selecteerde.
[55] Zie hierna bij de verwijzing naar artikel 9 van Richtlijn 2002/58/EG en de artikelen 122 en 123 van de wet van 13 juni 2005 betreffende de elektronische communicatie.

45. Net als de EDPS[56] en zoals in de sector van slimme meters steunt de Commissie toch de voorkeursoptie om de overige ITS-diensten aangeboden door private actoren enkel op vrijwillige basis aan te bieden. De wetgever zou op dat vlak expliciet kunnen bepalen dat "gebruikers vrijelijk moeten kunnen instemmen met het gebruik van het systeem en met de specifieke doeleinden waarvoor het zal worden gebruikt", bvb als het gaat om lokatiegegevens verwerkt via satellietnavigatie.

46. De Commissie wenst dat de wetgever voorziet dat het begrip toestemming voor de overige ITS-diensten moet worden begrepen conform de laatste evolutie in het dataprotectierecht, dat evolueert[57] in de richting van een vereiste van expliciete, specifieke wilsuiting die gebaseerd is voorafgaande afdoende duidelijke informatie (dus geen impliciete toestemming).

47. Verder impliceert dergelijke keuze voor de "toestemming" van de betrokkene als rechtsbasis (bvb bij geavanceerde dienstverleningen door autoverhuurbedrijven) dat het systeem vlot moet kunnen worden in- en uitgeschakeld door de gebruiker, zonder externe druk of nadelige gevolgen voor de betrokkene bij uitschakeling (bvb hogere kosten of extra inspanningen)[58] (zie de definitie van toestemming in artikel 1 § 8 WVP en de nadruk op het voorzien van een herroepbare toestemming). Een observatie in dat verband is dat diensten vaak starten als een vrijwillige optie, maar ontwikkelen zich gaandeweg als een situatie waar geen echt alternatief bestaat door de inferieure kwaliteit van de "verouderde", klassieke dienstverlening (bvb e-ticketing inzake openbaar vervoer waar de klassieke, "papieren optie" duurder en omslachtiger wordt of zelfs verdwijnt). De financiële sector (de klassieke overschrijving op papier vs. via e-banking) bevat wat dat betreft reeds precedenten.

48. Gebruik van de vrije toestemming van de betrokkene zal ook niet voor alle ITS toepassingen evident zijn. Toestemming is verder niet vereist bij vrijwaring van een vitaal belang van de betrokkene (artikel 5 d) WVP), die als rechtsbasis voor sommige ITS toepassingen zal kunnen worden aangewend.

---

[56] Zie randnummer 18 van het advies van de EDPS
[57] Zie het voorstel van Europese Dataprotectieverordening van de Europese Commissie van 25 januari 2012, gepubliceerd op http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_nl.pdf
[58] Zie pagina 4 punt 3.1. van het werkdocument WP 125 van de groep 29.

E. Het finaliteitsbeginsel

49. Het finaliteitsbeginsel werd vastgelegd in artikel 4 van de WVP, die de verantwoordelijke voor de verwerking verplicht enkel gegevens te verzamelen voor welbepaalde, uitdrukkelijke en gerechtvaardigde doeleinden en die verzamelde gegevens slechts te verwerken op een wijze die verenigbaar is met deze doeleinden.

50. De richtlijn maar ook het voorontwerp van wet tot omzetting van de richtlijn, streven algemene beleidsdoeleinden na (zie supra randnummers 3, 5 en 6) die met de invoering van ITS worden nagestreefd.

51. Het is duidelijk dat de kaderwet, net als het Actieplan van de Europese Commissie voor de periode 2009-2014 en de ITS-richtlijn zich beperken tot het bepalen van zeer algemene beleidsdoeleinden en prioritaire gebieden. Hierbij was het niet meteen de opzet om alle concrete gebruiksdoeleinden van persoonsgegevens te bepalen. Toch ziet de Commissie zich genoodzaakt om, in navolging van de EDPS[59], reeds de plicht van de actoren te herhalen om de concrete gebruiksdoeleinden te bepalen (artikel 4 § 1, 2° WVP en 22 Grondwet). Het bepalen van precieze gebruiksdoelstellingen is immers een essentieel onderdeel van de reglementering op de bescherming van persoonsgegevens[60].

52. Het voorgestelde wetgevingskader is inderdaad voorlopig *"te breed en te algemeen (…) om de problemen inzake privacy en gegevensbescherming waartoe de invoering van ITS (…) aanleiding geeft, adequaat te kunnen aanpakken.(…)."*[61]

53. De kaderwet had wel de actoren minstens kunnen wijzen op de plicht om alle concrete gebruiksdoeleinden van systemen en applicaties duidelijk te omschrijven.

54. Meer aandacht dient ook te gaan naar het feit dat een het ITS beginsel van compatibiliteit en interoperabiliteit van systemen (artikel 4 § 2 van het voorontwerp) wordt getemperd door het finaliteitsbeginsel vervat in artikel 4 § 1, 2° WVP en de eis tot beveiliging van verwerkingen (artikel 16 WVP). Ongebreidelde compatibiliteit en interoperabiliteit van systemen kan derhalve geen doel op zich zijn, gelet op de risico's die eigen zijn aan "function creep".

---

[59] Zie nummer 21 van voormeld advies van de EDPS
[60] Zie het Advies nr. 45.459 van 14 november 2008 betreffende een voorontwerp van decreet "betreffende het Centraal Referentieadressenbestand" ("CRAB"-decreet), Vl. Parlement, 2008-2009, 2067, gepubliceerd op http://docs.vlaamsparlement.be/docs/stukken/2008-2009/g2067-1.pdf
[61] Zie nummer 14 van voormeld advies van de EDPS

55. Naar analogie met haar aanbeveling inzake slimme meters[62] acht de Commissie het opnieuw van belang dat de wetgever een duidelijker onderscheid oplegt tussen gekende basisdoelstellingen die eigen zijn aan systemen die door de Europese wetgever als prioriteit of verplichting worden ontwikkeld en ondersteund (bvb eCall), systemen die reeds zijn uitgerold en waar de gebruiker vaak geen keuze heeft zoals inzake openbaar vervoer (bvb MOBIB), en daarna de toepassingen die door derden kunnen worden ontwikkeld door potentieel hergebruik van de beschikbare data in bestaande ITS systemen in voertuigen (bvb verzekeringssector) of andere applicaties gebaseerd bovenop de primaire finaliteit van satellietnavigatie (GPS fabrikanten). Dit onderscheid is zowel relevant vanuit de perceptie van de gebruiker als qua reglementaire basis (artikel 4 § 1, 2° WVP)

F. Proportionaliteit

F.1. ITS systemen en toepassingen en artikel 4 WVP § 1, 3° ,anonimisering of pseudonimisering

56. De persoonsgegevens dienen *"ter zake dienend en niet overmatig te zijn uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt"* (artikel 4 § 1, 3° WVP). Wanneer de verantwoordelijke voor de verwerking de middelen voor de verwerking bepaalt, waarmee hij zijn vooropgestelde doeleinde kan verwezenlijken, moet hij er ook over waken dat hij de middelen kiest die het minst het privéleven van de betrokken personen aantasten. Een inmenging in het recht op bescherming van de gegevens van de betrokken personen, moet inderdaad proportioneel zijn ten aanzien van het nut en de noodzaak van de verwerking voor de verantwoordelijke voor de verwerking.

57. Indien bepaalde systemen en basisapplicaties derhalve geen verwerking van persoonsgegevens noodzaken, dient duidelijk te worden bepaald dat er geen nood is aan het verwerken van persoonsgegevens (bvb anoniem reizen per openbaar vervoer blijft behouden op dezelfde voet als het niet-anoniem reizen). De Commissie merkt in dit kader op dat de wetgever artikel 10.3 van de ITS-richtlijn niet omzet. Dit artikel legt de lidstaten op om, waar passend, het gebruik van anonieme gegevens voor de ITS-toepassingen aan te moedigen. Overweging 13 van de ITS richtlijn stelt ook heel duidelijk *"Anonimisering moet worden aangemoedigd als een van de beginselen om de persoonlijke levenssfeer sterker af te schermen".*

---

[62] Zie randnummers 31 en volgende van de aanbeveling 04/2011 van 15 juni 2011, gepubliceerd op http://www.privacycommission.be/sites/privacycommission/files/documents/aanbeveling_04_2011_0.pdf.

58. De Commissie is van oordeel dat het voorontwerp de ITS-richtlijn op dat punt dient uit te voeren, of minstens de logica van artikel 10.3 van de ITS-richtlijn dient om te zetten.

59. Ter herinnering wijst de Commissie er op dat "anonieme gegevens" strikt is gedefinieerd in artikel 1, 5° van het K.B. van 13 februari 2001. Ook zal het niet altijd mogelijk en wenselijk zijn om echte anonimisering te garanderen voor bepaalde ITS basisapplicaties (bvb E-Call). In dat geval zal pseudonimisering een meer aangewezen keuze zijn[63].

F.2. Bewaringsmechanisme en wissen van gegevens.

60. Krachtens artikel 4, §1, 5 van de WVP mag de bewaartermijn van de verwerkte gegevens niet langer zijn dat de tijd die noodzakelijk is om de doeleinden te verwezenlijken waarvoor de gegevens werden verkregen.

61. Gelet op de complexiteit van veel ITS systemen en toepassingen zal het vastleggen van een eenvoudige bewaringstermijn van gegevens niet altijd evident zijn (bvb wissen van gegevens na facturatie bij E-tollsystemen).

62. Voor de gegevens die worden verwerkt en die tussen de bevoegde actoren worden uitgewisseld, dient minstens een bewaringsbeleid te worden bepaald, dat voor de diverse toepassingen elementen bevat zoals de relevante bewaringstermijnen van de gegevens (of berekeningsmethodes om de vereiste bewaringstermijn te berekenen in functie van relevante factoren), de bewaringsmodaliteiten qua vorm (bvb bewaring in anonieme of gecodeerde vorm al dan niet via pseudoniem of andere methode), de plaats van opslag (centrale opslag, lokale opslag zoals in de wagen of bij bepaalde actoren, of een combinatie hiervan), de methodes van en het interne toezicht op schrapping van verouderde of irrelevant geworden gegevens,….

[63] Zie bij analogie de mededeling van de Europese Commissie COM(2007) 228 definitief van 2 mei 2007 inzake de verbetering van de gegevensbescherming door technologieën ter bevordering van de persoonlijke levenssfeer, gepubliceerd op http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:NL:PDF. In deze mededeling worden duidelijk de maatregelen omschreven om de verwerking van persoonsgegevens zoveel mogelijk te beperken en waar mogelijk gebruik te maken van anonieme of pseudonieme data, meer bepaald door de ontwikkeling van technologieën ter bevordering van de persoonlijke levenssfeer te ondersteunen en deze technologieën door de voor de verwerking van persoonsgegevens verantwoordelijken en door particulieren te doen gebruiken.

F.3. Verwerking van lokatiegegevens

63. Er dient over gewaakt te worden dat er geen permanente registratie is van lokatiegegevens, en dat volgsystemen hetzij op een hoge granulariteit kunnen worden geplaatst, hetzij worden uitgeschakeld voor alle verwerkingen die niet gebaseerd zijn op een wettelijke of reglementaire verplichting (artikel 5 c) WVP), of een taak van openbaar belang (artikel 5 e) WVP).

G. Verantwoordelijke(n) voor de verwerking(en)

64. Het voorontwerp bevat geen expliciete regeling tot aanwijzing van de verantwoordelijke(n) voor de verwerking(en) of rolverdeling (artikel 1 § 4 WVP) in de context van al dan niet coöperatieve ITS systemen en applicaties. Dit is een pijnpunt voor de naleving van de WVP, want vaak zal het niet duidelijk zijn *"wat de rol en verantwoordelijkheden zijn van de verschillende operatoren in de ITS-toepassingsketen en het is dus moeilijk om te weten welke operatoren verantwoordelijk zullen zijn voor de verwerking en dus ook voor het nakomen van de verplichtingen inzake gegevensbescherming. Indien al deze punten niet worden verduidelijkt in de wetgeving, zullen de ITS-operatoren met grote problemen te kampen krijgen, aangezien zij uiteindelijk degenen zijn die de in de voorgestelde richtlijn vervatte maatregelen moeten toepassen."*[64]

65. ITS systemen en applicaties van coöperatieve aard zullen sowieso de tussenkomst van diverse actoren impliceren[65] zoals de ontwikkelaar en leverancier van het systeem, de leverancier van besturingssysteem en bepaalde applicaties, de data integrator,… , Zodoende zal voor elk systeem en project een zeer duidelijk antwoord voorhanden moeten zijn op de vraag wie de verantwoordelijke is voor welke verwerking(en). Dit is cruciaal wil men de WVP naleven.

66. De Commissie acht het aangewezen om een centraal aanspreekpunt (zgn " single point of contact") per systeem te voorzien, waarbij de betrokkenen zich kunnen aanmelden om hun rechten van toegang, verbetering, verzet en schrapping enz… uit te oefenen.

---

[64] Zie punt 14 van het advies van de EDPS.

[65] Bij MOBIB is voor het beheer sprake van een consortium van THV Prodata Systems, Prodata Mobility Systems Fabricom GDF Suez (bron : http://www.mobimix.be/inhoud/2011/8/18/2574), naast de gekende vervoersmaatschappijen (De Lijn, MIVB, TEC en NMBS)

67. Dit staat overigens los van de algemene kwestie van de juridische aansprakelijkheid van elke actor die op basis van de algemene burgerlijke zorgvuldigheidsverplichting systemen de recentste evolutie van het europese dataprotectierecht zal dienen op te volgen. Hierbij zal rekening moeten worden gehouden met de beginselen van veiligheid, een afdoende hoog beschermingsniveau voor de betrokkenen via ingebouwde privacy (zgn. "privacy by design")[66] en gegevensbescherming door standaardinstellingen ("privacy by default")[67].

68. In navolging van andere dossiers (bvb IMI, slimme meters…) had de wetgever meer algemeen de aandacht kunnen vestigen op dit aspect, door bijvoorbeeld volgende verwijzing op te nemen : *"de toewijzing van verschillende verantwoordelijkheden aan de overheden en actoren dient te worden verricht conform de WVP."*

H. Transparantiebeginsel en informatieplicht aan de betrokken personen

69. De informatieplicht van de verantwoordelijke voor de verwerking is een van de basisverplichtingen onder de WVP (artikel 9 WVP). Er bleek reeds uit de buurlanden dat een probleem van perceptie en maatschappelijke aanvaarding van ITS systemen en toepassingen kan ontstaan. Daardoor wordt de wetgever best aangemoedigd om een nog ruimere sensibilisering en informatie aan het grote publiek te voorzien dan omschreven in artikel 9 WVP.

70. Artikel 9 van de WVP verplicht iedere verantwoordelijke voor de verwerking om de personen van wie de gegevens worden verwerkt in te lichten over de doeleinden van de verwerking, de identiteit van de verantwoordelijke voor de verwerking en de ontvangers (of categorieën ontvangers) van de gegevens evenals het bestaan van een recht op toegang en op verbetering voor de betrokken persoon.

[66] Zie de definitie hierna in het tekstvoorstel
[67] Zie de definitie hierna in het tekstvoorstel

71. Inzake lokalisatiegegevens laat het voorontwerp na om enige verwijzing te maken naar de bijzondere informatieverplichting in toepassing van artikel 9 van Richtlijn 2002/58/EG[68].

72. De ITS projecten waarmee het grote publiek mee in aanraking is gekomen (vooral het openbaar vervoer[69]) kregen de afgelopen jaren bijna steeds negatieve media-aandacht[70] door (al dan niet[71] vermeende) privacyproblemen. Zo lijkt het "bon ton" om elke e-ticketing ETS applicatie te "bedanken" met een "Big Brother Award". Passende nadruk door de wetgever om meer transparantie naar de gebruikers aan te moedigen in de meest ruime zin is derhalve van groot belang, ook inzake de relevante informatie die strikt genomen niet vermeld staat in artikel 9 WVP maar die van aard is om het vertrouwen en de acceptatie van de gebruikers met deze nieuwe toepassingen aan te moedigen.

73. Het is raadzaam dat een ruimere informatieverstrekking wordt verplicht die de Koning (eventueel via gedragscodes) voorafgaand zou kunnen aanmoedigen voor systemen en applicaties. Elementen van deze ruimere informatieverstrekking kunnen zijn :
    - het toepasselijke recht (gelet op de Europese mobiliteit van ingebouwde ITS systemen in personenwagens);
    - de verwerkte persoonsgegevens (vermelding welke gegevens niet worden verwerkt, of er sprake is van anonimisering of pseudonimisering. Niet voor elke applicatie zal opslag in het systeem van het gedetailleerd mobiliteitspatroon van de betrokkene vereist zijn. Inzake Etoll systemen kunnen actoren steeds op de belangstelling rekenen van de politie- en veiligheidsdiensten, wat tot onnodige vragen leidt indien het systeem niet is ontwikkeld om bepaalde data op te slaan. De betrokken moet weten of gedragsmatige aspecten in kaart wordt gebracht (bvb risicovol rijgedrag)

---

[68] *"Wanneer andere locatiegegevens dan verkeersgegevens die betrekking hebben op gebruikers of abonnees van elektronische- communicatienetwerken of -diensten verwerkt kunnen worden, mogen deze gegevens slechts worden verwerkt wanneer zij anoniem zijn gemaakt of wanneer de gebruikers of abonnees daarvoor hun toestemming hebben gegeven, voorzover en voor zolang zulks nodig is voor de levering van een dienst met toegevoegde waarde. De dienstenaanbieder moet de gebruikers of abonnees, voorafgaand aan het verkrijgen van hun toestemming, in kennis stellen van de soort locatiegegevens anders dan verkeersgegevens, die zullen worden verwerkt, en van de doeleinden en de duur van die verwerking, en hun meedelen of deze gegevens aan een derde zullen worden doorgegeven*
ten behoeve van de levering van de dienst met toegevoegde waarde. Gebruikers of abonnees kunnen hun toestemming voor de verwerking van andere locatiegegevens dan verkeersgegevens te allen tijde intrekken.
2. Wanneer de gebruikers of abonnees toestemming hebben gegeven voor de verwerking van andere locatiegegevens dan verkeersgegevens, moet de gebruiker of abonnee de mogelijkheid behouden om op eenvoudige en kosteloze wijze tijdelijk de verwerking van dergelijke gegevens te weigeren voor elke verbinding met het netwerk of voor elke transmissie van communicatie.
3. De verwerking van locatiegegevens anders dan verkeersgegevens in overeenstemming met de leden 1 en 2, moet worden beperkt tot personen die werkzaam zijn onder het gezag van de aanbieder van het openbare elektronische-communicatienetwerk of de openbare elektronische-communicatiedienst of de derde die de dienst met toegevoegde waarde levert, en moet beperkt blijven tot hetgeen noodzakelijk is om de dienst met toegevoegde waarde te kunnen aanbieden."

[69] Zie de pers inzake de Nederlandse chipkaart, MOBIB in België en NAVIGO in Frankrijk.

[70] Zie een "Big Brother award" voor NAVIGO in Frankrijk (http://bigbrotherawards.eu.org/article646.html), OV-Chip in Nederland (http://www.ov-chipkaart.nl/nieuws/laatstenieuws/big_brother_award) en MOBIB (http://www.brusselnieuws.be/artikel/mivb-krijgt-big-brother-award-voor-mobib-kaart)

[71] Een aantal inbreuken werden reeds door andere privacycommissies vastgesteld zoals door Tomtom (http://www.cbpweb.nl/Pages/pb_20120112_tomtom-geolocatie-persoonsgegevens.aspx)

- de gebruiksdoeleinden (onderscheid basisdoelstellingen van het system van de afgeleide applicaties van derde partijen die een andere basis vereisen zoals toestemming van de betrokkene);
- een omschrijving van wie (geen) toegang heeft tot de gegevens (wordt gebruik beoogd van gegevens met het oog op profilering door derden zoals verzekeringsondernemingen en/of direct marketing van producten door derden die zelf geen vervoersdiensten aanbieden), of wat de garanties zijn in dat verband (zie het recht van verzet in artikel 12 WVP);
- de bewaringstermijn (het dataretentiebeleid of –schema van het systeem eventueel naargelang de uiteenlopende applicaties);
- de wijze van bescherming tegen ongeoorloofde toegang (hacking,…) en de toegang tot de eigen gegevens;
- de wijze van toegang tot zijn eigen gegevens.
- de contactgegevens van de verantwoordelijke voor verdere informatie over de rechten van betrokkene (inzage en verbetering,…)

I. Rechten van toegang en verbetering – centraal aanspreekpunt en internationale samenwerking

74. Gelet op de complexiteit van system en toepassingen wordt het aanbevolen om aan de betrokken personen een eenvoudig en makkelijk beschikbaar mechanisme aan te bieden via een centraal aanspreekpunt (zie hiervoor onder randnummer 57) zodat zij hun rechten van toegang en verbeteringen op vlotte wijze kunnen uitoefenen ten aanzien van de verwerkingen in hun eigen taal.

75. Bovendien vraagt de Commissie dat meer aandacht zou worden gegeven aan de impact van het grensoverschrijdend karakter van bepaalde toepassingen. De wetgever zal dan ook moeten voorzien dat (samenwerkings)mechanismen met andere actoren in het buitenland moeten worden ingesteld om burgers in hun eigen taal te helpen bij eventuele vragen van toegang, verbetering,... wanneer grensoverschrijdende problemen worden veroorzaakt (of enkel zich stellen) door data uit het buitenland[72]. Het voorzien van een nationaal centraal aanspreekpunt door de diverse verantwoordelijken zou in dat geval de burger in eigen taal dienen te helpen in plaats van de betrokkene door te verwijzen.

[72] Bijvoorbeeld indien foutieve data zich enkel in het buitenland bevinden en niet in België

J. Veiligheidsbeginsel bij een verwerking

76. Gegevensbescherming- en informatiebeveiligingselementen moeten zijn ingebouwd in ITS voordat zij worden ingevoerd en intensief worden gebruikt. Dergelijke elementen kunnen de controle van de betrokkenen over de verwerking van hun persoonsgegevens versterken, het risico op "function creep" en misbruiken verminderen én minstens de perceptie van een probleem wegnemen.

77. Een van deze maatregelen is het model van lokale opslag (zgn. "distributed processing" of het verdelen van de opslag van gegevens doorheen de ganse ITS-ketting (bvb in de wagen) zodat er geen centrale opslag is van alle ITS data op een plaats bij één actor, maar elke actor slechts een deel heeft van het ganse gedetailleerde mobiliteitspatroon van de betrokkene).

78. De verantwoordelijke voor de verwerking en desgevallend zijn verwerker, moeten de nodige technische en organisatorische veiligheidsmaatregelen[73] nemen om de ITS systemen en de daarmee verwerkte gegevens te beschermen tegen al dan niet toevallige vernietiging, tegen toevallig verlies, alsook tegen wijziging, toegang en iedere andere ongeoorloofde verwerking van persoonsgegevens. Hieromtrent verwijst de Commissie ter informatie naar de door haar opgestelde veiligheidsnormen welke volgens de Commissie, naargelang van geval tot geval, toepasbaar dienen te zijn op een verwerking van persoonsgegevens[74.]

K. Effectbeoordelingen met betrekking tot gegevensbescherming ("Privacy Impact Assessment" of "PIA")

77. De Commissie stelt vast dat bij de roll-out van nieuwe technologieën en systemen het risico bestaat dat verantwoordelijken veel te laat rekening houden met alle gegevensbeschermingsrisico's en de reglementering inzake gegevensbescherming. Privacybescherming via maatregelen zoals effectbeoordelingen (zogenaamde privacy impact assessment of "PIA") met betrekking tot gegevensbescherming of ingebouwde privacy mag niet worden afgedaan als formalisme en/of onnodige maatregelen die enkel de kosten doen oplopen. De Commissie stelt immers vast in de diverse nationale dossiers die haar werden voorgelegd dat indien verantwoordelijken wachten tot na de uitrol van systemen en toepassingen om privacyaanpassingen in te voeren, dit (nog) hogere aanpassingskosten en

[73] Artikel 16 van de WVP
[74] Zie http://www.privacycommission.be/sites/privacycommission/files/documents/01.01.04.05-referentiemaatregelen_voor_de_beveiliging_van_elke_verwerking_van_persoonsgegevens.pdf

reputatieschade tot gevolg heeft. Een Europese studie[75] verricht in 2010 in opdracht van de Europese Commissie in diverse lidstaten bevestigde ook de economische voordelen van het voorzien van ingebouwde privacy, tenminste indien systemen en projecten geval per geval worden beoordeeld[76].

78. Naar geldend recht in de energiesector[77] moet reeds worden voorzien in effectbeoordelingen met betrekking tot gegevensbescherming voor intelligente systemen en applicaties. Dit moeten het mogelijk maken om, rekening houdend met de tenuitvoerleggingskosten, van bij de start van de ontwikkeling van nieuwe systemen de risico's voor de gegevensbescherming zo vroeg als mogelijk (liefst voor de start van het ontwikkelen van de systeemarchitectuur, dus bij de voorafgaande analyse) in te schatten. Zonder deze aanpak komt een efficiënte uitrol van systemen of applicaties vroeg of laat op de helling te staan.

79. De wetgever dient de diverse actoren te verplichten om een effectbeoordeling te verrichten. De Commissie adviseert om hierbij de Koning te belasten met het bepalen van de inhoud van dergelijke effectbeoordeling, op voorwaarde dat het ontwerp Koninklijk besluit aan haar voorafgaand advies wordt voorgelegd. Bij een effectbeoordeling zal men rekening moeten houden met de aard en doelstelling van het systeem en de toepassing, de schaal van toepassing, de al dan niet officiële Europese erkenning van een systeem als prioritair of wettelijke plicht, de verwachte ontwikkelingen van het systeem in de toekomst, de mogelijke diversiteit van applicaties die kunnen worden geënt op een systeem (open[78] of meer gesloten architectuur). Dit alles uiteraard rekening houdend met de tenuitvoerleggingskosten van elk project.

80. Effectbeoordelingen moeten ook tijdig worden verricht. De wetgever dient te voorzien in een verplichting voor alle ITS actoren om teen effectbeoordeling met betrekking tot gegevensbescherming te verrichten op het moment wanneer ITS systemen, diensten of toepassingen worden ontwikkeld. Dit rekening houdend met de tenuitvoerleggingskosten (privacybescherming als onderdeel van een zgn. "kosten-batenanalyse").

---

[75] Zie pagina 7 en volgende van de studie van juli 2010 over de economische voordelen van technologieën ter bevordering van de persoonlijke levenssfeer verricht door London Economics in opdracht van DG Justice, gepubliceerd op http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf

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

[77] Zie Aanbeveling 2012/148/EU van de Europese Commissie van 9 maart 2012 inzake de voorbereiding van de uitrol van slimme metersystemen, gepubliceerd op http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:073:0009:0022:NL:PDF

[78] De verwachting is dat "onboard devices" in wagens meerdere diensten zullen ondersteunen. Dit is minder evident voor andere ITS diensten zoals tolheffing.

81. Tenslotte acht de Commissie het nuttig dat dergelijke effectbeoordelingen steeds ter beschikking worden gehouden van de relevante toezichthouders (Commissie, BIPT,…) en dit reeds tijdens het vroege (analyse)stadium, dit wil zeggen nog voor de start van ontwikkeling van systemen en applicaties . Dit kan desgevallend als bijlage bij een eventuele aangifte (artikel 17 WVP) en/of machtigingsaanvraag van de verantwoordelijke.

L. Uitvoeringsmaatregelen – Wettelijkheidsbeginsel

82. Artikel 9 van het voorontwerp bepaalt dat de Koning wordt gemachtigd om ""*onder de voorwaarden vermeld in dit artikel de federale wetten aan te vullen, op te heffen of te vervangen om ze in overeenstemming te brengen met de vereisten inzake ITS.* "

83. gelet op artikel 22 Grondwet[79] zal deze opdracht aan de Koning onvermijdelijk haar limieten kennen.

M. Uitvoeringsmaatregelen – Beginsel van voorafgaand onderzoek (advies door de Commissie)

84. Omdat uit eerdere adviezen (geolocatie, RFID,…) toch al bleek dat ITS "mogelijk specifieke risico's voor de persoonlijke rechten en vrijheden" inhoudt waarvoor het Europese beginsel van voorafgaand onderzoek geldt[80] verzoekt de Commissie dat alle uitvoeringsmaatregelen in de artikelen 9 tot en met 11 die betrekking hebben op de verwerking van persoonsgegevens steeds worden genomen na verplicht voorafgaand advies van de Commissie (artikel 29 WVP).

85. De artikelen 9 tot en met 11 dienen dienovereenkomstig te worden aangepast.

---

[79] Een delegatie aan een andere macht is niet in strijd met het legaliteitsbeginsel voor zover de machtiging voldoende nauwkeurig is omschreven en betrekking heeft op de tenuitvoerlegging van maatregelen waarvan de essentiële elementen voorafgaandelijk door de wetgever zijn vastgesteld (zie de arresten van het Grondwettelijk Hof nrs. 202/2004 van 21 december 2004, overweging B.6.2, en 29/2010 van 28 maart 2010, overweging B.16.1). Zie ook advies R.v.St. 38.385 van 3 oktober 2005 betreffende een ontwerp van koninklijk besluit "tot regeling van het statuut van de bijzondere veldwachters, gepubliceerd op http://www.emis.vito.be/EMIS/Media/Legislation_Docs/sb240206-1-a.pdf

[80] Artikel 20 Richtlijn 95/46/EG. Bijvoorbeeld als het gaat om systemen en toepassingen die mobiliteitspatronen van personen of voertuigen gedetailleerd of zelfs volledig in kaart brengen

V. BESLUIT

86. De Commissie stelt vast dat er inzake ITS sprake is van sterke analogieën met andere "slimme" systemen en toepassingen ("internet of things"), en aanverwante technologieën en projecten die reeds eerder of elders werden besproken (MOBIB, RFID, geolocsatie,…). Zij adviseert de wetgever rekening te willen houden met de bestaande opinies, standpunten of privacy impact assessments in vergelijkbare domeinen (in het bijzonder inzake slimme meters) op nationaal en Europees vlak.

87. ITS is in feite een "containerbegrip" voor het gebruik van technologieën in en rond "slimme voertuigen" waarvan de risico's voor de bescherming van de persoonlijke levenssfeer eerder, vaak rond deelaspecten, werden toegelicht. Nieuwe, nog onopgeloste kwesties met betrekking tot privacy en gegevensbescherming werden eerder door de Europese Commissie "aangemerkt als één van de voornaamste belemmeringen voor het stimuleren van ITS"[81].

88. Het voorontwerp houdt duidelijk geen rekening met de expliciete Europese bekommernis van het ITS Actieplan en de ITS-richtlijn inzake gegevensbescherming. Het artikel 7 van het voorontwerp ("grondrechtenbescherming") biedt op dat vlak onvoldoende elementen om voormelde kwesties op te lossen ten behoeve van de actoren en betrokkenen. Enerzijds zet het voorontwerp de relevante en expliciete bepalingen inzake privacy en gegevensbescherming van de ITS-Richtlijn niet om (bvb de plicht bij alle systemen en projecten om enkel de gegevens te verwerken die toereikend, ter zake dienend en niet overmatig zijn), en anderzijds moeten niet alleen de ITS-kaderwet maar ook alle ITS-systemen, toepassingen en –diensten conform de (elektronische-) privacywetgeving zijn.

89. De Commissie is van oordeel dat het voorontwerp te abstract is om haar doelstelling van effectieve samenwerking inzake ITS waar te maken. Het voorontwerp behoeft een algemene omkadering op het gebied van gegevensbescherming door verwijzing naar enkele algemene (dataprotectie)beginselen en de evoluerende Europese context sinds 2010[82]. Zonder deze omkadering dreigt de vlotte uitrol van prioritaire Belgische ITS systemen eerder bemoeilijkt te worden in plaats van te worden aangepakt.

90. Ook dient de wetgever oog te hebben voor het feit dat voor elk systeem en toepassing er steeds geval per geval een bijzondere privacyanalyse zal vereist zijn, waarbij de Commissie wenst dat zij in staat wordt gesteld haar wettelijk voorziene advies- en toezichtsrol te vervullen.

---

[81] Zie randnummer 10 advies EDPS.

[82] publicatie van de impact assessment onder het Europese actieplan wordt verwacht in september, negatieve perceptie en media-aandacht van concrete ITS projecten

91. De Commissie achtte verder (in de memorie van toelichting) meer verwijzing naar concrete, reeds gekende systemen en toepassingen gepast (zie de lijst in randnummer 3) om het zeer abstracte en algemene karakter voor de normadressant te temperen en de voorzienbaarheid van de inmengingen van de ITS reglementering ten opzichte van de persoonlijke levenssfeer te verhogen (artikel 8 EVRM).

92. De concrete beginselen en waarborgen waarnaar de wetgever had kunnen verwijzen zijn :
    - De toepasselijkheid van de Wet van 13 juni 2005 inzake elektronische communicatie en de WVP;
    - Het voorhanden zijn van de juiste legitimiteitsbasis naargelang het systeem en de concrete ITS toepassing;
    - De tempering van het Europese beginsel in de ITS Richtlijn van interoperabiliteit door de dataprotectiebeginselen van doelbinding, proportionaliteit en beveiliging van verwerkingen.
    - Het voorzien van het beginsel van anonimisering of pseudonimisering in de ITS kaderwet, zoals opgelegd door de ITS-richtlijn op basis van beginselen van proportionaliteit, ingebouwde privacy ("privacy by design") en de Europese eis tot het voorzien van technologieën ter bevordering van de persoonlijke levenssfeer (zgn. "privacy enhancing technologies" of "PETS")[83]
    - De omschrijving van het bewaringsplicht.
    - Een verplichte rolverdeling als verantwoordelijke of verwerker in de zin van de WVP, zeker bij complexere ITS systemen van coöperatieve aard.
    - Een wettelijke plicht tot ruime sensibilisering en transparantie van de systemen en toepassingen bovenop de informatieverplichting in artikel 9 WVP en de Wet van 13 juni 2005.
    - het ontwikkelen van eenvoudige en makkelijk beschikbare mechanismen voor de betrokkenen om hun rechten van toegang en verbetering uit te oefenen;
    - De wijze van bescherming tegen ongeoorloofde toegang en de toegang tot de eigen gegevens via technische en organisatorische maatregelen om het risico van misbruik te temperen (bvb verdeling van de opslag van gegevens over verschillende locaties zoals bij e-ticketing, betaling van parkeerplaatsen…) ;
    - Het opleggen aan alle ITS actoren om een verplichte effectbeoordelingen met betrekking tot gegevensbescherming ("Privacy Impact Assessment" of "PIA") te maken, op basis van een door Koninklijk besluit bepaald effectbeoordelingsmodel.

[83] Zie aangaande dit begrip de mededeling van de Europese Commissie van 2 mei 2007 aan het Europees Parlement en de Raad inzake de verbetering van de gegevensbescherming door technologieën ter bevordering van de persoonlijke levenssfeer, COM(2007) 228 definitief, gepubliceerd op http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:NL:PDF

- Toepassing van het Europese regel van voorafgaand onderzoek door het voorzien van de adviesplicht over alle ontwerpen van reglementering via de onderwerping van eventuele wetwijzigingen via bijzondere machten aan de Koning of uitvoeringsmaatregelen door de Koning onder de artikelen 9 tot en met 11 aan het voorafgaand advies van de Commissie.

OM DEZE REDENEN,

De Commissie is er zich van bewust dat de Belgische wetgever hier voor een moeilijke opdracht wordt geplaatst. Dit door het feit dat diverse overheden op federaal, regionaal en lokaal vlak bevoegd zijn om de ITS Richtlijn om te zetten en/of de ontwikkeling van ITS systemen en diensten te regelen of ondersteunen. Er is echter ook het gebrek aan voorzienbaarheid wegens het te brede en algemene karakter van de ITS Richtlijn die onvoldoende rekening houdt met de hoge kwaliteitseisen die de Europese en nationale privacyreglementering opleggen aan de wetgevers, dit in een materie waarvan de concrete toepassingen hoge risico's kunnen inhouden voor de bescherming van de persoonlijke levenssfeer.

Gelet op de opmerkingen hierboven, pleit de Commissie voor het afsluiten van samenwerkingsakkoorden in deze materie. Zij brengt in bijlage ook elementen voor een concreet tekstvoorstel uit om het artikel 7 van het voorontwerp van wet te voorzien van een passende algemene omkadering inzake privacy en gegevensbescherming conform het Europese en Belgische privacy en dataprotectierecht. Zij verleent een positief advies mits met dit tekstvoorstel rekening wordt gehouden.

Gelet op het belang van de diverse systemen en toepassingen blijft de Commissie zich ter beschikking houden bij eventueel verder overleg over ITS systemen of toepassingen, en bij herziening en/of uitvoering van de bepalingen van het voorontwerp.

De Wnd. Administrateur, De Voorzitter,,

(get.) Patrick Van Wouwe (get.) Willem Debeuckelaere

TEKSTVOORSTEL

Artikel 3 Definities

Tekstvoorstel	Memorie van Toelichting
§ 1. (…)	De definities onder 21, 22 en 23 zijn geïnspireerd op bestaande Europese definities in de aanbeveling 2012/148/EU van de Europese Commissie van 9 maart 2012 inzake de voorbereiding van de uitrol van slimme metersystemen. Zij kunnen bij analogie worden toegepast.
21. "effectbeoordeling met betrekking tot de gegevensbescherming": een systematisch proces voor de evaluatie van de potentiële effecten en van risico's voor de rechten en vrijheden van de betrokkenen; meer bepaald door de aard van de verwerkingen van persoonsgegevens, hun bereik of hun doeleinden;	21. Bij de ontwikkeling van slimme vervoerssystemen moet veel aandacht gaan naar de beveiliging en bescherming van daarin verwerkte persoonsgegevens. Conform de laatste evolutie in het Europese recht inzake gegevensbescherming moet effectbeoordeling met betrekking tot gegevensbescherming het mogelijk maken om van bij de start van de ontwikkeling van slimme systemen de risico's voor de gegevensbescherming in te schatten. De overweging 9 van de aanbeveling van de Europese Commissie van 9 Maart 2012 inzake de voorbereiding van de uitrol van slimme metersystemen legt inmiddels in de energiesector een analoge uitrolplicht op aan de lidstaten. De verplichting is uit te voeren door de voor de verwerking verantwoordelijke of de verwerker, dan wel door de verwerker handelend namens de voor de verwerking verantwoordelijke.
22. „gegevensbescherming door ontwerp": het geheel van passende technieken en organisatorische maatregelen en procedures van	22. De definitie onder punt 22 heeft betrekking op wat men in het jargon "privacy by design" noemt. Hierbij is volgens een Europese

concept, over uitvoering tot evaluatie, om te voldoen aan de eisen van wet-en regelgeving ter bescherming van de rechten en vrijheden van de betrokkenen met betrekking tot privacy en de bescherming van persoonsgegevens.	definitie[84] sprake van de tenuitvoerlegging — op basis van moderne technologie en rekening houdend met de tenuitvoerleggingskosten, zowel op het moment dat de verwerkingsmethodologie wordt vastgelegd als op het tijdstip van de verwerking zelf — van passende technische en organisatorische maatregelen en procedures, zodat de verwerking voldoet aan de eisen van Richtlijn 95/46/EG en de Wet van 8 december 1992. De tekst komt ook overeen met artikel 16 § 4 tweede lid van de Wet van 8 december 1992 die gelijkaardige elementen bevat[85] qua stand van de techniek en de betreffende kosten.
23. „gegevensbescherming door standaardinstellingen": de verplichting om de best mogelijke gegevensbescherming als standaard aan te bieden zonder dat de betrokkene zelf moet optreden.	23. Wat men doorgaans "Privacy by default" noemt bevat de tenuitvoerlegging van mechanismen om te waarborgen dat door standaardinstellingen alleen die persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking en dat die gegevens met name niet uitgebreider worden verzameld en langduriger worden bijgehouden dan minimaal vereist is voor die doeleinden, zowel wat de hoeveelheid gegevens als wat de duur van hun opslag betreft;

[84] Deze elementen komen uit artikel 3 van een bestaande aanbeveling van de Europese Commissie in de energiesector. Zie http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:073:0009:0022:NL:PDF

[85] "Deze maatregelen moeten een passend beveiligingsniveau verzekeren, rekening houdend, enerzijds, met de stand van de techniek terzake en de kosten voor het toepassen van de maatregelen en, anderzijds, met de aard van de te beveiligen gegevens en de potentiële risico's."

Artikel 7 Grondrechtenbescherming

Tekstvoorstel	Memorie van Toelichting
§1. Geen bepaling van deze wet doet afbreuk aan de wettelijke en reglementaire bescherming van de persoonlijke levenssfeer en de verwerking van persoonsgegevens.	§1. Dit artikel bevat een concordantieregeling ten opzichte van de diverse wetgevingen inzake bescherming van persoonlijke levenssfeer en de bescherming van persoonsgegevens. Aangezien de wetten van 8 december 1992 en 13 juni 2005 de concretisering inhouden van de internationaal- en supranationaalrechtelijke normen inzake gegevensbescherming wordt deze wet in de eerste plaats getoetst aan de wetten van 8 december 1992 en 13 juni 2005. Bij de redactie werd rekening gehouden met de rechtspraak van het Grondwettelijk Hof inzake artikel 22 Grondwet en de eerdere adviezen van de Raad van State[86] over dit artikel. Uit de parlementaire voorbereiding van de Grondwet[87] bleek reeds dat regionale en/of sectorale regelgeving op basis van het tweede lid van artikel 22 Grondwet meer garanties kan bieden. De wetgeving kan evenwel op basis van artikel 8 EVRM niet minder garanties bieden tenzij in heel specifieke gevallen waar dit zou noodzakelijk blijken en met specifieke basis hiervoor in de wet- of regelgeving. Gedacht kan worden aan toepassing van artikel 3 § 5 van de Wet van 8 december 1992 waardoor de artikelen 9,10 en 12 van de Wet van 8 december 1992 niet van toepassing zouden worden geacht voor verwerkingen die worden verricht met ITS

[86] Zie pagina 90, punten 3.2 en 5 van het Advies nr. 45.459 van 14 november 2008 betreffende een voorontwerp van decreet "betreffende het Centraal Referentieadressenbestand" ("CRAB"-decreet), Vl. Parlement, 2008-2009, 2067, gepubliceerd op http://docs.vlaamsparlement.be/docs/stukken/2008-2009/g2067-1.pdf

[87] Rapport op naam van de Commissie tot herziening van de Grondwet teneinde een nieuw artikel 24quater in te lassen in verband met de bescherming van de persoonlijke levenssfeer, Doc. Parl., kamer, 1993-1994, 1278/2 p 3 en 4, ook geciteerd door Degrave, E., o.c., J.T., 366 voetnoot 6, gepubliceerd op http://www.dekamer.be/FLWB/PDF/48/1278/48K1278002.pdf

	gegevens voor doeleinden van bestuurlijke of gerechtelijke politie.
§2. In geval van tegenstrijdigheid tussen de in §1 bedoelde gelijktijdig toepasselijke wettelijke en reglementaire beschermingsmechanismen wordt in het kader van ITS steeds voorrang gegeven aan de bepalingen die de ITS gebruiker ter zake de ruimste rechtsbescherming bieden.	§2. Er werd ook rekening gehouden met de mogelijkheid om, op regionaal vlak of in CAO's, te voorzien in bijzondere bescherming van de betrokkenen, zonder dat hierbij afbreuk kan worden gemaakt aan de basisbescherming onder de wetten van 8 december 1992 en 13 juni 2005 die zelf de vertaling zijn van het Europese recht inzake privacy- en gegevensbescherming waaronder de Richtlijnen 95/46/EG en 2002/58/EG.
§ 3. Het gebruik van anonieme gegevens, eventueel gecodeerde gegevens, voor de ITS-toepassingen en –diensten wordt voorzien door de ITS-dienstenaanbieders en ontwikkelaars van platformen, architectuur en interfaces.	§ 3. houdt rekening met de vrijheid van elkeen om anoniem te komen en te gaan, vervat in het recht op het respect voor de persoonlijke en familiale levenssfeer (overweging 13 en eerste lid van artikel 10.3 van de Richtlijn 2010/40/EU en de opmerking van de Commissie voor de Bescherming van de persoonlijke levenssfeer inzake artikel 4 § 1, 3° van de wet van 8 december 1992). De begrippen anonieme gegevens en gecodeerde persoonsgegevens worden begrepen in de betekenis van artikel 1, 3° en 5° van het K.B. van 13 februari 2001 ter uitvoering van de wet van 8 december 1992.
§ 4. Er wordt aangeduid wie de verantwoordelijke van de verwerking is voor ITS-toepassingen en –diensten .	§ 4. Bij het invoeren van ITS-toepassingen en –diensten dient men de verantwoordelijkheid onder de wet van 8 december 1992 toe te wijzen in de zin van artikel 1 van de wet van 8 december 1992.
§ 5. Er wordt aangegeven in het interne of externe privacybeleid welke legitimiteitsbasis in de zin van artikel 5 van de wet van 8 december	§ 5. Het voorhanden zijn van een gepaste legitimiteitsbasis in de zin van artikel 5 van de wet van 8 december 1992 voor elke dienst of

1992 voorhanden is voor elke gebruiksdoelstelling van ITS-toepassingen en –diensten.	toepassing is een aandachtspunt. Zo zal de toestemming van de betrokkene voor een aantal private toepassingen wel vereist zijn, maar niet mogelijk of gewenst voor een aantal andere toepassingen die bijvoorbeeld de vervulling van een taak van openbaar belang nastreven.
§ 6. Persoonsgegevens worden enkel verwerkt indien dergelijke verwerking noodzakelijk is voor de ITS-toepassingen en -diensten.	§ 6. is een letterlijke omzetting van het tweede lid van artikel 10.3 van de Richtlijn 2010/40/EU. Deze paragraaf bevat een uitdrukkelijke herhaling van de noodzakelijkheidsvereiste als toetsingscriterium voor de conformiteit van ITS projecten en diensten met artikel 4 § 1 3° van de wet van 8 december 1992. Dit gelet op het risico op een gebrek aan aandacht voor het tijdig schrappen of encoderen van gegevens in toepassingen en diensten waarvan het operationele nut niet langer aanwezig is.
§ 7. Natuurlijke personen mogen niet continu gevolgd worden en moeten een volgsysteem kunnen uitschakelen tenzij wettelijk of contractueel verplicht.	§ 7. Zie randnummer 13 van het advies van de Commissie. Locatietechnologieën worden als bijzonder bedreigend beschouwd voor de privacy en kunnen een schending van de individuele vrijheden inhouden. Het gaat in het bijzonder om de vrijheid om zich anoniem te verplaatsen. Daarom moet de mogelijkheid geboden worden om volgsystemen uit te schakelen zodat de natuurlijke personen niet meer gevolgd worden bijvoorbeeld voor bepaalde toepassingen buiten de werkuren. Er wordt wel een uitzondering voorzien wanneer er een wettelijke verplichting bestaat om ze ingeschakeld te laten of wanneer er een contractuele verplichting bestaat. Wat de contractuele verplichting betreft moet het om een toestemming gaan zoals bedoeld in artikel 1, §8 van de privacywet.
§ 8. de ITS-dienstenaanbieders en ontwikkelaars van platformen, architectuur en interfaces	§ 8. Deze paragraaf heeft betrekking op de gegevensbescherming door ontwerp zoals

passen gegevensbescherming door ontwerp toe, overeenkomstig hun verplichtingen krachtens de wetten van 8 december 1992 en 13 juni 2005, .	vermeld in artikel 3 punt 22. Een absolute voorwaarde om slimme vervoerssystemen te kunnen invoeren is dat passende technische en juridische oplossingen worden gevonden voor de beveiliging van de persoonsgegevens als fundamenteel recht overeenkomstig artikel 8 van het Handvest van de grondrechten van de Europese Unie en artikel 16 van het Verdrag betreffende de werking van de Europese Unie. De overheden en betrokken partijen moeten erop toezien, met name in de eerste fase van de invoering van slimme voertuigen, dat toepassingen in slimme vervoerssystemen gemonitord worden en dat de fundamentele rechten en vrijheden van individuen worden beschermd[88]. Artikel 10 van de Richtlijn 2010/40/EU stelt dat *"de verwerking van persoonsgegevens in de context van de exploitatie van ITS-toepassingen en –diensten"* (moet worden) *"uitgevoerd overeenkomstig de uniale regelgeving ter bescherming van de fundamentele rechten en vrijheden van het individu, met name de Richtlijn 95/46/EG en Richtlijn 2002/58/EG.* Dit artikel komt bovendien tegemoet aan de kritiek van de Commissie voor de Bescherming van de persoonlijke Levenssfeer "Niet alleen moeten de ITS-kaderwet maar ook de ITS-systemen, toepassingen en –diensten conform de (elektronische-) privacywetgeving zijn".
ITS-dienstenaanbieders en ontwikkelaars van platformen, architectuur, interfaces voorzien gegevensbescherming door ontwerp en gegevensbescherming door	Het risico bestaat dat privacyinstellingen, zoals in de online wereld, soms aanzienlijke moeite vereisen om operationeel te worden. Zulke privacyinstellingen dienen, zeker indien de ITS

[88] Zie overweging 5 van de bij analogie toepasselijke Aanbeveling 2012/148/EU van de Europese Commissie van 9 maart 2012 inzake de voorbereiding van de uitrol van slimme metersystemen, gepubliceerd op http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:073:0009:0022:NL:PDF

standaardinstellingen bij de planning en kosten-baten analyses die de ontwikkeling en uitrol van ITS systemen en van toepassingen en diensten voorafgaan. Gegevensbescherming door standaardinstellingen wordt zodanig ten uitvoer gelegd door de ITS-dienstenaanbieders en ontwikkelaars van platformen, architectuur en interfaces dat de meest gegevensbeschermingsvriendelijke optie als standaardconfiguratie aan de klant wordt aangeboden.	toepassingen afhankelijk zijn van de toestemming van de gebruiker, eerder standaard te worden voorzien in plaats van als een optie voor de gebruiker. Zie het zogenaamde beginsel van gegevensbescherming door standaardinstellingen ("privacy by default"). De termen "gegevensbescherming door ontwerp" en "gegevensbescherming door standaardinstellingen" zoals gedefinieerd in aanhef zijn overgenomen van de Europese aanbeveling voor de uitrol van slimme netwerken en de invoering van slimme meters (zie de aanbeveling 2012/148/EU van de Europese Commissie van 9 maart 2012 inzake de voorbereiding van de uitrol van slimme metersystemen). Ingebouwde privacy wordt ten uitvoer gelegd op wetgevingsniveau (via samenwerkingsakkoorden met de regionale wetgeving en overeenkomstig de gegevensbeschermingswetten op federaal vlak die de omzetting van de Richtlijnen 1995/46/EG en 2002/58/EG tot doel hebben), op technisch niveau (door de vaststelling van passende eisen in de normen voor ITS die ervoor zorgen dat de infrastructuur volledig spoort met de gegevensbeschermingswetten) en op organisatorisch niveau (in verband met de verwerking.
§. 9 ITS-dienstenaanbieders en ontwikkelaars van platformen, architectuur en interfaces beschermen persoonsgegevens tegen misbruik, met inbegrip van onrechtmatige toegang, wijziging of verlies.	
§ 10. ITS-dienstenaanbieders en ontwikkelaars van platformen, architectuur, interfaces nemen de nodige maatregelen om een ruime	§ 10. Het voorzien van transparantie is een fundamentele voorwaarde voor het uitoefenen van controle op verwerkingen van

informatieverstrekking te verrichten aan de betrokkenen die minstens de elementen omvat in artikel 9 van de wet van 8 december 1992, en de elementen van het databeheer. § 11. De ITS-dienstenaanbieders en ontwikkelaars van platformen, architectuur en interfaces gebruiken passende privacycertificatiemechanismen en gegevensbeschermingsverzegelingen en -merktekens, verstrekt door onafhankelijke partijen. De Koning kan, na advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer, passende privacycertificatiemechanismen en gegevensbeschermingsverzegelingen en –merktekens bepalen en de criteria voor het bepalen van de voorwaarden van onafhankelijkheid en bekwaamheid van de partijen die de privacyimpact van de mechanismen, verzegelingen en merktekens kunnen beoordelen.	persoonsgegevens en om het vertrouwen van de betrokkenen in de ontwikkeling van ITS systemen en toepassingen aan te moedigen. Derhalve moet worden aangemoedigd dat overige relevante elementen die niet vermeld worden in artikel 9 van de wet van 8 december 1992 worden opgenomen in een publiek privacybeleid. Deze elementen omvatten het toepasselijke recht, de verwerkte persoonsgegevens (vermelding welke gegevens niet worden verwerkt, of er sprake is van anonimisering of encodering, de beschrijving van de basisdoelstellingen van het systeem en de afgeleide applicaties van derde partijen die een andere basis vereisen zoals toestemming van de betrokkene, een omschrijving van wie (al dan niet) toegang heeft tot de gegevens aanbieden), of wat de garanties zijn in dat verband, de bewaringstermijn (het dataretentiebeleid of –schema van het systeem eventueel naargelang de uiteenlopende applicaties), de wijze van bescherming tegen ongeoorloofde toegang (hacking,…) en de toegang tot de eigen gegevens, beschrijving van de concrete, praktische wijze van toegang tot de eigen gegevens (recht van toegang onder artikel 10 van de wet van 8 december 1992).
§ 12. ITS-dienstenaanbieders en ontwikkelaars van platformen, architectuur, interfaces verrichten een effectbeoordeling met betrekking tot de gegevensbescherming voor de start van de ontwikkeling van de platformen, architectuur, interfaces, systemen en applicaties. Zij houden hierbij rekening met de kenmerken en globale kosten-batenanalyse van elk project,	§ 12. De vraag om een effectbeoordeling te verrichten zal onderdeel moeten vormen van de globale kosten-batenanalyse van elk project, zodat zeer dure aanpassingen na de uitrol van systemen en toepassingen en risico op reputatieschade ingevolge ontbrekende elementen qua gegevensbescherming tijdig kunnen worden vermeden. Dit houdt ook rekening met de bevinding in de Europese

De ITS-dienstenaanbieders en ontwikkelaars kondigen de effectbeoordelingen af aan het publiek en, maken ze, van zodra beschikbaar, kenbaar gemaakt aan het publiek. De verantwoordelijken voor ITS-systemen en diensten bezorgen de Commissie voor de Bescherming van de Persoonlijke Levenssfeer zo vroeg als mogelijk de verrichte effectbeoordeling, en in elk geval voor de start van de ontwikkeling van de ITS platformen, architectuur, interfaces, systemen en applicaties. De Koning kan, na advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer, elementen bepalen die moeten deel uitmaken van de effectenbeoordeling.	studie over de economische voordelen van technologieën ter bevordering van de persoonlijke levenssfeer dat een zorgvuldige geval per geval beoordeling noodzakelijk is wil men economische en privacyvoordelen halen[89].

[89] Zie pagina 80 van voormelde studie gepubliceerd op http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf

§ 13. De verantwoordelijken voor publieke of private ITS-systemen en diensten die worden ontplooid of aangeboden vragen het advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer in een of meer van de volgende gevallen: - wanneer (gevoelige) persoonsgegevens in de zin van artikel 6, 7 of 8 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens worden verwerkt; - wanneer uit het ITS systeem, de ITS toepassing, de ITS dienst of ITS gegevens een besluit volgt waaraan voor een persoon rechtsgevolgen verbonden zijn of een besluit dat hem in aanmerkelijke mate treft, of dat bestemd is om bepaalde aspecten van zijn persoonlijkheid te evalueren; - wanneer persoonsgegevens worden verwerkt zonder de (vrije en specifieke) toestemming van de betrokkene. De Koning kan voormelde lijst van gevallen waarin het advies van de Commissie moet worden gevraagd uitbreiden.	§ 13. Deze wijziging houdt rekening met randnummer 28 van het advies van de Commissie. De betrokkene heeft sowieso het recht op basis van artikel 12bis van de wet van 8 december 1992 om niet uitsluitend te worden onderworpen aan op geautomatiseerde gegevensverwerking gebaseerde beslissingen, die worden genomen ten aanzien van de betrokkene en die hem in aanmerkelijke mate treffen. Hierbij kan gedacht worden aan beslissingen over beroepsprestatie, betrouwbaarheid of gedrag. Deze paragraaf viseert evenwel de situaties van hoger risico die niet onder artikel 12bis van de Wet van 8 december 1929 vallen, bijvoorbeeld omdat besluiten worden genomen met menselijke tussenkomst en niet puur op basis van een reeds verboden want volledig geautomatiseerd beslissingssysteem.
§ 14. Het niet naleven van de maatregelen vermeld in de paragrafen 3, 4, 6, 7, 8, 9 of 10 door de ITS-dienstenaanbieders en ontwikkelaars wordt beschouwd als een inbreuk op de artikelen 4 § 1, 1° en 16 § 4 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.	§ 14. Deze bepaling is een interpretatieve bepaling die de toepassing van de bepalingen van artikelen 4 § 1, 1° en 16 § 4 van de wet van 8 december 1992 op de sector van intelligente transportsystemen en -diensten verduidelijkt.
§ 15. De Koning kan, na advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer, elementen bepalen die moeten deel uitmaken van de effectbeoordeling met betrekking tot de gegevensbescherming.	§ 15. Wanneer actoren zoals ITS-dienstaanbieders en ontwikkelaars van platformen, architectuur, interfaces edm in de zin van deze wet een effectbeoordeling met betrekking tot de gegevensbescherming

	verrichten, moeten zij rekening houden met de adviezen van de relevante onafhankelijke toezichthoudende autoriteiten inzake gegevensbescherming op Europees en Belgisch vlak, waaronder de Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens en de Commissie voor de Bescherming van de Persoonlijke Levenssfeer. Naar analogie met de energiesector en om de kwaliteit en onafhankelijke beoordeling van de effectbeoordelingen te waarborgen werd de mogelijkheid gegeven aan de Koning om een template van een beoordeling te bepalen, na voorafgaand advies door de Commissie voor de Bescherming van de Persoonlijke Levenssfeer. Het gebrek aan het bestaan van een Koninklijk Besluit ontslaat de actoren evenwel niet van de verplichting om een effectbeoordeling met betrekking tot de gegevensbescherming vast te stellen en toe te passen.

Artikel 9 Machtiging aan de Koning

Tekstvoorstel	Memorie van Toelichting
§1. De Koning wordt gemachtigd om onder de voorwaarden vermeld in dit artikel de federale wetten aan te vullen, op te heffen of te vervangen om ze in overeenstemming te brengen met de vereisten inzake ITS.	
§2. De in dit artikel bedoelde machtiging kan slechts worden aangewend mits. de bepalingen waarvoor gebruik werd gemaakt van de machtiging het voorwerp uitmaken van een voorafgaand advies door de Commissie voor de bescherming van de persoonlijke levenssfeer.	§ 2. Bij gebruik van de bijzondere machten door de Koning dienen de verwerkingsvoorschriften en met name de risico's voor de bescherming van de persoonsgegevens van de betrokkene en de daarmee verband houdende beveiliging te worden geëvalueerd gelet op artikel 20 Richtlijn 95/46/EG en artikel 22 Grondwet.