WETTEN, DECRETEN, ORDONNANTIES EN VERORDENINGEN
LOIS, DECRETS, ORDONNANCES ET REGLEMENTS

GRONDWETTELIJK HOF

[2018/201410]

Uittreksel uit arrest nr. 29/2018 van 15 maart 2018

Rolnummer 6552

In zake : het beroep tot gedeeltelijke vernietiging van de wet van 13 mei 2016 « tot wijziging van de programmawet (I) van 29 maart 2012 betreffende de controle op het misbruik van fictieve adressen door de gerechtigden van sociale prestaties, met het oog op de invoering van het systematisch doorzenden naar de KSZ van bepaalde verbruiksgegevens van nutsbedrijven en distributienetbeheerders tot verbetering van de datamining en de datamatching in de strijd tegen de sociale fraude », ingesteld door de vzw « Ligue des Droits de l'Homme ».

Het Grondwettelijk Hof,

samengesteld uit de voorzitters A. Alen en J. Spreutels, de rechters L. Lavrysen, J.-P. Moerman, E. Derycke en F. Daoût, en, overeenkomstig artikel 60*bis* van de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof, emeritus voorzitter E. De Groot, bijgestaan door de griffier P.-Y. Dutilleux, onder voorzitterschap van emeritus voorzitter E. De Groot,

wijst na beraad het volgende arrest :

I. *Onderwerp van het beroep en rechtspleging*

Bij verzoekschrift dat aan het Hof is toegezonden bij op 28 november 2016 ter post aangetekende brief en ter griffie is ingekomen op 29 november 2016, heeft de vzw « Ligue des Droits de l'Homme », bijgestaan en vertegenwoordigd door Mr. R. Jespers, advocaat bij de balie te Antwerpen, beroep tot gedeeltelijke vernietiging ingesteld van de wet van 13 mei 2016 « tot wijziging van de programmawet (I) van 29 maart 2012 betreffende de controle op het misbruik van fictieve adressen door de gerechtigden van sociale prestaties, met het oog op de invoering van het systematisch doorzenden naar de KSZ van bepaalde verbruiksgegevens van nutsbedrijven en distributienetbeheerders tot verbetering van de datamining en de datamatching in de strijd tegen de sociale fraude » (bekendgemaakt in het *Belgisch Staatsblad* van 27 mei 2016).

(...)

II. *In rechte*

(...)

Ten aanzien van de context van de bestreden bepalingen

B.1.1. De bestreden wet van 13 mei 2016 « tot wijziging van de programmawet (I) van 29 maart 2012 betreffende de controle op het misbruik van fictieve adressen door de gerechtigden van sociale prestaties, met het oog op de invoering van het systematisch doorzenden naar de KSZ van bepaalde verbruiksgegevens van nutsbedrijven en distributienetbeheerders tot verbetering van de datamining en de datamatching in de strijd tegen de sociale fraude » (hierna : programmawet (I) van 29 maart 2012) regelt, in het kader van de strijd tegen de sociale domiciliefraude, ten eerste de gegevensuitwisseling tussen, enerzijds, nutsbedrijven en distributienetbeheerders en, anderzijds, overheidsdiensten en ten tweede de analyse van een grote verzameling van sociale gegevens. KSZ staat voor Kruispuntbank van de Sociale Zekerheid.

B.1.2. Met de bestreden wet heeft de wetgever willen tegemoetkomen aan zijn duidelijk voornemen in het regeerakkoord en navolgende beleidsplannen om een nieuwe stap te zetten in de strijd tegen sociale fraude. De wetgever beoogde in verschillende stappen geleidelijk de strijd tegen sociale domiciliefraude op te voeren en effectiever te maken met nieuwe instrumenten in het kader van de controle op misbruiken (*Parl. St.*, Kamer, 2011-2012, DOC 53-2081/017, p. 22; *Parl. St.*, Kamer, 2015-2016, DOC 54-1554/001, p. 8; *Parl. St.*, Kamer, 2015-2016, DOC 54-1554/005, p. 54).

B.1.3. Vóór de programmawet (I) van 29 maart 2012 werden de gerechtigden van sociale prestaties in het kader van een controle verzocht om hun verbruiksgegevens inzake water, gas en elektriciteit in voorkomend geval voor te leggen. Bij de voormelde programmawet werd de wettelijke mogelijkheid gecreëerd voor de sociale inspectie om die verbruiksgegevens bij nutsbedrijven of distributienetbeheerders op te vragen (het zogenaamde « pull »-systeem).

Artikel 101 van de programmawet (I) van 29 maart 2012, vóór de wijziging ervan bij het bestreden artikel 2, bepaalde :

« Indien de sociaal inspecteurs op basis van andere elementen in het kader van een onderzoek vermoeden dat een gerechtigde gebruik maakt van een fictief adres om aanspraak te maken op sociale prestaties waarop hij geen aanspraak kan maken, kunnen zij de verbruiksgegevens van water, elektriciteit en gas opvragen bij de nutsbedrijven of de distributienetbeheerders.

Deze verbruiksgegevens kunnen gebruikt worden als bijkomende aanwijzing om aan te tonen dat het adres fictief is ».

Dat artikel is in de parlementaire voorbereiding toegelicht als volgt :

« Deze afdeling beoogt, in uitvoering van de notificatie van de begrotingsopmaak 2012, enkele nieuwe instrumenten aan te reiken aan de controle-instanties om de fraudebestrijding bij uitkeringen vanwege de overheid aan te scherpen. Het wil een aanzet vormen voor een betere handhaving van de uitkeringen. Het doel is te bewerkstelligen dat aan elke sociaal [verzekerde] de correcte uitkering wordt betaald.

In concreto krijgen de sociale inspecteurs de mogelijkheid om de verbruiksgegevens van water, elektriciteit en gas van personen die recht hebben op een sociale prestatie op te vragen bij de nutsbedrijven en de distributiebeheerders.

Deze laatste zijn verplicht om op een dergelijk verzoek in te gaan en de gegevens te verschaffen » (*Parl. St.*, Kamer, 2011-2012, DOC 53-2081/001, p. 71).

« Sociale inspecteurs krijgen het recht om de verbruiksgegevens van nutsvoorzieningen (water, elektriciteit en gas) op te vragen bij nutsbedrijven en distributienetbeheerders indien zij op basis van andere elementen vermoeden dat een gerechtigde van sociale prestaties domiciliefraude pleegt. Voor de nutsbedrijven en distributienetbeheerders, die tot nu toe niet in alle gevallen op een informatieverzoek ingaan, zal een verplichting gelden om op dergelijk verzoek in te gaan en de gegevens te verschaffen. De aangereikte informatie kan een bijkomende indicatie van misbruik, doch geen sluitend bewijs opleveren.

Deze maatregel is een eerste stap, maar zorgt niet voor een integrale oplossing van het probleem. Andere hervormingen zijn in de toekomst nodig om domiciliefraude te beteugelen » (*Parl. St.*, Kamer, 2011-2012, DOC 53-2081/017, p. 22).

B.1.4. Dat zogenaamde « pull »-systeem is nooit in de praktijk toegepast (*Parl. St.*, Kamer, 2015-2016, DOC 54-0020/063, p. 14).

B.2.1. De bestreden wet vervangt het voormelde « pull »-systeem door het zogenaamde « push »-systeem en voorziet in nieuwe mogelijkheden betreffende « data mining » in de strijd tegen sociale domiciliefraude.

B.2.2. Inzake de overgang naar het « push »-systeem van gegevensuitwisseling vermeldt de parlementaire voorbereiding :

« Het bestaande zogenaamde ' pull ' systeem, waarbij nutsbedrijven en de distributienetbeheerders deze verbruiksgegevens op vraag van de inspectiediensten moeten overmaken, wordt omgezet in een ' push ' systeem. Dit betekent dat de nutsbedrijven en distributienetbeheerders de bedoelde verbruiksgegevens voortaan automatisch elektronisch sturen naar de [Kruispuntbank van de Sociale Zekerheid; hierna : KSZ]. Deze gegevens zullen dienen als bijkomende indicatoren om de sociale inspectiediensten toe te laten domiciliefraude beter te detecteren. *In concreto* zullen de verbruiksgegevens door de KSZ aangewend worden bij datamatching en, in een latere fase, als extra indicatoren bij de datamining. Op deze manier komt de regering tegemoet aan punt 31 van het advies van de Commissie ter bescherming van de persoonlijke levenssfeer (CBPL) dat geen bijkomende gegevens noch over het sociaal statuut van de betrokkene, noch over de gezinssamenstelling, worden doorgegeven aan de nutsbedrijven en distributienetbeheerders » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/001, pp. 5-6).

Wat de overgang naar het nieuwe systeem betreft, wordt nog het volgende vermeld :

« Het in 2012 ingevoerde *pull*-systeem was een stap in de goede richting. Nu is het nodig om over te gaan naar het meer doeltreffende *push*-systeem, in eerste instantie in het kader van een testfase die toelaat om de methode te verbeteren » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/005, p. 54).

In de parlementaire voorbereiding wordt vervolgens de meerwaarde van het « push »-systeem toegelicht :

« De meerwaarde van deze beleidsverschuiving ligt in het feit dat de push van extreem laag of extreem hoog verbruik ten opzichte van het gemiddelde verbruik, afhankelijk van de gezinssamenstelling, een knipperlicht activeert in de gevallen waar er nog geen vermoeden van fraude is. Daar ligt ook de toegevoegde waarde van de datamining: de controles meer efficiënt en gerichter maken. Bij het ' pull ' systeem is deze toegevoegde waarde zeer beperkt aangezien men op basis van een concreet dossier met een vermoeden van fraude bijkomende gegevens opvraagt » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/001, p. 6).

B.2.3.1. Met betrekking tot de door de wetgever nagestreefde doelstellingen, vermeldt de parlementaire voorbereiding :

« Overeenkomstig de begrotingsnotificatie die door de Ministerraad op 3 april 2015 (blz. 39-40) goedgekeurd werd, is het doel van dit ontwerp van wet om het mogelijk te maken verbruiksgegevens van particulieren systematisch door te zenden van nutsbedrijven naar de Kruispuntbank van de sociale zekerheid. Dit moet de controle op de correcte toekenning van sociale prestaties versterken.

Meer en meer groeit het bewustzijn dat uitkeringsfraude een hypotheek legt op onze sociale zekerheid. Deze kan maar bestaan in zoverre zij een breed draagvlak heeft dat wordt gedragen door de solidariteit.

Uitkeringsfraude treft onze sociale zekerheid in het hart. Zij ondermijnt immers één van haar basisbeginselen, met name de solidariteit. Dit principe vormt één van de grondslagen van ons stelsel.

Tal van burgers betalen hun bijdragen eerlijk en ontvangen hun uitkeringen rechtmatig. Slechts een bepaalde groep respecteert de regels niet en benadeelt zo de andere burgers die wel correct bijdragen aan het regime van de sociale zekerheid en die er van genieten wanneer ze er recht op hebben.

In verschillende takken van de sociale zekerheid, zoals de werkloosheid en de ziekte- en invaliditeitsverzekering, worden sommige prestaties met een verhoging/toeslag immers toegekend in functie van de familiale situatie van de sociaal verzekerde.

Fictieve domiciliëring is een fraudemechanisme dat hierop inspeelt doordat de sociaal verzekerde bewust zijn werkelijke domicilie en/of familiale situatie niet aangeeft om op ongeoorloofde wijze een hogere uitkering te krijgen dan diegene waarop hij recht heeft.

Rekening houdende met de impact hiervan, is de aan de fictieve domiciliëring verbonden sociale fraude een fenomeen waaraan de inspectiediensten bijzondere aandacht besteden.

In het kader van een versterking van de strijd tegen de sociale fraude, werden externe maatregelen (versterking van de samenwerking met de magistraten, de politie en de andere openbare instellingen van sociale zekerheid) alsook interne maatregelen (invoering van nieuwe administratieve procedures) uitgewerkt en ingevoerd.

Er werd eveneens beslist om een globale strategie voor de bestrijding van fictieve domiciliëring te voorzien waarbij alle instellingen van sociale zekerheid en de organismen voor toekenning van sociale voordelen zijn betrokken en dit door opsporings- en vervolgingsrichtlijnen voor te schrijven met respect voor de privacy.

Het College van Procureurs-generaal heeft een omzendbrief uitgevaardigd over dit sociaal fraudefenomeen bestaande uit fictieve inschrijvingen. Deze omzendbrief van het College (COL PG 17/2013) en het bijhorend vademecum zijn in voege getreden op 2 september 2013 » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/001, pp. 4-5).

B.2.3.2. Daaruit blijkt dat de wetgever, uitgaande van het standpunt dat uitkeringsfraude de solidariteit als fundament van de sociale zekerheid ondermijnt, de strijd tegen sociale fraude als een belangrijke maatschappelijke aangelegenheid heeft beschouwd. Met het oog op die strijd werden reeds meerdere maatregelen genomen. In het bijzonder wordt met de bestreden regeling de aandacht gericht op de sociale domiciliefraude, gelet op de nauwe band tussen de hoogte van de sociale uitkeringen, de domicilie- en de gezinssituatie.

B.3.1. Aldus beoogt de wetgever de strijd tegen sociale domiciliefraude te versterken door gebruik te maken van moderne verwerkingstechnieken zonder dat de geselecteerde en doorgestuurde verbruiksgegevens, de zogenaamde fraudeknipperlichten, determinerend zijn om uit te maken of een sociaal gerechtigde gebruik maakt van een fictief adres.

De bestreden wet strekt er derhalve toe de overheidsdiensten, te dezen de sociaal inspecteurs en de openbare instellingen van sociale zekerheid (hierna : OISZ's) meer effectieve en efficiëntere instrumenten te geven om hun wettelijke taken in de sociale zekerheid uit te voeren. Sociaal inspecteurs zijn de ambtenaren die onder het gezag staan van de ministers tot wier bevoegdheid de werkgelegenheid en arbeid, de sociale zekerheid, de sociale zaken en volksgezondheid behoren of die onder het gezag staan van de openbare instellingen die ervan afhangen, en die zijn belast met het toezicht op de naleving van de sociale wetten (artikel 16, 1°, van het Sociaal strafwetboek). OISZ's zijn de overheidsdiensten die belast zijn met de toepassing van de wetgeving betreffende de sociale zekerheid.

B.3.2. De wetgever heeft onder meer ingevolge de mogelijkheden van « profiling »-technieken, die steunen op « data warehousing », « data matching » en « data mining », geoordeeld dat, enerzijds, het automatisch en systematisch aan de in B.3.1 vermelde overheidsdiensten ter beschikking stellen van geselecteerde adres- en verbruiksgegevens met betrekking tot water, gas en elektriciteit en, anderzijds, het analyseren van de beschikbare samengevoegde gegevens en het zoeken naar risico-indicatoren daarin door die diensten, nuttige instrumenten zijn in de strijd tegen sociale domiciliefraude.

B.3.3. De « profiling » verloopt in drie te onderscheiden fases waarbij wordt gezocht naar of op basis van patronen en modellen (zogenaamde profielen) : een eerste fase waarbij informatie met betrekking tot het gedrag of kenmerken van personen op grote schaal wordt verzameld en bewaard (« data warehousing »); een tweede en een derde fase waarin die gegevens worden geanalyseerd en diepgaand onderzocht om verbanden tussen gedragingen en karakteristieken vast te stellen, en waarin op basis van de voormelde vastgestelde verbanden voorheen onbekende of verborgen (bestaande, toekomstige dan wel vroegere) karakteristieken en gedragingen voor personen uit de gegevens worden afgeleid (« data mining »).

B.3.4. Die « profiling »-techniek strekt er derhalve toe op basis van een profiel, een geheel van kenmerken dat een categorie van personen karakteriseert (bv. fraudeurs), een individueel persoon te detecteren met het oog op, enerzijds, het nemen van beslissingen (bv. het starten van een onderzoek) ten aanzien van die persoon en, anderzijds, het analyseren of voorspellen van zijn persoonlijke voorkeuren, gedragingen en houding (punt 1, d. en e., van de aanbeveling nr. (2010)13 van het Comité van Ministers aan de verdragsstaten van 23 november 2010 inzake de bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens in de context van « profiling » (hierna : aanbeveling (2010)13).

B.3.5. Het is evenwel van groot belang dat bij die techniek de juiste selectiecriteria (geheel van karakteristieken) worden gebruikt om de strijd tegen sociale fraude te versterken (het zgn. fraudeknipperlicht of de zgn. risico-indicatoren). Er zijn immers, *a fortiori* in de beginfase van het opzet, ernstige gebreken verbonden aan die techniek, met name vals positieve en vals negatieve resultaten, hetgeen noopt tot een permanente opvolging en evaluatie van de criteria (zie Privacycommissie, advies 24/2015, p. 7; advies 05/2016, p. 6).

B.4. Uit de parlementaire voorbereiding van de bestreden wet blijkt dat de door de wetgever nagestreefde doelstelling wordt geïmplementeerd door een wettelijke basis te verschaffen aan de versterkte controle op sociale domiciliefraude via automatische gegevensuitwisseling tussen dienstenverstrekkers en overheidsdiensten en aan de moderne technieken van onderzoek in grote gegevensverzamelingen (« data warehousing »), zoals « data matching » en « data mining », zonder afbreuk te doen aan de vereisten inzake de bescherming van de privacy (zie artikel 104 van de programmawet (I) van 29 maart 2012) :

« Het ontwerp voorziet daarom in een wettelijke basis om bepaalde verbruiksgegevens van water, gas en elektriciteit en adresgegevens van bepaalde particulieren elektronisch over te maken aan de Kruispuntbank van de sociale zekerheid (KSZ) » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/001, p. 5).

« De Commissie [voor de bescherming van de persoonlijke levenssfeer] adviseerde een gelijkaardige algemene wettelijke basis voor het gebruik van ' *datamining* ' en ' *datamatching* ' aan de hand van de relevante databanken, zoals gebruikt door onder meer het platform OASIS. Hoewel de Commissie duidelijk stelt dat deze aanbeveling het huidige dossier overstijgt, wordt met de toevoeging van deze paragraaf reeds tegemoetgekomen aan deze aanbeveling van de Commissie voor wat betreft de energiegegevens en wordt hiervoor een wettelijke basis voor datamining ingesteld » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/004, p. 9).

« Met respect voor de privacy zal er zodoende, zoals dit reeds in Nederland het geval is, op automatische wijze kunnen worden nagegaan of de opgegeven verbruiksgegevens al dan niet matchen met domiciliegegevens. Deze gegevenskruising kan knipperlichten doen branden waardoor verder onderzoek noodzakelijk is. De energiegegevens worden vandaag al effectief aangewend in de strijd tegen woningleegstand in Brussel, bijvoorbeeld.

Om dit alles te realiseren wordt de bestaande wetgeving, opgenomen in de artikelen 100 tot en met 105 van de programmawet van 29 maart 2012, aangepast. Deze wet bevat reeds een bepaling die de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens van toepassing maakt. Deze bepaling blijft uiteraard behouden in het nieuwe systeem » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/001, p. 6).

B.5.1. De maatregelen waarmee de wetgever zijn doelstelling beoogt te verwezenlijken, zijn vervat in de artikelen 2 en 3 van de bestreden wet.

B.5.2. Artikel 2 van de bestreden wet stelt een « push »-systeem in - dat in meerdere fasen met een zeer specifieke doelstelling verloopt - waarbij verbruiksgegevens van water, gas en elektriciteit en adresgegevens van bepaalde particulieren elektronisch worden doorgestuurd naar de KSZ, die ze filtert en kruist (« data matching ») met andere gegevens om ze te bezorgen aan de belanghebbende OISZ's en sociaal inspecteurs teneinde de strijd tegen uitkeringsfraude te versterken en efficiënter te maken (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/001, p. 5).

In een eerste fase worden de nutsbedrijven en de distributienetbeheerders verplicht om verbruiks- en adresgegevens te verzamelen. Zij dienen vervolgens bepaalde gegevens minimaal eenmaal per jaar aan de KSZ te bezorgen. Die gegevens worden geselecteerd omdat het verbruik ten minste 80 pct. afwijkt van het gemiddelde verbruik op grond van de officieel meegedeelde gezinssamenstelling (artikel 101, § 1, eerste lid, van de programmawet (I) van 29 maart 2012, zoals vervangen door artikel 2 van de bestreden wet). De gezinstypes en het gemiddelde verbruik per gezinstype worden jaarlijks bepaald door het beheerscomité van de KSZ in overleg met de nutsbedrijven en de distributienetbeheerders (artikel 101, § 1, tweede lid, van de programmawet (I) van 29 maart 2012, zoals vervangen door artikel 2 van de bestreden wet).

In een tweede fase worden de aldus verzamelde en ontvangen gegevens door de KSZ, na kruising met het Rijksregister om te achterhalen wie op de doorgegeven adressen woont, bezorgd aan de OISZ's en de sociaal inspecteurs in zoverre zij de gerechtigde op wie de gegevens betrekking hebben een sociale uitkering toekennen of enige vorm van toezicht uitoefenen op de naleving van wetten die een voordeel toekennen (« data matching »; artikel 101, § 1, derde lid, van de programmawet (I) van 29 maart 2012, zoals vervangen door artikel 2 van de bestreden wet).

De sociale inspectie of een OISZ kan vervolgens, na machtiging door het sectoraal comité van de sociale zekerheid en van de gezondheid op basis van de ontvangen gegevens, in combinatie met andere (persoons)gegevens uit de sociale gegevensbanken, de KSZ en het Rijksregister, controleren of een sociale uitkeuring wordt toegekend op basis van een fictief adres (« data mining »; artikel 101, § 1, derde lid, van de programmawet (I) van 29 maart 2012, zoals vervangen door artikel 2 van de bestreden wet).

Evenwel kunnen de toegezonden verbruiks- en adresgegevens op zichzelf niet leiden tot het oordeel dat de betrokken gerechtigde sociale domiciliefraude heeft gepleegd (artikel 102 van de programmawet (I) van 29 maart 2012, zoals vervangen door artikel 4 van de bestreden wet).

B.5.3. Daarnaast laat artikel 3 het onderzoek toe naar verbanden en risico-indicatoren met betrekking tot sociale domiciliefraude in samengevoegde gegevens uit relevante sociale databanken (« data mining ») door een OISZ.

In deze derde fase kan een OISZ, waaronder ook de sociale inspectie ressorteert, de ontvangen verbruiks- en adresgegevens samenvoegen met andere gegevens waarover zij beschikt met het oog op het uitvoeren van analyses op relationele gegevens teneinde de diensten in staat te stellen om gerichte fraudecontroles uit te voeren op basis van risico-indicatoren inzake de toekenning van steun op basis van een fictief adres (artikel 101/1 van de programmawet (I) van 29 maart 2012, zoals ingevoegd door artikel 3 van de bestreden wet). Die analyse gebeurt op basis van gecodeerde gegevens die slechts worden gedecodeerd nadat ze zijn afgezonderd indien uit de analyse het risico op een gebruik van een fictief adres blijkt.

B.6. De wetgever heeft er voorts voor gekozen de uitvoeringsregels met betrekking tot het ingestelde systeem op te dragen aan het beheerscomité van de KSZ. Die delegatie wordt in de parlementaire voorbereiding toegelicht als volgt :

« Er wordt tevens voorzien dat niet de Koning, maar wel het beheerscomité van de Kruispuntbank van de sociale zekerheid het gemiddelde verbruik per gezinstype zal moeten bepalen. Het beheerscomité moet dit doen in overleg met de actoren op het terrein, namelijk de nutsbedrijven en distributienetbeheerders. Deze aanpak maakt het volgens de regering mogelijk om de meest adequate grenswaarden vast te leggen en deze, indien nodig, snel aan te passen aan de veranderende omstandigheden op het terrein om domiciliefraude efficiënt te kunnen bestrijden. Domiciliefraude is immers een evolutief gegeven en bovendien wenst de regering uiteraard in geen geval bonafide gerechtigden te treffen. Aan deze bekommernis wordt tegemoetgekomen door de voorziene delegatie aan het beheerscomité » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/001, pp. 7-8).

Ten aanzien van de bestreden bepalingen

B.7.1.1. Artikel 2 van de bestreden wet vervangt artikel 101 van de programmawet (I) van 29 maart 2012 als volgt :

« § 1. In functie van de periodiciteit van hun gegevensinzameling en minstens één maal per kalenderjaar bezorgen de nutsbedrijven en distributienetbeheerders bepaalde verbruiks- en adresgegevens van bepaalde van hun particuliere klanten op elektronische wijze aan de Kruispuntbank van de Sociale Zekerheid. Het betreft de gegevens door de nutsbedrijven en distributienetbeheerders geselecteerd omdat het verbruik van de particuliere klant ten minste 80 % in neerwaartse of opwaartse zin afwijkt van een gemiddeld verbruik waarbij rekening gehouden wordt met de officieel meegedeelde gezinssamenstelling.

De gezinstypes en het gemiddelde verbruik per gezinstype worden jaarlijks bepaald door het beheerscomité van de Kruispuntbank van de Sociale Zekerheid in overleg met de nutsbedrijven en distributienetbeheerders.

De Kruispuntbank van de Sociale Zekerheid bezorgt de in het eerste lid bedoelde gegevens na kruising met de gegevens die zijn opgeslagen in het Rijksregister, bedoeld in de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, aan de openbare instellingen van sociale zekerheid en de sociaal inspecteurs op voorwaarde dat de bedoelde instellingen aan de gerechtigde op wie deze gegevens betrekking hebben een sociale uitkering toekennen, hetzij op basis van de sociale zekerheid, hetzij op basis van een regeling voor maatschappelijke bijstand, of van andere voordelen toegekend door de reglementeringen waarop de sociaal inspecteurs toezicht uitoefenen. Dat moet hen in staat stellen om, na machtiging van het sectoraal comité van de Sociale Zekerheid en van de gezondheid, in combinatie met andere sociale gegevens en sociale gegevens van persoonlijke aard die beschikbaar zijn in het netwerk, zoals bedoeld in de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid, te controleren of de sociale uitkering wordt toegekend op basis van een fictief adres.

§ 2. Voor de gegevensverwerkingen als bedoeld in § 1 wordt als verantwoordelijke voor de verwerking als bedoeld in artikel 1, § 4, van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, de Kruispuntbank van de Sociale Zekerheid aangeduid ».

B.7.1.2. De parlementaire voorbereiding bij de eerste paragraaf van de nieuwe bepaling vermeldt :

« Dit artikel verplicht de nutsbedrijven en distributienetbeheerders om in functie van de periodiciteit van hun eigen gegevensinzameling, maar minstens één maal per kalenderjaar bepaalde verbruiks- en adresgegevens van bepaalde van hun particuliere klanten op elektronische wijze aan de Kruispuntbank van de sociale zekerheid te bezorgen. Dit betekent dus dat de gegevens voortaan ' gepusht ' worden. Dit moet dus minstens één maal per jaar, maar indien het voor bepaalde nutsbedrijven en distributienetbeheerders mogelijk is, kunnen de gegevens ook meermaals per jaar doorgestuurd worden. Het gaat om de gegevens die door de nutsbedrijven en distributienetbeheerders geselecteerd worden omdat ze minstens 80 % in neerwaartse of opwaartse zin afwijken van een gemiddeld verbruik waarbij rekening gehouden wordt met [de] officieel meegedeelde gezinssamenstelling. De gezinstypes en het gemiddeld verbruik per gezinstype worden jaarlijks bepaald door het beheerscomité van de Kruispuntbank van de sociale zekerheid in overleg met de nutsbedrijven en distributienetbeheerders.

In het voorontwerp van wet was voorzien dat de mededeling van verbruiksgegevens zou gebeuren op basis van bepaalde grenswaarden die kunnen wijzen op een te laag of te hoog verbruik in functie van de officieel meegedeelde gezinssamenstelling. Deze grenswaarden zouden worden vastgesteld door de Koning bij een besluit vastgesteld na overleg in de Ministerraad. De Raad van State heeft in punt 8.2. van zijn advies echter opgemerkt dat deze delegatie aan de Koning te uitgebreid is. Gelet op deze opmerking heeft de regering geoordeeld dat het raadzaam is om inderdaad reeds in de wet zelf een beperking te voorzien. Daarom wordt de 80 % regel in de wet zelf ingeschreven. Er wordt tevens voorzien dat niet de Koning, maar wel het beheerscomité van de Kruispuntbank van de sociale zekerheid het gemiddelde verbruik per gezinstype zal moeten bepalen. Het beheerscomité moet dit doen in overleg met de actoren op het terrein, namelijk de nutsbedrijven en distributienetbeheerders. Deze aanpak maakt het volgens de regering mogelijk om de meest adequate grenswaarden vast te leggen en deze, indien nodig, snel aan te passen aan de veranderende omstandigheden op het terrein om domiciliefraude efficiënt te kunnen bestrijden. Domiciliefraude is immers een evolutief gegeven en bovendien wenst de regering uiteraard in geen geval bonafide gerechtigden te treffen. Aan deze bekommernis wordt tegemoetgekomen door de voorziene delegatie aan het beheerscomité.

Daarnaast moet volgens de CBPL beter verantwoord worden waarom wordt overgestapt van een ' pull ' naar een ' push ' model. Aangezien verschillende openbare instellingen van sociale zekerheid (OISZ) uitkeringen toekennen die variëren in functie van de gezinssamenstelling, is het voor hen van belang om zo goed mogelijk te kunnen controleren of de opgegeven gezinssamenstelling wel correct is. Momenteel doen de inspectiediensten dit onder andere door middel van controles ter plaatse in het opgegeven domicilie of door het opvragen van de verbruiksgegevens bij de sociaal verzekerde zelf of bij de nutsbedrijven of distributienetbeheerders. Het voorgestelde push model dient deze bestaande instrumenten te versterken en de controle dus meer sluitend en performanter te maken. Tijdens de bespreking in de Nationale Arbeidsraad heeft de Rijksdienst voor Arbeidsvoorziening bijvoorbeeld aangegeven dat dit systeem hun sociale inspecteurs inderdaad beter in staat zal stellen om de naleving van de regels van de werkloosheidsreglementering gerichter en doeltreffender te controleren.

Bovendien vraagt de CBPL ook waarom zowel een te laag als te hoog verbruik geviseerd wordt. Gelet op het voorgaande is het logisch dat beide uitersten in aanmerking genomen worden. Het is immers mogelijk dat beide partners van een koppel een uitkering genieten. Om hun beider uitkeringen te verhogen verklaren ze beide

alleenstaande te zijn. Om dit te staven hebben ze een apart domicilie. Hierdoor kunnen ze beide een uitkering als alleenstaande genieten. Deze bedraagt uiteraard meer dan een uitkering als samenwonende. In de feiten wonen ze echter nog steeds samen. In het ene domicilie zal het werkelijk verbruik dus in principe lager zijn dan het gemiddelde verbruik van een alleenstaande. In het andere domicilie in principe te hoog. Dankzij deze maatregel kunnen beide vormen van uitkeringsfraude gedetecteerd worden.

Tevens wordt de finaliteit van deze verplichting vastgelegd. Deze gegevens moeten de bevoegde sociaal inspecteurs in staat stellen om na te gaan of de betaalde sociale zekerheids- of bijstandsuitkeringen terecht toegekend werden.

Om dit te kunnen doen moeten deze gegevens gecombineerd worden met andere gegevens waar de bevoegde diensten over beschikken of toegang toe hebben.

Om toegang te krijgen tot de verbruiksgegevens en om ze te mogen combineren met de andere gegevens moeten de geïnteresseerde diensten, zoals steeds, een machtiging vragen van het sectoraal comité van de sociale zekerheid en van de gezondheid.

Ingevolge opmerking 9.4 van de Raad van State werd de tekst aangepast om duidelijker tot uiting te laten komen dat de afwijkende verbruiksgegevens enkel worden meegedeeld door de KSZ indien de betrokken personen uitkeringen ontvangen van de betrokken instellingen.

Deze aanpassing biedt meteen ook een antwoord op de bemerking van de CBPL dat de private bedrijven (nutsbedrijven en distributienetbeheerders) geen aanvullende informatie over de sociaal verzekerde mogen krijgen van de sociale inspectie of het rijksregister. Het gaat zeer duidelijk om éénrichtingsverkeer. De private bedrijven moeten informatie verschaffen. Ze krijgen er geen » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/001, pp. 7-9).

Bij de tweede paragraaf vermeldt de parlementaire voorbereiding :

« In de adviezen van 17 juni 2015 en 3 februari 2016 wijst de Privacycommissie erop dat de verantwoordelijke voor de verwerking niet uitdrukkelijk is aangewezen in het ontwerp. Daar er bij de door het wetsontwerp beoogde aanpak van sociale fraude een groot aantal spelers betrokken zal zijn (distributienetbeheerders, KSZ, sociale inspectie, eventuele verwerkers,...) zal vroeg of laat de vraag rijzen wie de verantwoordelijke is of de verwerker voor de diverse bewerking(en) die het wetsontwerp beoogt. Omdat voor al deze verwerkingen de actuele en toekomstige rechten en plichten moeten worden nageleefd door elke verantwoordelijke onder de WVP en de GDPR, is het belangrijk dat dienaangaande verduidelijking wordt verschaft. Het advies van de Privacycommissie stelt zelf dat deze aanduiding ook op een precieze wijze kan geschieden in de machtigingen tot gegevensuitwisseling. Om de transparantie te verhogen zal de verantwoordelijke voor de verwerking ook duidelijk in de wet worden vermeld. Voor wat betreft de ' *datamatching* ' wordt de ' Kruispuntbank van de Sociale Zekerheid ' aangewezen als de verantwoordelijke voor de verwerking » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/004, p. 7).

B.7.2.1. Artikel 3 van de bestreden wet voegt een nieuw artikel 101/1 in de programmawet (I) van 29 maart 2012 in, dat bepaalt :

« § 1. Elke openbare instelling van sociale zekerheid (OISZ) kan de overeenkomstig artikel 101 van dezelfde wet ingezamelde gegevens samenvoegen met andere gegevens waar de OISZ's over beschikken met het oog op het uitvoeren van analyses op relationele gegevens waarmee deze diensten in staat worden gesteld om gerichte controles uit te voeren op basis van risico-indicatoren voor de toekenning van steun berekend op basis van een fictief adres. De analyse gebeurt op basis van gecodeerde gegevens. De gegevens waar een risico op het gebruik van een fictief adres uit blijkt, worden afgezonderd en gedecodeerd.

§ 2. Elke categorie van gegevens die aan een OISZ doorgegeven wordt in het kader van artikel 101, § 1 is onderworpen aan een machtiging van een sectoraal comité ingesteld binnen de Commissie voor de bescherming van de persoonlijke levenssfeer. De machtiging bepaalt de voorwaarden in verband met de bewaringstermijn van de gecodeerde en gedecodeerde gegevens.

§ 3. De in artikel 101, § 1, bedoelde analyses op relationele gegevens hebben als verantwoordelijke voor de verwerking, als bedoeld in artikel 1, § 4, van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, de OISZ die de analyse op relationele gegevens uitvoert ».

B.7.2.2. De parlementaire voorbereiding bij de eerste paragraaf van deze bepaling vermeldt :

« Het advies van 3 februari 2016 van de Privacycommissie verwijst naar artikel 5, § 1, van de wet van 3 augustus 2012 houdende bepalingen betreffende de verwerking van persoonsgegevens door de Federale Overheidsdienst Financiën in het kader van zijn opdrachten, die stelt :

' § 1. De Federale Overheidsdienst Financiën kan de overeenkomstig artikel 3 ingezamelde gegevens samenvoegen met het oog op de oprichting van een datawarehouse waarmee zijn diensten enerzijds in staat worden gesteld om gerichte controles uit te voeren op basis van risico-indicatoren en anderzijds analyses kunnen uitvoeren op relationele gegevens afkomstig van verschillende administraties en, of diensten van de Federale Overheidsdienst Financiën. ' De Commissie adviseerde een gelijkaardige algemene wettelijke basis voor het gebruik van ' *datamining* ' en ' *datamatching* ' aan de hand van de relevante databanken, zoals gebruikt door onder meer het platform OASIS. Hoewel de Commissie duidelijk stelt dat deze aanbeveling het huidige dossier overstijgt, wordt met de toevoeging van deze paragraaf reeds tegemoetgekomen aan deze aanbeveling van de Commissie voor wat betreft de energiegegevens en wordt hiervoor een wettelijke basis voor datamining ingesteld » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/004, p. 9).

Wat de tweede paragraaf betreft, wordt vermeld :

« In de adviezen van 17 juni 2015 en 3 februari 2016 stelt de Privacycommissie de vraag naar een gepaste bewaringstermijn voor de gegevens, rekening houdend met artikel 4, § 1, 4º, van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (WVP). De Commissie stelt dat de vaststelling van een bewaringstermijn op precieze wijze kan geschieden in de machtigingen tot gegevensuitwisseling. In paragraaf 2 wordt vastgelegd dat deze machtigingen bewaringstermijnen moeten bevatten voor gecodeerde en gedecodeerde gegevens » (*ibid.*).

De derde paragraaf wordt toegelicht als volgt :

« Voor wat betreft de ' datamining ' wordt de ' OISZ die de analyse op relationele gegevens uitvoert ' aangewezen als de verantwoordelijke voor de verwerking » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/004, p. 10).

B.7.3.1. Artikel 4 van de bestreden wet vervangt artikel 102 van de programmawet (I) van 29 maart 2012 als volgt :

« De gegevens bedoeld in artikel 101 kunnen enkel als bijkomend element gebruikt worden om uit te maken of een gerechtigde gebruik maakt van een fictief adres ».

B.7.3.2. De parlementaire voorbereiding bij deze bepaling vermeldt :

« Dit artikel bepaalt dat de gegevens enkel als bijkomend element gebruikt kunnen worden om uit te maken of een gerechtigde gebruik maakt van een fictief adres.

Het is inderdaad niet de bedoeling om louter op basis van verbruiksgegevens te besluiten dat er fraude in het spel is. Daarvoor zijn deze gegevens op zichzelf genomen niet voldoende doorslaggevend » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/001, pp. 9-10).

B.7.4. Artikel 5 van de bestreden wet vervangt het woord « opvragen » in artikel 103 van de programmawet (I) van 29 maart 2012 door het woord « gebruiken ».

B.7.5.1. Artikel 6 van de bestreden wet vervangt artikel 105 van de programmawet (I) van 29 maart 2012 als volgt :

« Het beheerscomité van de Kruispuntbank van de Sociale Zekerheid bepaalt de nadere regels, onder meer de structuur en inhoud van de berichten waarmee de gegevens worden bezorgd, de wijze en het tijdstip waarop de verbruiks- en adresgegevens worden bezorgd ».

B.7.5.2. De parlementaire voorbereiding bij die bepaling vermeldt :

« Dit artikel voorziet in een delegatie aan het beheerscomité van de Kruispuntbank van de sociale zekerheid.

Het beheerscomité dient de nadere regels te bepalen om de maatregel in de praktijk te implementeren. Het gaat onder meer om de structuur en inhoud van de berichten en de wijze en het tijdstip waarop de verbruiks- en adresgegevens moeten worden overgemaakt. Dergelijke delegatie aan het beheerscomité is niet nieuw en wordt verantwoord door het feit dat het gaat om vaak technische aspecten waarvoor het noodzakelijk is om in een snel veranderende informatica-omgeving kort op de bal te kunnen spelen » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/001, pp. 9-10).

Ten aanzien van de ontvankelijkheid van het beroep

B.8.1. Vermits de verzoekende partij uitsluitend grieven aanvoert tegen de artikelen 2, 3 en 4 van de bestreden wet, is het beroep slechts ontvankelijk in zoverre het is gericht tegen die artikelen.

B.8.2.1. De Ministerraad betwist de ontvankelijkheid van de meeste grieven van het enige middel omdat zij niet voldoende zouden zijn uiteengezet of geen relevantie zouden hebben. Bovendien werpt hij meermaals op dat een grief geheel of ten dele niet ontvankelijk zou zijn omdat het Hof niet bevoegd is om rechtstreeks te toetsen aan verdragsbepalingen, wetskrachtige bepalingen (wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens; hierna : Privacywet), wetgevingshandelingen van de Europese Unie (richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (hierna : richtlijn 95/46/EG) en verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)) en algemene beginselen van noodzakelijkheid, subsidiariteit, evenredigheid, transparantie, opslagbeperking, verantwoordingsplicht, integriteit en veiligheid.

B.8.2.2. Het Hof is bevoegd om wetskrachtige normen te toetsen aan de regels die de bevoegdheden verdelen tussen de federale Staat, de gemeenschappen en de gewesten, alsook aan de artikelen van titel II (« De Belgen en hun rechten ») en de artikelen 143, § 1, 170, 172 en 191 van de Grondwet.

Alle grieven zijn afgeleid uit de schending van één of meer van die regels waarvan het Hof de naleving waarborgt.

In zoverre de verzoekende partij daarnaast verdragsbepalingen, wetgevingshandelingen van de Europese Unie, wetskrachtige bepalingen en algemene beginselen vermeldt, onderzoekt het Hof die enkel in zoverre een schending wordt aangevoerd van de voormelde grondwetsbepalingen, in samenhang gelezen met de voormelde bepalingen, handelingen en beginselen. In die mate zijn de grieven ontvankelijk.

B.8.3. Om te voldoen aan de vereisten van artikel 6 van de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof moeten de middelen van het verzoekschrift niet alleen te kennen geven welke van de regels waarvan het Hof de naleving waarborgt, zouden zijn geschonden, maar ook welke de bepalingen zijn die deze regels zouden schenden, en uiteenzetten in welk opzicht die regels door de bedoelde bepalingen zouden zijn geschonden.

Het Hof onderzoekt de grieven van het enige middel in zoverre zij aan de voormelde vereisten voldoen.

B.8.4. De excepties worden verworpen.

Ten aanzien van het recht op eerbiediging van het privéleven

B.9. Het enige middel is in hoofdzaak, zij het niet uitsluitend, afgeleid uit de schending van het recht op eerbiediging van het privéleven, gewaarborgd bij artikel 22 van de Grondwet, in samenhang gelezen met artikel 8 van het Europees Verdrag voor de rechten van de mens, met artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten en met de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie.

B.10.1. Artikel 22 van de Grondwet bepaalt :

« Ieder heeft recht op eerbiediging van zijn privéleven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald.

De wet, het decreet of de in artikel 134 bedoelde regel waarborgen de bescherming van dat recht ».

B.10.2. Artikel 8 van het Europees Verdrag voor de rechten van de mens bepaalt :

« 1. Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn gezinsleven, zijn huis en zijn briefwisseling.

2. Geen inmenging van enig openbaar gezag is toegestaan met betrekking tot de uitoefening van dit recht dan voor zover bij de wet is voorzien en in een democratische samenleving nodig is in het belang van 's lands veiligheid, de openbare veiligheid, of het economisch welzijn van het land, de bescherming van de openbare orde en het voorkomen van strafbare feiten, de bescherming van de gezondheid of de goede zeden, of voor de bescherming van de rechten en vrijheden van anderen ».

B.10.3. De Grondwetgever heeft gestreefd naar een zo groot mogelijke concordantie tussen artikel 22 van de Grondwet en artikel 8 van het voormelde Europees Verdrag (*Parl. St.*, Kamer, 1992-1993, nr. 997/5, p. 2).

De draagwijdte van dat artikel 8 is analoog aan die van de voormelde grondwetsbepaling, zodat de waarborgen die beide bepalingen bieden, een onlosmakelijk geheel vormen.

B.10.4. Artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten bepaalt :

« 1. Niemand mag worden onderworpen aan willekeurige of onwettige inmenging in zijn privé-leven, zijn gezinsleven, zijn huis en zijn briefwisseling, noch aan onwettige aantasting van zijn eer en goede naam.

2. Eenieder heeft recht op bescherming door de wet tegen zodanige inmenging of aantasting ».

B.10.5. De artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie bepalen :

« Art. 7. Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn communicatie ».

« Art. 8. 1. Eenieder heeft recht op bescherming van zijn persoonsgegevens.

2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht van inzage in de over hem verzamelde gegevens en op rectificatie daarvan.

3. Een onafhankelijke autoriteit ziet erop toe dat deze regels worden nageleefd ».

Bij de toetsing aan de voormelde artikelen 7 en 8, dient rekening te worden gehouden met artikel 52, lid 1, van het Handvest, dat bepaalt :

« Beperkingen op de uitoefening van de in dit Handvest erkende rechten en vrijheden moeten bij wet worden gesteld en de wezenlijke inhoud van die rechten en vrijheden eerbiedigen. Met inachtneming van het evenredigheidsbeginsel kunnen slechts beperkingen worden gesteld, indien zij noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen ».

B.11. Het recht op eerbiediging van het privéleven, zoals gewaarborgd in de voormelde grondwets- en verdragsbepalingen, heeft als essentieel doel de personen te beschermen tegen inmengingen in hun privéleven.

Dat recht heeft een ruime draagwijdte en omvat, onder meer, de bescherming van persoonsgegevens en van persoonlijke informatie. De rechtspraak van het Europees Hof voor de Rechten van de Mens doet ervan blijken dat, onder meer, de volgende gegevens en informatie betreffende personen vallen onder de bescherming van dat recht : de naam, het adres, de professionele activiteiten, de persoonlijke relaties, digitale vingerafdrukken, camerabeelden, foto's, communicatiegegevens, DNA-gegevens, gerechtelijke gegevens (veroordeling of verdenking), financiële gegevens en informatie over bezittingen (zie onder meer EHRM, 23 maart 1987, *Leander* t. Zweden, § § 47-48; grote kamer, 4 december 2008, *S. en Marper* t. Verenigd Koninkrijk, § § 66-68; 17 december 2009, *B.B.* t. Frankrijk, § 57; 10 februari 2011, *Dimitrov-Kazakov* t. Bulgarije, § § 29-31; 18 oktober 2011, *Khelili* t. Zwitserland, § § 55-57; 9 oktober 2012, *Alkaya* t. Turkije, § 29; 18 april 2013, *M.K.* t. Frankrijk, § 26; 18 september 2014, *Brunet* t. Frankrijk, § 31).

B.12. De rechten die bij artikel 22 van de Grondwet en bij artikel 8 van het Europees Verdrag voor de rechten van de mens worden gewaarborgd, zijn evenwel niet absoluut.

Zij sluiten een overheidsinmenging in het recht op eerbiediging van het privéleven niet uit, maar vereisen dat zij wordt toegestaan door een voldoende precieze wettelijke bepaling, dat zij beantwoordt aan een dwingende maatschappelijke behoefte in een democratische samenleving en dat zij evenredig is met de daarmee nagestreefde wettige doelstelling. Die bepalingen houden voor de overheid bovendien de positieve verplichting in om maatregelen te nemen die een daadwerkelijke eerbiediging van het privéleven verzekeren, zelfs in de sfeer van de onderlinge verhoudingen tussen individuen (EHRM, 27 oktober 1994, *Kroon e.a.* t. Nederland, § 31; grote kamer, 12 oktober 2013, *Söderman* t. Zweden, § 78).

B.13.1. Doordat artikel 22 van de Grondwet aan de bevoegde wetgever de bevoegdheid voorbehoudt om vast te stellen in welke gevallen en onder welke voorwaarden afbreuk kan worden gedaan aan het recht op eerbiediging van het privéleven, waarborgt het aan elke burger dat geen enkele inmenging in dat recht kan plaatsvinden dan krachtens regels die zijn aangenomen door een democratisch verkozen beraadslagende vergadering.

Een delegatie aan een andere macht is evenwel niet in strijd met het wettigheidsbeginsel 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.

B.13.2. Naast de formele wettigheidsvereiste legt artikel 22 van de Grondwet eveneens de verplichting op dat de inmenging in het recht op eerbiediging van het privéleven in duidelijke en voldoende nauwkeurige bewoordingen wordt geformuleerd die het mogelijk maken de hypothesen te voorzien waarin de wetgever een dergelijke inmenging in het recht op eerbiediging van het privéleven toestaat.

Evenzo houdt de vereiste van voorzienbaarheid waaraan de wet moet voldoen om in overeenstemming te zijn met artikel 8 van het Europees Verdrag voor de rechten van de mens, in dat de formulering ervan voldoende precies is zodat eenieder - desnoods met gepast advies - in de gegeven omstandigheden in redelijke mate de gevolgen van een bepaalde handeling kan voorzien (EHRM, grote kamer, 4 mei 2000, *Rotaru* t. Roemenië, § 55; grote kamer, 17 februari 2004, *Maestri* t. Italië, § 30). De wetgeving moet eenieder een voldoende indicatie geven over de omstandigheden waarin en de voorwaarden waaronder de overheden gebruik mogen maken van maatregelen die raken aan de rechten gewaarborgd door het Verdrag (EHRM, grote kamer, 12 juni 2014, *Fernández Martínez* t. Spanje, § 117).

Meer in het bijzonder wanneer het optreden van de overheid een geheim karakter vertoont, dient de wet voldoende waarborgen te bieden tegen willekeurige inmengingen in het recht op eerbiediging van het privéleven, namelijk door de beoordelingsbevoegdheid van de betrokken overheden op voldoende duidelijke wijze af te bakenen, enerzijds, en door te voorzien in procedures die een effectief jurisdictioneel toezicht toelaten, anderzijds (EHRM, grote kamer, 4 mei 2000, *Rotaru* t. Roemenië, § 55; 6 juni 2006, *Segerstedt-Wiberg* t. Zweden, § 76; 4 juli 2006, *Lupsa* t. Roemenië, § 34).

B.13.3. Uit artikel 8 van het Europees Verdrag voor de rechten van de mens en artikel 22 van de Grondwet volgt aldus dat voldoende precies moet worden bepaald in welke omstandigheden een verwerking van persoonsgegevens is toegelaten (EHRM, grote kamer, 4 mei 2000, *Rotaru* t. Roemenië, § 57; grote kamer, 12 januari 2010, *S. en Marper* t. Verenigd Koninkrijk, § 99).

De vereiste graad van precisie van de betrokken wetgeving - die niet in elke hypothese kan voorzien - is, volgens het Europees Hof voor de Rechten van de Mens, onder meer afhankelijk van het domein dat wordt gereguleerd en van het aantal en de hoedanigheid van de personen tot wie de wet is gericht (EHRM, grote kamer, 12 januari 2010, *S. en Marper* t. Verenigd Koninkrijk, § § 95 en 96). Zo heeft het Europees Hof voor de Rechten van de Mens geoordeeld dat de vereiste van voorzienbaarheid in domeinen die te maken hebben met de nationale veiligheid, niet dezelfde draagwijdte kan hebben als in andere domeinen (EHRM, 26 maart 1987, *Leander* t. Zweden, § 51; 4 juli 2006, *Lupsa* t. Roemenië, § 33).

B.14.1. Een overheidsinmenging in het recht op eerbiediging van het privéleven dient niet alleen te steunen op een voldoende precieze wettelijke bepaling, maar ook te beantwoorden aan een dwingende maatschappelijke behoefte in een democratische samenleving en evenredig te zijn met de daarmee nagestreefde wettige doelstelling.

De wetgever beschikt ter zake over een appreciatiemarge. Die appreciatiemarge is evenwel niet onbegrensd : opdat een wettelijke regeling verenigbaar is met het recht op eerbiediging van het privéleven, is vereist dat de wetgever een billijk evenwicht heeft ingesteld tussen alle rechten en belangen die in het geding zijn.

B.14.2. Bij de beoordeling van dat evenwicht houdt het Europees Hof voor de Rechten van de Mens onder meer rekening met de bepalingen van het Verdrag van de Raad van Europa van 28 januari 1981 « tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens » (hierna : Verdrag nr. 108) (EHRM, 25 februari 1997, *Z* t. Finland, § 95; grote kamer, 12 januari 2010, *S. en Marper* t. Verenigd Koninkrijk, § 103).

Dat Verdrag bevat onder meer de beginselen inzake de verwerking van persoonsgegevens : rechtmatigheid, behoorlijkheid, transparantie, doelbinding, evenredigheid, juistheid, opslagbeperking, integriteit en vertrouwelijkheid, en verantwoordingsplicht.

Te dezen dient bij de invulling ervan in het bijzonder rekening te worden gehouden met de inhoud van de aanbeveling (2010)13.

B.14.3. Een inmenging in het recht op eerbiediging van het privéleven door middel van een verwerking van persoonsgegevens, te dezen door een toegang van overheidsdiensten tot en het gebruik van bepaalde persoonsgegevens via bijzondere technieken (EHRM, 23 maart 1987, *Leander* t. Zweden, § 48; grote kamer, 4 mei 2000, *Rotaru* t. Roemenië, § 46; HvJ, grote kamer, 8 april 2014, C-293/12, *Digital Rights Ireland Ltd*, en C-594/12, *Kärntner Landesregierung e.a.*), moet derhalve berusten op een redelijke verantwoording en dient evenredig te zijn met de door de wetgever nagestreefde doelstellingen.

B.14.4. Wat de evenredigheid betreft, houden het Europees Hof voor de Rechten van de Mens en het Hof van Justitie van de Europese Unie rekening met het al dan niet aanwezig zijn van de in B.13.2 vermelde materiële en procedurele waarborgen in de betrokken regeling.

Bij de beoordeling van de evenredigheid van maatregelen met betrekking tot de verwerking van persoonsgegevens, dient aldus rekening te worden gehouden met, onder meer, het geautomatiseerde karakter ervan, de gebruikte technieken, de accuraatheid, de pertinentie en het al dan niet buitensporige karakter van de gegevens die worden verwerkt, het al dan niet voorhanden zijn van maatregelen die de duur van de bewaring van de gegevens beperken, het al dan niet voorhanden zijn van een systeem van onafhankelijk toezicht dat toelaat na te gaan of de bewaring van de gegevens nog langer is vereist, het al dan niet voorhanden zijn van afdoende controlerechten en rechtsmiddelen voor de betrokkenen, het al dan niet voorhanden zijn van waarborgen ter voorkoming van stigmatisering van de personen van wie de gegevens worden verwerkt, het onderscheidend karakter van de regeling en het al dan niet voorhanden zijn van waarborgen ter voorkoming van foutief gebruik en misbruik van de verwerkte persoonsgegevens door de overheidsdiensten (EHRM, grote kamer, 4 mei 2000, *Rotaru* t. Roemenië, § 59; beslissing, 29 juni 2006, *Weber en Saravia* t. Duitsland, § 135; 28 april 2009, *K.H. e.a. t.* Slowakije, § § 60-69; grote kamer, 12 januari 2010, *S. en Marper* t. Verenigd Koninkrijk, § § 101-103, 119, 122 en 124; 18 april 2013, *M.K.* t. Frankrijk, § § 37 en 42-44; 18 september 2014, *Brunet* t. Frankrijk, § § 35-37; 12 januari 2016, *Szabó en Vissy* t. Hongarije, § 68; HvJ, grote kamer, 8 april 2014, C-293/12, *Digital Rights Ireland Ltd*, en C-594/12, *Kärntner Landesregierung e.a.*, punten 56-66).

B.15.1. De artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie hebben, wat de verwerking van persoonsgegevens betreft, een draagwijdte die analoog is aan die van artikel 8 van het Europees Verdrag voor de rechten van de mens (HvJ, grote kamer, 9 november 2010, C-92/09 en C-93/09, *Volker und Markus Schecke GbR e.a.*) en van artikel 22 van de Grondwet. Hetzelfde geldt voor artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten.

B.15.2. De bestaanbaarheid van wetskrachtige bepalingen met de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie, in samenhang gelezen met analoge grondwetsbepalingen of met de artikelen 10 en 11 van de Grondwet, kan slechts door het Hof worden onderzocht in zoverre de bestreden bepalingen het Unierecht ten uitvoer brengen (HvJ, grote kamer, 26 februari 2013, C-617/10, *Åklagaren*, punten 17 e.v.).

Te dezen dient rekening te worden gehouden met de richtlijn 95/46/EG en de algemene verordening gegevensbescherming.

B.15.3. Vermits de bestreden bepalingen betrekking hebben op de verwerking van persoonsgegevens die onder het toepassingsgebied van die wetgevingshandelingen van de Unie vallen, worden de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie in samenhang gelezen met analoge grondwetsbepalingen of met de artikelen 10 en 11 van de Grondwet.

Ten aanzien van het enige middel

B.16. De grieven van de verzoekende partij hebben in hoofdorde betrekking op de bestaanbaarheid van diverse aspecten van het « push »-systeem en de vooropgestelde « data mining » met het recht op eerbiediging van het privéleven.

Wat de voorzienbaarheid van de wet betreft

B.17. De verzoekende partij vordert de vernietiging van de artikelen 2, 3 en 4 van de bestreden wet omdat de inmenging in het recht op eerbiediging van het privéleven niet bestaanbaar zou zijn met de in B.9 vermelde bepalingen doordat er geen of een onvoldoende precieze wettelijke grondslag voor de door de wetgever beoogde inmenging zou zijn en doordat de artikelen 3 en 4 onvoldoende precies zouden zijn.

B.18. Eenieder dient voldoende precies te weten in welke omstandigheden en onder welke voorwaarden een inmenging in zijn privéleven, in het bijzonder door de geautomatiseerde verwerking van persoonsgegevens, is toegelaten. Derhalve moet eenieder een voldoende duidelijk inzicht hebben in de gegevens die worden verwerkt, de betrokkenen bij, de voorwaarden voor en de doeleinden van de verwerking.

Gelet op de artikelen 5, *b)*, en 9, lid 2, van het Verdrag nr. 108 en het beginsel 3.4 van de aanbeveling (2010)13, geldt dit vereiste des te meer wanneer persoonsgegevens door overheidsdiensten verder worden verwerkt voor andere doeleinden dan die waarvoor ze oorspronkelijk werden verkregen.

B.19. De wetgever heeft in het bestreden artikel 2 bepaald dat verbruiks- en adresgegevens dienen te worden verzameld en doorgestuurd aan de KSZ door de nutsbedrijven en de distributienetbeheerders op basis van het overschrijden van een afwijkingsdrempel met betrekking tot het gemiddelde verbruik voor een bepaalde gezinssamenstelling, dat die gegevens door de KSZ worden gefilterd, gekruist met andere gegevens om na te gaan of de betrokkene is gekend als sociaal gerechtigde, en ten slotte dat ze worden doorgestuurd aan de OISZ's en de sociaal inspecteurs zodat deze laatsten op basis van de ontvangen gegevens, in combinatie met gegevens in het netwerk zoals bedoeld in de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid (hierna : KSZ-Wet), na machtiging van het sectoraal comité van de sociale zekerheid en van de gezondheid, kunnen onderzoeken of een sociale uitkering wordt toegekend op basis van een fictief adres. De wetgever heeft in het bestreden artikel 4 duidelijk bepaald dat de verbruiksgegevens slechts een bijkomend en geen determinerend element kunnen zijn om tot fraude door een gerechtigde op sociale prestaties te besluiten.

De wetgever heeft in het bestreden artikel 3 de mogelijkheid gecreëerd voor OISZ's om gegevens samen te voegen met het oog op analyses van die gegevens teneinde zo meer gerichte controles uit te voeren op basis van risico-indicatoren voor sociale domiciliefraude.

Artikel 104 van de programmawet (I) van 29 maart 2012 bepaalt voorts dat de bepalingen van de Privacywet blijven gelden, zodat de algemene voorwaarden voor de verwerking van persoonsgegevens in artikel 4 van die wet ook gelden in het kader van de thans bestreden inmenging.

B.20. Uit hetgeen voorafgaat, in het bijzonder rekening houdend met de in B.4 vermelde parlementaire voorbereiding, volgt dat de inmenging berust op een wettelijke grondslag, zodat eenieder op voldoende precieze wijze de omstandigheden en de voorwaarden betreffende de verwerking van zijn persoonsgegevens kan kennen. De inmenging in het recht op bescherming van het privéleven beantwoordt derhalve aan de in B.13.2 vermelde vereisten.

B.21. Rekening houdend evenwel met de bewoordingen van het bestreden artikel 3, in het bijzonder de verwijzing naar « gecodeerde » en « gedecodeerde » gegevens, en met de in B.7.2.2 vermelde parlementaire voorbereiding en de daaruit voortvloeiende wil om zich te inspireren op de regeling voor de verwerking van persoonsgegevens door de FOD Financiën, is de verwijzing naar artikel 101 in de paragrafen 2 en 3 van dat artikel klaarblijkelijk een materiële vergissing.

In artikel 101/1, § § 2 en 3, van de programmawet (I) van 29 maart 2012, ingevoegd bij het bestreden artikel 3, dienen de woorden « in het kader van artikel 101, § 1 », respectievelijk « in artikel 101, § 1, bedoelde » te worden vernietigd.

Wat het wettigheidsbeginsel betreft

De bewaringstermijn van de gegevens

B.22. De verzoekende partij voert aan dat met betrekking tot de bij de bestreden artikelen 2 en 3 ingestelde inmenging niet alle voorwaarden waaronder afbreuk kan worden gedaan aan het recht op eerbiediging van het privéleven door de wetgever zijn vastgesteld, doordat de precieze bewaringstermijn door het sectoraal comité van de sociale zekerheid en van de gezondheid zou worden bepaald.

B.23. Artikel 4, § 1, 4° en 5°, van de Privacywet bepaalt dat de persoonsgegevens niet langer dan noodzakelijk voor het verwezenlijken van de doelstelling mogen worden bewaard en dat ze in voorkomend geval dienen te worden verbeterd of gewist. Rekening houdend met het feit dat de wetgever niet voor alle specifieke gevallen in afzonderlijke en precieze regels kan voorzien, vermocht hij de vereisten inzake de bewaring van persoonsgegevens en de duur van die bewaring op een algemene wijze te regelen.

Uit het voorgaande volgt dat de wetgever de essentiële elementen inzake de duur van de bewaring heeft geregeld.

De in B.22 aangevoerde grief is niet gegrond.

Wat het evenredigheidsbeginsel betreft

Het « push »-systeem

B.24. De verzoekende partij vordert de vernietiging van het bestreden artikel 2 omdat het daarin vervatte « push »-systeem verder zou gaan dan hetgeen noodzakelijk is voor de bestrijding van sociale domiciliefraude en de waarborgen inzake de bewaringstermijnen, het optreden van het sectoraal comité van de sociale zekerheid en van de gezondheid, de controlerechten van de betrokkenen, de procedure en de veiligheid, zouden ontbreken of niet voldoen.

B.25. Gelet op het feit dat het « push »-systeem ingevolge de omvang en de techniek van de verwerking van persoonsgegevens, een ernstige inmenging in het privéleven inhoudt, dient die inmenging niet alleen een wettelijke grondslag te hebben, maar dient zij ook te beantwoorden aan de in B.14 vermelde vereisten.

B.26. Zoals reeds in B.2 is vermeld, beoogde de wetgever de sociale fraude, die nauw verband houdt met het gebruik van een fictieve woonplaats, effectiever en efficiënter te bestrijden.

Aldus streefde de wetgever met de bestreden maatregel een legitieme doelstelling na.

B.27. De wetgever dient die doelstelling ook met een adequate maatregel na te streven.

B.28. De wetgever vermocht redelijkerwijs te oordelen dat het « push »-systeem adequaat is om het nagestreefde doel te bereiken daar het toelaat om, zonder dat er *a priori* een vermoeden van fraude is lastens een specifieke gerechtigde, verbruiksgegevens op basis van afwijkend verbruik als een autonoom signaal voor mogelijke domiciliefraude te hanteren, hetgeen toelaat om met een beperkte personeelscapaciteit toch meer het gebruik van potentieel fictieve adressen te detecteren en vervolgens ook gerichte controles uit te oefenen.

B.29. Wat de noodzakelijkheid van de inmenging in het recht op eerbiediging van het privéleven bij de verwerking van persoonsgegevens betreft, dient te worden nagegaan welke impact de bestreden regeling, rekening houdend met de bestaande waarborgen, heeft op dat privéleven en of die regeling geen onevenredige afbreuk doet aan de in B.14 vermelde waarborgen.

B.30.1. De overheden, diensten, instellingen of personen die persoonsgegevens, via het in de bestreden wet beoogde systeem selecteren, doorgeven of ontvangen, dienen de toepasselijke bepalingen van de Privacywet te eerbiedigen.

B.30.2. Te dezen heeft de wetgever met de Privacywet ervoor gekozen een algemene wettelijke regeling, die zowel voor de publieke als private sector geldt, aan te nemen (*Parl. St.*, Kamer, 1990-1991, nr. 1610/1, p. 3), waarbij desalniettemin rekening wordt gehouden met de eigenheden van bepaalde sectoren en het verzoenen van allerlei belangen. Om die reden heeft de wetgever in artikel 104 van de programmawet (I) van 29 maart 2012 uitdrukkelijk de gelding van de Privacywet voor het « push »-systeem bevestigd.

B.30.3. De Privacywet bevat de regels die essentieel zijn voor de bescherming van het recht op eerbiediging van het privéleven : onder meer individuele waarborgen (artikel 4) op het stuk van de registratie van gegevens van gevoelige aard (artikelen 6 tot 8), het recht op toegang en verbetering (artikelen 10 en 12), de vertrouwelijkheid en beveiliging (artikel 16, § 4), de openbaarheid van de verwerkingen en de ruime informatieverstrekking aan de betrokken personen (artikelen 5 en 9) en de controle door een onafhankelijk orgaan (artikel 31) en door de hoven en rechtbanken (artikel 14). Op de door de wetgever aangewezen verantwoordelijke voor de verwerking rusten bijgevolg verschillende verplichtingen.

B.31. Desalniettemin kunnen de ernst, de aard en de omvang van de door de wetgever ingestelde verwerking van persoonsgegevens nopen tot specifieke of bijkomende waarborgen.

Rekening houdend met het gegeven dat het bestreden systeem erin bestaat automatisch - dit is zonder enig voorafgaand vermoeden van de overheidsdiensten jegens individuele gerechtigden van sociale prestaties - vermoedens van domiciliefraude te signaleren, heeft de wetgever ervoor gekozen verbruikers van gas, water of elektriciteit aan « profiling » te onderwerpen. Het is inherent aan die techniek dat gebruik wordt gemaakt van bepaalde parameters om in verbruiksgegevens van een ongedifferentieerd aantal personen een bepaald gedrag (fraude) als signaal te detecteren of om zulk gedrag te voorspellen op basis van een analyse van die massa gegevens. Het voormelde signaal wordt te dezen gedestilleerd uit de vergelijking van het reële verbruik van water, gas en elektriciteit op een bepaald adres met het gemiddelde verbruik voor de officieel meegedeelde gezinssamenstelling op datzelfde adres.

Die verwerkingstechniek houdt desalniettemin risico's voor het recht op bescherming van het privéleven van de betrokkenen in (zie het Explanatory Memorandum bij de aanbeveling (2010)13, punten 50-64) doordat onder meer verkeerde verbanden tussen kenmerken van een bepaald gedrag en personen kunnen worden gelegd. Derhalve dient de wetgever te voorzien in voldoende waarborgen.

B.32.1. De verzoekende partij voert aan dat niet voor alle fases van het « push »-systeem een verantwoordelijke voor de verwerking werd aangewezen.

B.32.2. Voorafgaand aan het « push »-systeem gebeurt de verwerking van de verbruiks- en adresgegevens in het kader van de normale bedrijfsvoering door de nutsbedrijven en de distributienetbeheerders overeenkomstig de bepalingen van de Privacywet, die daarvoor een verantwoordelijke in de zin van artikel 1, § 4, van de Privacywet dienen aan te wijzen.

Wat de selectie van de door te sturen gegevens en de eigenlijke gegevensstroom in het kader van het bestreden systeem betreft, heeft de wetgever er echter voor gekozen de KSZ als verantwoordelijke voor de verwerking aan te wijzen.

Bijgevolg heeft de wetgever bepaald dat de in B.30 vermelde verplichtingen in het kader van het « push »-systeem in de eerste plaats rusten op de KSZ, die ook verantwoordelijk is voor de naleving ervan bij de verwerker in de zin van artikel 1, § 5, van de Privacywet, te dezen de nutsbedrijven en de distributienetbeheerders.

De in B.32.1 aangevoerde grief is niet gegrond.

B.33.1. De verzoekende partij voert aan dat de verwerking van de persoonsgegevens via het bestreden systeem niet minimaal is.

B.33.2. De wetgever verplicht de nutsbedrijven en de distributienetbeheerders om in het kader van het bestreden systeem enkel verbruiks- en de daaraan gekoppelde adresgegevens verplicht te verzamelen. De aldus opgelegde verplichting is beperkt tot twee gegevens die voor de normale bedrijfsvoering worden aangewend.

De nutsbedrijven en de distributienetbeheerders worden vervolgens verplicht de verbruiks- en adresgegevens door te sturen naar de KSZ. Het doorzenden is door de wetgever wel afhankelijk gemaakt van een zwaarwichtigheidsdrempel, namelijk de afwijking van meer dan 80 pct. ten opzichte van het gemiddelde verbruik voor de officieel meegedeelde gezinssamenstelling.

B.33.3. Het is aannemelijk dat er een verband bestaat tussen de gezinssamenstelling en het verbruik van water, gas en elektriciteit. Aldus kan op basis van de verbruiksgegevens een afwijking ten opzichte van het verwachte gemiddelde verbruik voor het officieel meegedeelde gezinstype worden afgeleid. Rekening houdend met hetgeen in B.3.5 is vermeld en met de beleidsmarge van de wetgever bij complexe beoordelingen, blijkt niet dat de voormelde drempel kennelijk onredelijk zou zijn.

B.34. Die drempel laat immers toe het aantal personen van wie de gegevens dienen te worden doorgestuurd naar de KSZ te beperken tot diegenen voor wie er redelijke gronden aanwezig zijn voor verder onderzoek, des te meer daar het gaat om een significante afwijking.

B.35. Alvorens de ontvangen gegevens te bezorgen aan de sociale inspectie of een OISZ wordt door de KSZ via het personenrepertorium (artikel 6 van de KSZ-Wet), na kruising met gegevens in het Rijksregister nagegaan of de verbruiks- en adresgegevens betrekking hebben op een gerechtigde van sociale prestaties, hetgeen ertoe leidt dat in de laatste fase uiteindelijk enkel de gegevens van de gerechtigden voor wie een vermoeden van sociale domiciliefraude bestaat, worden doorgestuurd.

B.36. Uit hetgeen voorafgaat, volgt dat de wetgever erin heeft voorzien dat de structurele en omvangrijke gegevensstroom wordt gefilterd en beperkt tot hetgeen noodzakelijk is in de strijd tegen sociale domiciliefraude.

Aldus hebben de overheidsdiensten via het « push »-systeem slechts toegang tot de gegevens die zij voor hun controle op het al dan niet fictieve karakter van de woonplaats van een sociaal gerechtigde nodig hebben. Die verwerking heeft derhalve geen onevenredige gevolgen.

De in B.33.1 aangevoerde grief is niet gegrond.

B.37.1. De verzoekende partij voert aan dat de controlerechten van de betrokkenen bij de verwerking van hun persoonsgegevens worden miskend doordat de rechtstreekse uitoefening ervan wordt uitgesloten.

B.37.2. Artikel 3, § 5, 3°, van de Privacywet bepaalt dat de artikelen 9, 10, § 1, en 12 van diezelfde wet (recht op informatie, toegang, verbetering en uitwissing) niet van toepassing zijn op de bij koninklijk besluit met het oog op de uitoefening van hun opdrachten van bestuurlijke politie aangewezen openbare overheden. Ter uitvoering van artikel 3, § 5, 3°, van de Privacywet bepaalt artikel 1 van het koninklijk besluit van 11 maart 2015 :

« § 1. De artikelen 9, 10, § 1, en 12 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens zijn niet van toepassing op de sociale inspecteurs en op de ambtenaren van de openbare overheden opgesomd in § 2, in het raam van hun opdrachten van bestuurlijke politie bedoeld in Boek 1, Titel 2 en Titel 4, Hoofdstuk 3 van het Sociaal Strafwetboek.

§ 2. Deze overheden zijn :

- Federale Overheidsdienst Werkgelegenheid, Arbeid en Sociaal Overleg;
- Rijksdienst voor Arbeidsvoorziening;
- Rijksdienst voor Sociale Zekerheid;
- Rijksdienst voor Jaarlijkse Vakantie;
- Rijksinstituut voor Ziekte- en Invaliditeitsverzekering;
- Federaal Agentschap voor de Kinderbijslag;
- Dienst voor de Bijzondere Socialezekerheidsstelsels;
- Fonds voor Arbeidsongevallen;
- Fonds voor de Beroepsziekten;
- Controledienst voor de Ziekenfondsen en de Landsbonden van ziekenfondsen;
- Rijksdienst voor Pensioenen;
- Rijksinstituut voor de sociale verzekeringen der zelfstandigen ».

Aldus kan een betrokkene zijn controlerechten met betrekking tot de verwerking door sociaal inspecteurs en de OISZ's, in zoverre die verwerking past in het kader van de uitoefening van hun opdrachten van bestuurlijke politie, niet rechtstreeks uitoefenen.

B.37.3. Artikel 13 van de Privacywet bepaalt evenwel :

« Eenieder die zijn identiteit bewijst, is gerechtigd zich kosteloos tot de Commissie voor de bescherming van de persoonlijke levenssfeer te wenden, teneinde de in de artikelen 10 en 12 bedoelde rechten uit te oefenen ten aanzien van de verwerkingen van persoonsgegevens bedoeld in artikel 3, § § 4, 5, 6 en 7.

De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en bij een in Ministerraad overlegd besluit, de wijze waarop deze rechten worden uitgeoefend.

De Commissie voor de bescherming van de persoonlijke levenssfeer deelt uitsluitend aan de betrokkene mede dat de nodige verificaties werden verricht.

Evenwel bepaalt de Koning, na advies van de commissie voor de bescherming van de persoonlijke levenssfeer, bij een in Ministerraad overlegd besluit, welke informatie de commissie aan de betrokkene mag meedelen indien het verzoek van de betrokkene een verwerking van persoonsgegevens betreft door politiediensten met het oog op identiteitscontrole ».

Een betrokkene kan aldus zijn controlerechten via de Privacycommissie uitoefenen.

B.38.1. Krachtens artikel 9, lid 2, van het Verdrag nr. 108 kan van de in artikel 8 van dat Verdrag vermelde controlerechten worden afgeweken, in zoverre een wet daarin voorziet en in zoverre die afwijking noodzakelijk is in een democratische samenleving ten behoeve van de bescherming van de veiligheid van de Staat, de openbare veiligheid, de geldelijke belangen van de Staat, de bestrijding van strafbare feiten, de bescherming van de betrokkene en de bescherming van de rechten en vrijheden van anderen.

B.38.2. De effectiviteit en de efficiëntie van de strijd tegen fraude - en dus de bescherming van de geldelijke belangen van de Staat en de rechten van anderen in een sociaal systeem - kunnen rechtvaardigen dat de controlerechten van de betrokkenen op de verwerking van hun persoonsgegevens worden beperkt in zoverre die beperking van de toegang in het kader van de bestuurlijke politie enkel betrekking heeft op de gegevens van sociaal gerechtigden en de uitsluiting van de rechtstreekse toegang niet langer duurt dan nodig is voor het onderzoek.

Uit hetgeen in B.37 is vermeld, volgt dat de niet-toepassing van de artikelen 9, 10 en 12 van de Privacywet alsook de indirecte toegang, waarin is voorzien bij artikel 13 van de Privacywet, is beperkt tot de gegevens die door de twaalf bedoelde overheden en de sociaal inspecteurs worden verwerkt in het raam van hun opdrachten van bestuurlijke politie. Met betrekking tot gegevens die door die openbare overheden en de sociaal inspecteurs worden verwerkt voor andere opdrachten of doeleinden, zijn zij ertoe gehouden de artikelen 9, 10 en 12 van de Privacywet na te leven.

Indien evenwel de noden van een onderzoek het niet meer rechtvaardigen, is het zonder redelijke verantwoording de betrokkene de rechtstreekse toegang tot en de controle van zijn persoonsgegevens te ontzeggen.

B.38.3. Onder voorbehoud van hetgeen in B.38.2, laatste alinea, is vermeld, is de in B.37.1 aangevoerde grief niet gegrond.

B.39.1. De verzoekende partij voert aan dat er onvoldoende waarborgen met betrekking tot de veiligheid en de vertrouwelijkheid zijn.

B.39.2. Artikel 16, § 4, van de Privacywet bepaalt dat de verantwoordelijke voor de verwerking alsmede de verwerker zelf gepaste organisatorische en technische maatregelen moeten nemen die nodig zijn voor de bescherming van de persoonsgegevens, rekening houdend met de stand van de techniek en met de aard van de te beveiligen gegevens en de potentiële risico's. De wetgever heeft uitdrukkelijk bepaald met welke risico's rekening dient te worden gehouden bij het nemen van die veiligheidsmaatregelen (toevallige vernietiging van gegevens, toevallig verlies van gegevens, ongeoorloofde wijziging van gegevens, enz.).

B.39.3. Naast de waarborgen in de Privacywet heeft de wetgever ook in waarborgen voorzien in de KSZ-Wet inzake het beroepsgeheim, de aanstelling van een veiligheidsconsulent en veiligheidsmaatregelen (artikelen 22, 23, 24, 25 en 28 van de KSZ-Wet). Ook wat de sociale inspectie betreft, waarborgt artikel 58 van het Sociaal Strafwetboek de vertrouwelijkheid van sociale gegevens waarmee de sociale inspectie in aanraking komt. De wetgever heeft eveneens in sancties voorzien in de artikelen 213 tot 215 van het Sociaal Strafwetboek bij miskenning van de vertrouwelijkheid van gegevens of bij het niet-nemen van de vereiste veiligheidsmaatregelen.

B.39.4. Uit hetgeen voorafgaat, blijkt dat de wetgever heeft voorzien in waarborgen om de veiligheid en de vertrouwelijkheid van de verwerkte persoonsgegevens te waarborgen.

De in B.39.1 aangevoerde grief is niet gegrond.

B.40. De verzoekende partij voert de ontstentenis aan van procedurele waarborgen zoals die bijvoorbeeld vervat liggen in de wet van 3 augustus 2012 « houdende bepalingen betreffende de verwerking van persoonsgegevens door de Federale Overheidsdienst Financiën in het kader van zijn opdrachten ».

B.41. De gegevens die in het kader van het « push »-systeem worden verwerkt, kunnen door de overheidsdiensten slechts worden gebruikt als bijkomend element om uit te maken of een sociaal gerechtigde domiciliefraude heeft gepleegd (artikel 102 van de programmawet (I) van 29 maart 2012, zoals vervangen bij artikel 4 van de bestreden wet), hetgeen een onmiddellijke nadelige impact voor de betrokkene tegengaat. De bevoegde overheidsinstanties dienen immers in voorkomend geval over andere elementen te beschikken om een nadelige beslissing (bv. sancties in geval van fraude) ten aanzien van een sociaal gerechtigde te nemen. De wetgever heeft in artikel 103 van de programmawet (I) van 29 maart 2012, zoals gewijzigd bij artikel 5 van de bestreden wet, bepaald dat de sociaal inspecteurs de betrokkene of een derde inlichten over de mogelijkheid dat zijn verbruiksgegevens kunnen worden gebruikt in een administratief onderzoek. Krachtens artikel 79 van het Sociaal Strafwetboek hebben de betrokkenen ook toegang tot het administratief dossier.

B.42. Indien er uiteindelijk een « vaststelling » van domiciliefraude zou volgen als resultaat van het « push »-systeem, kan de betrokken sociaal gerechtigde bovendien alle feitelijke en juridische elementen aanvoeren om aan te tonen dat er geen sprake is van domiciliefraude. De betrokkene geniet krachtens de algemene beginselen van behoorlijk bestuur of de regels inzake de strafrechtspleging waarborgen met betrekking tot zijn rechten van verdediging.

B.43. Artikel 14 van de Privacywet bepaalt dat de voorzitter van de rechtbank van eerste aanleg, zitting houdende zoals in kort geding, kennis neemt van de vorderingen betreffende het door of krachtens de wet verleende recht om kennis te krijgen van persoonsgegevens, alsook van de vorderingen tot verbetering, tot verwijdering of tot het verbieden van de aanwending van onjuiste persoonsgegevens of van gegevens die gelet op het doel van de verwerking onvolledig of niet ter zake dienend zijn, dan wel waarvan de registratie, de mededeling of de bewaring verboden is, tegen de verwerking waarvan de betrokkene zich heeft verzet of die langer bewaard werden dan de toegestane duur. Krachtens artikel 32, § 3, van de Privacywet, kan de voorzitter van de Commissie voor de bescherming van de persoonlijke levenssfeer, in voorkomend geval na een klacht van een betrokkene, ieder geschil aangaande de toepassing van die wet en haar uitvoeringsmaatregelen aan de rechtbank van eerste aanleg voorleggen.

Een betrokkene beschikt derhalve over rechtsmiddelen om de inmenging in zijn recht op bescherming van het privéleven door de verwerking van persoonsgegevens aan de rechter ter controle voor te leggen.

B.44. Uit hetgeen voorafgaat blijkt dat de bestreden wet voldoende procedurele waarborgen biedt.

De in B.40 aangevoerde grief is niet gegrond.

B.45. De verzoekende partij voert aan dat er onvoldoende specifieke bewaringstermijnen door de wetgever zijn vastgesteld.

B.46. Krachtens artikel 4, § 1, 3°, 4° en 5°, van de Privacywet geldt voor elke fase in het licht van de specifieke doelstelling de verplichting om persoonsgegevens die niet (meer) relevant of foutief zijn niet langer te verwerken, ze te verbeteren dan wel uit te wissen en ze in ieder geval niet langer te bewaren dan nodig is voor de nagestreefde specifieke doelstelling, te dezen de verzameling en de doorzending van verbruiksgegevens aan de KSZ, de koppeling en het doorzenden van die gegevens door de KSZ aan de belanghebbende overheidsdiensten. Voor de OISZ's en sociaal inspecteurs geldt eveneens dat zij de gegevens niet langer mogen bewaren dan nodig is voor het uitvoeren van controles op het gebruik van een fictief adres in het kader van uitkeringsfraude, hetgeen impliceert dat zij in ieder geval niet langer dan de verjaringstermijn in geval van fraude mogen worden bewaard.

De in B.45 aangevoerde grief is niet gegrond.

B.47. De verzoekende partij voert nog aan dat de wetgever niet heeft gekozen voor de minst verregaande maatregel om de strijd tegen de sociale domiciliefraude te versterken.

B.48. Uit de in B.2 vermelde parlementaire voorbereiding blijkt dat de wetgever twee alternatieven betreffende de wijze om verbruiksgegevens te betrekken in de strijd tegen sociale domiciliefraude in overweging heeft genomen : het « pull »-systeem (*status quo*) en het « push »-systeem (nieuw instrument).

B.49. In beide systemen krijgen de overheidsdiensten, met het oog op controle op sociale domiciliefraude, in geval van een vermoeden van fraude enkel kennis van de verbruiksgegevens van gerechtigden op sociale prestaties.

Het wezenlijk verschil tussen de beide systemen betreft de wijze waarop de overheid tot het voormelde vermoeden van fraude komt. In het bestreden systeem wordt dat vermoeden gevoed door technologische processen waarbij verbruiksgegevens van alle consumenten structureel en automatisch worden gescreend om aan de hand van een profiel fraudeknipperlichten te laten afgaan terwijl in het « pull »-systeem geen gegevens van derden worden betrokken.

B.50. Gelet op het feit dat de strijd tegen sociale domiciliefraude een permanente strijd is waarvoor blijvende inspanningen noodzakelijk zijn, alsook dat frauduleus handelen en de strijd daartegen onderhevig zijn aan veranderingen in het sociaal gedrag, en in het bijzonder op de voorhanden zijnde technische hulpmiddelen, kon de wetgever redelijkerwijs oordelen dat de strijd tegen sociale fraude effectiever en efficiënter kan worden gevoerd in het kader van het « push »-systeem.

B.51. Uit de uiteenzetting van het « pull »-systeem in B.1.3 blijkt dat dit systeem een enorme inzet van personeel en middelen vereist om met enige slagkracht de strijd tegen sociale domiciliefraude aan te gaan. Gelet op de beperkte actieradius ervan lijkt dat systeem niet in staat om dezelfde aantallen van sociaal gerechtigden aan een onderzoek te onderwerpen en bijgevolg ook niet om dezelfde aantallen vermoedelijke fraudegevallen als in het bestreden « push »-systeem te detecteren. Hetzelfde geldt *mutatis mutandis* eveneens voor de door de verzoekende partij aangevoerde onderzoeksinstrumenten zoals het huisbezoek, het inwinnen van informatie en het verhoor (artikelen 24, 26 en 27 van het Sociaal Strafwetboek). Gelet op de specifieke en individuele opvraging van gegevens, is het « pull »-systeem ook van dien aard dat het een stigmatiserende werking ten aanzien van de betrokkenen - enerzijds, als sociaal gerechtigde en, anderzijds, als vermoedelijke fraudeur - kan hebben en derhalve een nadelige impact op het privéleven kan teweegbrengen.

B.52. Het « push »-systeem verhindert door de rol van de KSZ dat de nutsbedrijven en de distributienetbeheerders zouden weten welke consumenten gerechtigden op sociale prestaties zijn, hetgeen de inmenging in het privéleven van de sociaal gerechtigden beperkt tot het strikt noodzakelijke. Uit hetgeen in B.29 tot B.44 is vermeld, blijkt eveneens dat de wetgever heeft voorzien in de nodige materiële en procedurele voorwaarden en waarborgen inzake de inmenging in het privéleven.

B.53. Uit hetgeen voorafgaat en inzonderheid rekening houdend met hetgeen in B.1.2 en B.52 is vermeld, alsook met de verschillen tussen de beide systemen, blijkt dat de wetgever redelijkerwijs kon oordelen dat het « push »-systeem, zoals ingesteld bij het bestreden artikel 2, niet verder gaat dan hetgeen voor het effectief en efficiënt detecteren, ontraden en aanpakken van sociale domiciliefraude noodzakelijk is.

De in B.47 vermelde grief is niet gegrond.

B.54. Het Hof dient nog na te gaan of het bestreden « push »-systeem, dat, zoals in B.3 is toegelicht, « profiling » en de verwerkingstechniek « data mining » impliceert, geen onevenredige gevolgen met zich meebrengt.

B.55. Gelet op het nagestreefde doel om onder meer de tot dan toe onmogelijk of zeer moeilijk vast te stellen vermoedelijke gevallen van domiciliefraude te detecteren, en rekening houdend met het ontradende karakter van het « push »-systeem, met de wijzigingen in het gedrag van personen in de doelgroep en met de onvoorspelbaarheid van het frauduleus handelen en van het aantal gevallen, is het niet zonder redelijke verantwoording dat de wetgever bij de vaststelling van de maatregel geen allesomvattende en definitieve inschattingen kan maken over de opbrengsten en de kosten verbonden aan het systeem en dus over de efficiëntie ervan.

De in B.54 vermelde grief is niet gegrond.

De « datawarehouse » en de « data mining »

B.56. De verzoekende partij vordert de vernietiging van artikel 3 omdat de samenvoeging en analyse van beschikbare gegevens door de OISZ's verder zou gaan dan hetgeen noodzakelijk is voor de bestrijding van sociale domiciliefraude, en omdat waarborgen zoals de vereiste van een machtiging door het sectoraal comité van de sociale zekerheid en van de gezondheid, en inzake integriteit en vertrouwelijkheid zouden ontbreken of onvoldoende zouden zijn.

B.57. Het samenvoegen van gegevens waarover de OISZ's en de eventueel daaronder ressorterende sociale inspectie kunnen beschikken, alsook het zoeken in die gegevens naar mogelijke verbanden en indicatoren met betrekking tot het risico op het gebruik van een fictief adres kunnen redelijkerwijs als een geschikt middel om de strijd tegen sociale domiciliefraude te versterken worden beschouwd.

B.58. Zoals blijkt uit hetgeen in B.30 is vermeld, gelden de waarborgen van de Privacywet ook in het kader van de verwerking, die voortvloeit uit het bestreden artikel 3.

B.59. De verzoekende partij voert aan dat er in het bestreden artikel 3 geen machtiging van een sectoraal comité van de sociale zekerheid en van de gezondheid wordt vereist voor wat het doorgeven van gegevens aan de sociaal inspecteurs betreft.

B.60. Rekening houdend met de in B.21 vermelde vernietiging en met de tot de OISZ's beperkte draagwijdte van het bestreden artikel is de in B.59 vermelde grief niet gegrond.

B.61. De verzoekende partij voert ten slotte aan dat het bestreden artikel 3 de beginselen inzake integriteit en vertrouwelijkheid schendt doordat er onvoldoende waarborgen zijn.

B.62. Artikel 16, § 4, van de Privacywet legt de OISZ's als verantwoordelijken voor de verwerking op om gepaste organisatorische en technische maatregelen te nemen die nodig zijn voor de bescherming van de persoonsgegevens, rekening houdend met de stand van de techniek en met de aard van de te beveiligen gegevens en de potentiële risico's. De wetgever heeft daarbij uitdrukkelijk bepaald met welke risico's rekening dient te worden gehouden bij het nemen van die veiligheidsmaatregelen (toevallige vernietiging van gegevens, toevallig verlies van gegevens, ongeoorloofde wijziging van gegevens, enz.).

De in B.61 vermelde grief is niet gegrond.

B.63. Uit hetgeen voorafgaat blijkt, mede rekening houdend met het initiële gecodeerde karakter van de beoogde analyses, dat artikel 3 van de bestreden wet niet verdergaat dan noodzakelijk is om de strijd tegen sociale domiciliefraude te versterken. Het detecteren van de verbanden en nieuwe indicatoren is bovendien noodzakelijk voor het opvolgen van evoluties in het frauduleus handelen en het opsporen van potentiële fraudegevallen.

De in B.56 vermelde grieven zijn niet gegrond.

Om die redenen,

het Hof

- vernietigt in de paragrafen 2 en 3 van artikel 101/1 van de programmawet (I) van 29 maart 2012, zoals ingevoegd bij artikel 3 van de wet van 13 mei 2016 « tot wijziging van de programmawet (I) van 29 maart 2012 betreffende de controle op het misbruik van fictieve adressen door de gerechtigden van sociale prestaties, met het oog op de invoering van het systematisch doorzenden naar de KSZ van bepaalde verbruiksgegevens van nutsbedrijven en distributienetbeheerders tot verbetering van de datamining en de datamatching in de strijd tegen de sociale fraude » de woorden « in het kader van artikel 101, § 1 », respectievelijk « in artikel 101, § 1, bedoelde »;

- verwerpt het beroep voor het overige, onder voorbehoud van hetgeen is vermeld in B.38.2, laatste alinea.

Aldus gewezen in het Nederlands, het Frans en het Duits, overeenkomstig artikel 65 van de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof, op 15 maart 2018.

De griffier,
P.-Y. Dutilleux

De voorzitter,
E. De Groot

COUR CONSTITUTIONNELLE

[2018/201410]

Extrait de l'arrêt n° 29/2018 du 15 mars 2018

Numéro du rôle : 6552

En cause : le recours en annulation partielle de la loi du 13 mai 2016 « modifiant la loi-programme (I) du 29 mars 2012 concernant le contrôle de l'abus d'adresses fictives par les bénéficiaires de prestations sociales, en vue d'introduire la transmission systématique de certaines données de consommation de sociétés de distribution et de gestionnaire de réseaux de distribution vers la BCSS améliorant le datamining et le datamatching dans la lutte contre la fraude sociale », introduit par l'ASBL « Ligue des Droits de l'Homme ».

La Cour constitutionnelle,

composée des présidents A. Alen et J. Spreutels, des juges L. Lavrysen, J.-P. Moerman, E. Derycke et F. Daoût, et, conformément à l'article 60*bis* de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, du président émérite E. De Groot, assistée du greffier P.-Y. Dutilleux, présidée par le président émérite E. De Groot,

I. *Objet du recours et procédure*

Par requête adressée à la Cour par lettre recommandée à la poste le 28 novembre 2016 et parvenue au greffe le 29 novembre 2016, l'ASBL « Ligue des Droits de l'Homme », assistée et représentée par Me R. Jespers, avocat au barreau d'Anvers, a introduit un recours en annulation partielle de la loi du 13 mai 2016 « modifiant la loi-programme (I) du 29 mars 2012 concernant le contrôle de l'abus d'adresses fictives par les bénéficiaires de prestations sociales, en vue d'introduire la transmission systématique de certaines données de consommation de sociétés de distribution et de gestionnaire de réseaux de distribution vers la BCSS améliorant le datamining et le datamatching dans la lutte contre la fraude sociale » (publiée au *Moniteur belge* du 27 mai 2016).

(...)

II. *En droit*

(...)

Quant au contexte des dispositions attaquées

B.1.1. La loi du 13 mai 2016 « modifiant la loi-programme (I) du 29 mars 2012 concernant le contrôle de l'abus d'adresses fictives par les bénéficiaires de prestations sociales, en vue d'introduire la transmission systématique de certaines données de consommation de sociétés de distribution et de gestionnaire de réseaux de distribution vers la BCSS améliorant le datamining et le datamatching dans la lutte contre la fraude sociale » (ci-après : la loi-programme (I) du 29 mars 2012), attaquée, règle, dans le cadre de la lutte contre la fraude sociale au domicile, premièrement l'échange de données entre, d'une part, les sociétés de distribution et les gestionnaires de réseaux de distribution et, d'autre part, les services publics et, deuxièmement, l'analyse d'une grande collection de données sociales. BCSS est l'abréviation de « Banque carrefour de la sécurité sociale ».

B.1.2. Par la loi attaquée, le législateur a voulu concrétiser son intention, clairement exprimée dans l'accord de gouvernement et dans les plans de politique successifs, de franchir une nouvelle étape dans la lutte contre la fraude sociale. Le législateur entendait lutter progressivement et plus efficacement contre la fraude sociale au domicile en prévoyant de nouveaux instruments de contrôle concernant l'usage abusif d'adresses fictives (*Doc. parl.*, Chambre, 2011-2012, DOC 53-2081/017, p. 22; *Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/001, p. 8; *Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/005, p. 54).

B.1.3. Avant l'entrée en vigueur de la loi-programme (I) du 29 mars 2012, les bénéficiaires de prestations sociales étaient susceptibles de se voir réclamer les données de leur consommation d'eau, de gaz et d'électricité, le cas échéant, à des fins de contrôle. La loi-programme précitée a légalement permis à l'inspection sociale de réclamer ces données de consommation auprès des sociétés de distribution et des gestionnaires de réseaux de distribution (système « pull »).

Avant sa modification par l'article 2 attaqué, l'article 101 de la loi-programme (I) du 29 mars 2012 disposait :

« Si, dans le cadre d'une enquête, les inspecteurs sociaux présument sur la base d'autres éléments qu'un bénéficiaire utilise une adresse fictive afin de prétendre à des prestations sociales auxquelles il ne peut pas prétendre, ils peuvent demander les données de consommation d'eau, d'électricité et de gaz aux sociétés de distribution et aux gestionnaires de réseau de distribution.

Ces données de consommation peuvent être utilisées comme indication supplémentaire afin de démontrer qu'il s'agit d'une adresse fictive ».

Dans les travaux préparatoires, cet article fait l'objet du commentaire suivant :

« En exécution de la notification budgétaire 2012, la présente section vise à fournir aux autorités de contrôle une série de nouveaux instruments qui permettraient aux pouvoirs publics de renforcer la lutte contre la fraude aux allocations. Il veut être une initiative afin de mieux contrôler les allocations. L'objectif est d'arriver à ce qu'à chaque assuré social soit payée l'allocation correcte.

En concret, il est rendu possible pour les inspecteur [s] sociaux de demander aux société [s] de distribution et aux gestionnaires de réseau de distribution les données de consommation d'eau, d'électricité et de gaz des personnes qui ont droit à une prestation sociale.

Celles-ci sont obligées à répondre à une telle demande en donnant les données » (*Doc. parl.*, Chambre, 2011-2012, DOC 53-2081/001, p. 71).

« Il est prévu de permettre aux inspecteurs sociaux de demander les données de consommation (d'eau, d'électricité et de gaz) aux sociétés de distribution et aux gestionnaires de réseau de distribution s'ils présument, sur la base d'autres éléments, que des bénéficiaires de prestations sociales commettent une fraude au domicile. Les sociétés de distribution et les gestionnaires de réseau de distribution, qui ne répondent pas toujours, aujourd'hui, à toutes les demandes d'informations, seront désormais obligés de répondre à ces demandes et de fournir les données demandées. Les informations fournies pourront constituer un indice supplémentaire d'abus mais pas une preuve concluante.

Cette mesure est une première étape mais ne réglera pas intégralement ce problème. D'autres réformes seront nécessaires à l'avenir pour lutter contre la fraude au domicile » (*Doc. parl.*, Chambre, 2011-2012, DOC 53-2081/017, p. 22).

B.1.4. Ce système « pull » n'a jamais été mis en pratique (*Doc. parl.*, Chambre, 2015-2016, DOC 54-0020/063, p. 14).

B.2.1. La loi attaquée remplace le système « pull », précité, par un système « push » et prévoit de nouvelles possibilités de « data mining » en matière de lutte contre la fraude sociale au domicile.

B.2.2. En ce qui concerne le passage au système « push » d'échange de données, les travaux préparatoires mentionnent ce qui suit :

« Le système actuel, appelé système ' pull ', dans lequel les sociétés de distribution et les gestionnaires de réseaux de distribution doivent transmettre ces données de consommation à la demande des services d'inspections, est converti en un système ' push '. Cela signifie que les sociétés de distribution et les gestionnaires de réseaux de distribution enverront dorénavant automatiquement et électroniquement à la [Banque-carrefour de la Sécurité Sociale; ci-après : la BCSS] les données de consommation visées. Ces données serviront d'indicateurs supplémentaires afin de permettre aux services d'inspection sociale de mieux détecter [la] fraude au domicile. Concrètement, les données de consommation seront utilisées par le BCSS pour le datamatching et, dans une phase ultérieure, comme des indicateurs supplémentaires pour le datamining. De cette manière le gouvernement rencontre le point 31 de l'avis de la Commission de la protection de la vie privée (CPVP) de ne pas transmettre aux sociétés de distribution et aux gestionnaires de réseaux de distribution, des données supplémentaires ni quant au statut social de la personne concernée, ni sur la composition de ménage » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/001, pp. 5-6).

En ce qui concerne la transition vers le nouveau système, il est encore mentionné ce qui suit :

« Le système ' pull ' introduit en 2012 était un pas dans la bonne direction. Il est nécessaire à présent de passer au système ' push ', plus efficace, tout d'abord dans le cadre d'une phase de test devant permettre d'améliorer la méthode » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/005, p. 54).

Dans les travaux préparatoires, la plus-value du système « push » fait ensuite l'objet du commentaire suivant :

« La plus-value de ce changement de politique se trouve dans le fait que le push d'une consommation extrêmement basse ou extrêmement haute, dépendant de la composition de ménage, permet d'activer un déclencheur d'alerte dans les cas où il n'y a pas encore une présomption de fraude. C'est là aussi que se trouve la plus-value du datamining: rendre les contrôles plus efficaces et plus focalisés. Dans le système ' pull ' cette plus-value est très limitée puisqu'on demande des données supplémentaires sur base d'un dossier concret avec présomption de fraude » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/001, p. 6).

B.2.3.1. En ce qui concerne les objectifs poursuivis par le législateur, les travaux préparatoires mentionnent ce qui suit :

« Conformément à la notification budgétaire approuvée par le Conseil des ministres du 3 avril 2015 (pages 39-40), le présent projet de loi a pour objectif de rendre possible la transmission systématique des données de consommation des sociétés de distribution vers la Banque Carrefour de la Sécurité Sociale. Cela devra renforcer le contrôle sur l'attribution correcte des prestations sociales.

On prend de plus en plus conscience de l'hypothèque que la fraude aux allocations fait peser sur notre sécurité sociale. Or, pour rester viable, celle-ci a besoin d'une large assise sociale fondée sur la solidarité.

La fraude aux allocations touche notre système de sécurité sociale en plein cœur. Elle mine en effet un de ses fondements, à savoir la solidarité. Ce principe constitue un des fondements de notre système.

De nombreux citoyens paient honnêtement leurs cotisations et perçoivent leurs allocations en toute régularité. Seul un groupe déterminé ne respecte pas les règles et lèse ainsi les autres citoyens qui, eux, contribuent correctement au régime de sécurité sociale et qui en bénéficient lorsqu'ils y ont droit.

Dans différentes branches de la sécurité sociale, comme le chômage et l'assurance maladie-invalidité, certaines prestations sont en effet octroyées avec majoration en fonction de la situation familiale de l'assuré social.

Les domiciliations fictives constituent un mécanisme de fraude qui en découle, vu que l'assuré social ne déclare pas, sciemment, son véritable domicile et/ou sa situation familiale afin d'obtenir de façon illicite une allocation plus élevée que celle à laquelle il a droit.

Compte tenu de son impact, la fraude sociale liée à la domiciliation fictive est un phénomène auquel les services d'inspection sont particulièrement attentifs.

Dans le cadre d'un renforcement de la lutte contre la fraude sociale, des mesures externes (renforcement de la collaboration avec les magistrats, la police et les autres institutions publiques de sécurité sociale) ainsi que des mesures internes (établissement de nouvelles procédures administratives) ont été élaborées et mises en application.

Il a également été décidé de prévoir une stratégie globale de lutte contre les domiciliations fictives, impliquant toutes les institutions de sécurité sociale et les organismes octroyant des avantages sociaux, en définissant des lignes directrices pour la recherche et la poursuite tout en respectant la vie privée.

Le Collège des Procureurs généraux a édicté une circulaire sur le phénomène de la fraude sociale par le biais d'inscriptions fictives. Cette circulaire du Collège des Procureurs généraux (COLL. PG 17/2013) et son vademecum sont entrés en vigueur le 2 septembre 2013 » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/001, pp. 4-5).

B.2.3.2. Il en ressort que le législateur, fort de l'idée que la fraude aux allocations mine la solidarité comme fondement de la sécurité sociale, a considéré la lutte contre la fraude sociale comme une préoccupation sociétale importante. Il a déjà pris plusieurs mesures dans le but de renforcer la lutte contre la fraude sociale. Par la réglementation attaquée, il se concentre en particulier sur la fraude sociale au domicile, eu égard au lien étroit entre le montant des prestations sociales, la situation de domicile et la situation familiale.

B.3.1. Le législateur vise donc à renforcer la lutte contre la fraude sociale au domicile en recourant à des techniques de traitement modernes sans que les données de consommation sélectionnées et transmises, qu'on appelle « signaux d'alerte », soient déterminantes pour établir si un bénéficiaire de prestations sociales a utilisé une adresse fictive.

La loi attaquée tend donc à fournir aux services publics, en l'espèce les inspecteurs sociaux et les institutions publiques de sécurité sociale (ci-après : les IPSS), des instruments plus efficaces et performants pour exécuter leurs tâches légales en matière de sécurité sociale. Les inspecteurs sociaux sont les fonctionnaires qui sont sous l'autorité des ministres ayant dans leurs attributions l'emploi et le travail, la sécurité sociale, les affaires sociales et la santé publique, ou qui relèvent des institutions publiques qui en dépendent, et qui sont chargés de veiller au respect des lois sociales (article 16, 1°, du Code pénal social). Les IPSS sont les services publics fédéraux chargés d'appliquer la législation relative à la sécurité sociale.

B.3.2. Le législateur a notamment considéré, entre autres en raison des possibilités qu'offrent les techniques de « profilage », qui s'appuient sur le « data warehousing », le « data matching » et le « data mining », que, d'une part, la mise automatique et systématique à disposition des services publics mentionnés en B.3.1 des adresses et données de consommation d'eau, de gaz et d'électricité sélectionnées et, d'autre part, l'analyse des données agrégées disponibles et la recherche, par ces services, d'indicateurs de risques dans ces données, sont des instruments utiles dans la lutte contre la fraude sociale au domicile.

B.3.3. Le « profilage » se déroule en trois étapes distinctes, au cours desquelles on recherche ou on se base sur des patrons et modèles (les « profils ») : une première étape de collecte et de conservation à grande échelle (« data warehousing ») d'informations au sujet des comportements et caractéristiques des individus; une deuxième et une troisième étape d'analyse et d'exploitation de ces données permettant de faire des corrélations entre certains comportements et certaines caractéristiques, et au cours desquelles sont déduites de ces données, à partir des corrélations précitées, de nouvelles caractéristiques ou variables comportementales inconnues ou cachées (existantes, futures ou antérieures « data mining »).

B.3.4. Cette technique de « profilage » tend donc à détecter, à partir d'un profil, un ensemble de particularités qui caractérisent une catégorie de personnes (p. ex. les fraudeurs), à identifier un individu afin, d'une part, de prendre des décisions à son égard (p. ex. lancer une enquête), et, d'autre part, d'analyser ou de prévoir ses préférences, comportements et attitudes personnels (point 1, d. et e., de la recommandation (2010)13 du Comité des ministres aux Etats membres du 23 novembre 2010 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage (ci-après : la recommandation (2010)13).

B.3.5. Lorsqu'on recourt à cette technique, il est toutefois primordial d'utiliser les bons critères de sélection (ensemble de caractéristiques) pour renforcer la lutte contre la fraude sociale (les « signaux d'alerte » ou « indicateurs de risque »). Cette technique présente en effet des inconvénients sérieux, *a fortiori* lors de la phase initiale de sa mise en œuvre, et notamment d'arriver à des résultats faussement positifs ou faussement négatifs, ce qui nécessite de faire une évaluation et un suivi permanents des critères (voy. Commission de la protection de la vie privée, avis 24/2015, p. 7; avis 05/2016, p. 6).

B.4. Il ressort des travaux préparatoires de la loi attaquée que le législateur a concrétisé son objectif en conférant un fondement légal au contrôle renforcé de la fraude sociale au domicile par un échange de données automatisé entre les prestataires de services et les services publics et aux techniques modernes de recherche dans de vastes banques de données (« data warehousing »), comme le « data matching » et le « data mining », sans porter atteinte aux exigences fixées en matière de protection de la vie privée (voy. article 104 de la loi-programme (I) du 29 mars 2012) :

« Pour cette raison, le projet prévoit une base légale permettant de transmettre électroniquement à la Banque-Carrefour de la Sécurité Sociale (BCSS) certaines données de consommation d'eau, de gaz et d'électricité et les adresses de certains particuliers » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/001, p. 5).

« La Commission [de la protection de la vie privée] a recommandé une base légale générale similaire pour le recours au ' datamining ' et au ' datamatching ' au moyen des banques de données pertinentes, tel qu'utilisées, entre autres, par la plateforme OASIS. Bien que la Commission indique clairement que cette recommandation dépasse le cadre du dossier actuel, l'ajout de ce paragraphe permet déjà de satisfaire à cette recommandation de la Commission pour ce qui concerne les données énergétiques et une base légale est établie à cet effet pour le datamining » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/004, p. 9).

« Cette méthode permettra, comme c'est déjà le cas aux Pays-Bas, de vérifier, de manière automatique et en respectant la vie privée, si les données de consommation déclarées correspondent ou non aux données de domiciliation. Ce croisement de données pourra déclencher une alerte qui nécessitera une enquête plus approfondie. Les données énergétiques sont déjà effectivement utilisées aujourd'hui dans la lutte contre les logements inoccupés, à Bruxelles, par exemple.

Afin de mettre tout ceci en œuvre, la législation existante, reprise aux articles 100 à 105 inclus de la loi-programme du 29 mars 2012, est modifiée. Cette loi contient déjà une disposition qui rend applicable la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Cette disposition est évidemment maintenue dans le nouveau système » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/001, p. 6).

B.5.1. Les mesures devant permettre au législateur de réaliser son objectif sont contenues dans les articles 2 et 3 de la loi attaquée.

B.5.2. L'article 2 de la loi attaquée prévoit un système « push » - sur plusieurs étapes au but très spécifique - qui permet de transmettre électroniquement certaines données de consommation d'eau, de gaz et d'électricité et les adresses de certains particuliers à la BCSS, qui se charge de les filtrer et de les croiser (« data matching ») avec d'autres données en vue de les communiquer aux IPSS et aux inspecteurs sociaux intéressés, dans le but de renforcer la performance et l'efficacité de la lutte contre la fraude aux allocations (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/001, p. 5).

Lors d'une première étape, les sociétés de distribution et les gestionnaires de réseaux de distribution sont tenus de collecter des données de consommation et des adresses. Ils doivent ensuite transmettre certaines de ces données à la BCSS, au minimum une fois par an. Ces données sont sélectionnées lorsqu'un écart d'au moins 80 % par rapport à la consommation moyenne correspondant à la composition de ménage officiellement communiquée est constaté (article 101, § 1er, alinéa 1er, de la loi-programme (I) du 29 mars 2012, tel qu'il a été remplacé par l'article 2 de la loi attaquée). Les types de familles et la consommation moyenne par type de famille sont annuellement fixés par le comité de gestion de la BCSS, en concertation avec les sociétés de distribution et les gestionnaires de réseaux de distribution (article 101, § 1er, alinéa 2, de la loi-programme (I) du 29 mars 2012, tel qu'il a été remplacé par l'article 2 de la loi attaquée).

Lors d'une deuxième étape, les données ainsi collectées et obtenues par la BCSS sont transmises, après avoir été croisées avec les données enregistrées au Registre national, pour déceler qui habite aux différentes adresses communiquées aux IPSS et aux inspecteurs sociaux, à condition que les institutions visées octroient une prestation sociale ou exercent une quelconque forme de contrôle du respect des lois octroyant un avantage (« data matching »; article 101, § 1er, alinéa 3, de la loi-programme (I) du 29 mars 2012, tel qu'il a été remplacé par l'article 2 de la loi attaquée).

Ensuite, les inspecteurs sociaux ou les IPSS peuvent contrôler, après autorisation du comité sectoriel de la sécurité sociale et de la santé, sur la base des données obtenues, en combinaison avec d'autres données (à caractère personnel) issues des banques de données sociales, de la BCSS et du Registre national, si une prestation sociale est allouée sur la base d'une adresse fictive (« data mining »; article 101, § 1er, alinéa 3, de la loi-programme (I) du 29 mars 2012, tel qu'il a été remplacé par l'article 2 de la loi attaquée).

Toutefois, les données de consommation et les adresses communiquées ne peuvent en soi amener à conclure que le bénéficiaire d'une prestation sociale s'est rendu coupable de fraude sociale au domicile (article 102 de la loi-programme (I) du 29 mars 2012, tel qu'il a été remplacé par l'article 4 de la loi attaquée).

B.5.3. L'article 3 autorise par ailleurs les IPSS à rechercher des corrélations et des indicateurs de risque en matière de fraude sociale au domicile dans les données, agrégées, issues de banques de données sociales pertinentes (« data mining »).

Au cours de cette troisième étape, les IPSS, dont relèvent aussi les inspecteurs sociaux, peuvent procéder au regroupement des données de consommation et des adresses recueillies avec d'autres données dont elles disposent, pour analyser des données relationnelles qui doivent permettre aux services concernés de réaliser des contrôles ciblés, sur la base d'indicateurs de risque d'octroi d'une aide calculée sur la base d'une adresse fictive (article 101/1 de la loi-programme (I) du 29 mars 2012, tel qu'il a été inséré par l'article 3 de la loi attaquée). Cette analyse se fait à partir de données codées qui ne peuvent être décodées qu'après avoir été isolées, lorsqu'une analyse indique le risque d'une utilisation d'une adresse fictive.

B.6. Le législateur a en outre choisi de confier la fixation des règles d'exécution relatives au système instauré au comité de gestion de la BCSS. Dans les travaux préparatoires, cette délégation est commentée en ces termes :

« Néanmoins, il est également prévu que non pas le Roi, mais le comité de gestion de la Banque-Carrefour de la sécurité sociale devra fixer la consommation moyenne par type de famille. Le comité de gestion devra le faire en concertation avec les acteurs du terrain, à savoir les sociétés de distribution et les gestionnaires de réseaux de distribution. Selon le gouvernement cette approche permet de fixer le seuil le plus adéquat et, si nécessaire, de l'adapter rapidement aux circonstances changeantes sur le terrain afin de lutter efficacement contre la fraude au domicile. En effet, la fraude au domicile est une donnée évolutive et en outre le gouvernement ne veut en aucun cas toucher aux ayants droit de bonne foi. Cette préoccupation est rencontrée par la possibilité d'une délégation prévu [e] au comité de gestion » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/001, pp. 7-8).

Quant aux dispositions attaquées

B.7.1.1. L'article 2 de la loi attaquée remplace l'article 101 de la loi-programme (I) du 29 mars 2012 par ce qui suit :

« § 1er. En fonction de la périodicité de leur collecte de données et au minimum une fois par année calendrier, les sociétés de distribution et les gestionnaires de réseaux de distribution transmettent électroniquement à la Banque Carrefour de la Sécurité Sociale certaines données de consommation et les adresses de certains de leurs clients privés. Il s'agit des données sélectionnées par les sociétés de distribution et les gestionnaires de réseaux de distribution parce que la consommation du client privé s'écarte d'au moins 80 % vers le haut ou vers le bas d'une consommation moyenne en fonction de la composition de ménage officiellement communiquée.

Les types de famille et la consommation moyenne par type de famille sont annuellement fixés par le comité de gestion de la Banque Carrefour de la Sécurité Sociale en concertation avec les sociétés de distribution et les gestionnaires de réseaux de distribution.

La Banque Carrefour de la Sécurité Sociale transmet les données visées à l'alinéa 1er, après croisement avec les données enregistrées au Registre national, visé par la loi du 8 août 1983 organisant un registre national des personnes physiques, aux institutions publiques de sécurité sociale et aux inspecteurs sociaux à condition que les institutions visées octroient au bénéficiaire auquel ces données ont trait une prestation sociale, soit de la sécurité sociale, soit d'un régime d'aide sociale, ou d'autres avantages accordés par les réglementations sur lesquelles les inspecteurs sociaux exercent la surveillance. Cela doit leur permettre de contrôler, après autorisation du comité sectoriel de la sécurité sociale et de la santé, en combinaison avec d'autres données sociales et des données sociales à caractère personnel qui sont disponibles dans le réseau, telles que visées à la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la Sécurité Sociale, si la prestation sociale est octroyée sur la base d'une adresse fictive.

§ 2. Pour les traitements de données visés au § 1er, il est désigné comme responsable de traitement tel que visé à l'article 1er, § 4, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, la Banque Carrefour de la Sécurité Sociale ».

B.7.1.2. En ce qui concerne le premier paragraphe de la disposition nouvelle, les travaux préparatoires mentionnent :

« Cet article oblige les sociétés de distribution et les gestionnaires de réseaux de distribution à transmettre électroniquement à la Banque Carrefour de la Sécurité Sociale, en fonction de la périodicité de leur collecte des données et au minimum une fois par année calendrier, certaines données de consommation et les adresses de certains de leurs clients privés. Ceci signifie donc que les données font désormais l'objet d'un système ' push '. Cela doit se faire donc au moins une fois par année, mais si cela est possible pour certaines sociétés de distribution et gestionnaires de réseaux de distribution, les données pourront également être transmises plusieurs fois par année. Il s'agit des données sélectionnées par les sociétés de distribution et les gestionnaires de réseaux parce qu'elles s'écartent d'au moins 80 % vers le haut ou vers le bas d'une consommation moyenne en fonction de la composition de ménage officiellement communiquée. Les types de famille et la consommation moyenne par type de famille sont annuellement fixés par le comité de gestion de la Banque-Carrefour de la sécurité sociale en concertation avec les sociétés de distribution et les gestionnaires de réseaux de distribution.

Dans l'avant-projet de loi il a été prévu que la communication des données de consommation se ferait sur base de certains seuils de consommation, qui peuvent indiquer une consommation inférieure ou supérieure en fonction de la composition de ménage officiellement communiquée. Ces seuils seraient fixés par le Roi par un arrêté royal délibéré en Conseil des ministres. Cependant, le Conseil d'État a remarqué dans le point 8.2. de son avis que cette délégation au Roi est trop large. Vu cette remarque le gouvernement a jugé souhaitable d'en effet prévoir déjà une limitation dans la loi même. Pour cette raison la règle de 80 % est inscrite dans la loi même. Néanmoins, il est également prévu que non pas le Roi, mais le comité de gestion de la Banque-Carrefour de la sécurité sociale devra fixer la consommation moyenne par type de famille. Le comité de gestion devra le faire en concertation avec les acteurs du terrain, à savoir les sociétés de distribution et les gestionnaires de réseaux de distribution. Selon le gouvernement cette approche permet de fixer le seuil le plus adéquat et, si nécessaire, de l'adapter rapidement aux circonstances changeantes sur le terrain afin de lutter efficacement contre la fraude au domicile. En effet, la fraude au domicile est une donnée évolutive et en outre le gouvernement ne veut en aucun cas toucher aux ayants droit de bonne foi. Cette préoccupation est rencontrée par la possibilité d'une délégation prévu [e] au comité de gestion.

En outre, d'après la CPVP, il convient de mieux justifier le passage d'un modèle ' pull ' à un modèle ' push '. Etant donné que différentes institutions publiques de sécurité sociale (IPSS) octroient des prestations qui varient en fonction de la composition du ménage, il est important pour elles de pouvoir contrôler le mieux possible si la composition du ménage déclarée est bien correcte. Pour l'instant, les services d'inspection vérifient cela au moyen, entre autres, de contrôles sur place au domicile déclaré ou en demandant les données de consommation auprès de l'assuré social même ou des sociétés de distribution ou des gestionnaires de réseau de distribution. Le modèle push proposé est destiné à renforcer ces instruments existants et à rendre le contrôle plus efficace et plus performant. Lors des discussions au Conseil National du Travail, l'Office national de l'Emploi a par exemple indiqué que ce système permettra en effet à leurs inspecteurs sociaux d'exercer un contrôle plus ciblé et plus efficace du respect des règles de la réglementation du chômage.

D'autre part, la CPVP se pose également la question de savoir pourquoi on vise à la fois une consommation trop faible et une consommation trop élevée. Compte tenu de ce qui précède, il est logique que les deux extrêmes soient pris en considération, car il est possible que chacun des partenaires d'un couple bénéficie [...] d'une allocation. Afin d'augmenter l'allocation de chacun d'entre eux, ils déclarent chacun d'être isolé. Pour le prouver, ils ont une

résidence séparée. Cela signifie qu'ils bénéficient tous les deux d'une allocation en qualité d'isolé. Celle-ci est évidemment plus élevée qu'une allocation en qualité de cohabitant. Cependant, dans les faits, ils vivent encore ensemble. Dans un des deux domiciles la consommation sera en principe plus faible que la consommation moyenne d'un isolé. Dans l'autre domicile, elle sera en principe plus élevée. Grâce à cette mesure, ces deux types de fraudes peuvent être détectés.

En outre, la finalité de cette obligation est précisée. Ces données doivent permettre aux inspecteurs sociaux de contrôler si les prestations de sécurité sociale ou d'assistance sociale payées ont été octroyées à juste titre.

A cette fin, ces données doivent être combinées avec d'autres données dont les services compétents disposent ou auxquelles ils ont accès.

Afin d'avoir accès à ces données de consommation et afin de pouvoir les combiner avec les autres données, les services intéressés doivent, comme toujours, demander une autorisation du Comité sectoriel de la Sécurité sociale et de la Santé.

Suite à la remarque 9.4 du Conseil d'Etat le texte a été adapté afin de mettre en évidence que les données de consommation divergentes sont uniquement communiquées par la BCSS au cas où les personnes concernées touchent des allocations des institutions concernées.

Cette adaptation permet de répondre d'emblée à la remarque de la CPVP selon laquelle les sociétés privées (sociétés de distribution ou gestionnaires de réseau de distribution) ne peuvent pas recevoir des informations complémentaires sur l'assuré social, venant de l'inspection sociale ou du registre national. Il s'agit très clairement d'une circulation de données à sens unique. Les sociétés privées doivent fournir des informations. Elles n'en reçoivent pas » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/001, pp. 7-9).

En ce qui concerne le second paragraphe, les travaux préparatoires mentionnent :

« Dans ses avis des 17 juin 2015 et 3 février 2016, la Commission vie privée souligne que le responsable de traitement n'est pas désigné explicitement dans le projet. Etant donné que de nombreux acteurs seront associés à la lutte contre la fraude sociale visée par le projet de loi (gestionnaires de réseau de distribution, BCSS, inspection sociale, sous-traitants éventuels...), la question se posera tôt ou tard de savoir qui est le responsable ou le sous-traitant du ou des différents traitements visés par le Projet. Etant donné que pour tous ces traitements, les droits et obligations actuels et futurs doivent être respectés par tout responsable aux termes de la LVP et du RGPD, il est important d'apporter des précisions à cet égard. La Commission vie privée indique dans son avis que cette désignation peut également avoir lieu d'une manière précise dans les autorisations d'échange de données. Afin d'accroître la transparence, le responsable de traitement sera également désigné clairement dans la loi. En ce qui concerne le ' datamatching ', la ' Banque-Carrefour de la Sécurité Sociale ' est désignée comme responsable de traitement » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/004, p. 7).

B.7.2.1. L'article 3 de la loi attaquée insère, dans la loi-programme (I) du 29 mars 2012, un article 101/1 (nouveau), qui dispose :

« § 1er. Chaque institution publique de sécurité sociale (IPSS) peut procéder à l'agrégation des données recueillies en application de l'article 101 avec d'autres données dont les IPSS disposent, pour effectuer des analyses sur des données relationnelles qui doivent permettre à ses services de réaliser des contrôles ciblés sur la base d'indicateurs de risque d'octroi d'une aide calculée sur la base d'une adresse fictive. L'analyse se fait à partir de données codées. Les données indiquant un risque d'utilisation d'une adresse fictive sont isolées et décodées.

§ 2. Toute catégorie de données communiquée dans le cadre de l'article 101, § 1er, à un IPSS fait l'objet d'une autorisation d'un comité sectoriel institué au sein de la Commission de la protection de la vie privée. L'autorisation fixe les conditions relatives au délai de conservation des données codées et décodées.

§ 3. Les analyses sur les données relationnelles visées à l'article 101, § 1er, ont pour responsable de traitement, tel que visé à l'article 1er, § 4, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, l'IPSS qui procède à l'analyse sur les données relationnelles ».

B.7.2.2. En ce qui concerne le premier paragraphe de cette disposition, les travaux préparatoires mentionnent :

« Dans son avis du 3 février 2016, la Commission vie privée fait référence à l'article 5, § 1er, de la loi du 3 août 2012, portant dispositions relatives aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances dans le cadre de ses missions, qui dispose que :

' § 1er. Le Service public fédéral Finances peut procéder également à l'agrégation des données recueillies en application de l'article 3 en vue de la création d'un datawarehouse qui doit permettre à ses services d'une part, de réaliser des contrôles ciblés sur la base d'indicateurs de risque et d'autre part, d'effectuer des analyses sur des données relationnelles provenant des différentes administrations et, ou services du Service public fédéral Finances. ' La Commission a recommandé une base légale générale similaire pour le recours au ' datamining ' et au ' datamatching ' au moyen des banques de données pertinentes, tel qu'utilisées, entre autres, par la plateforme OASIS. Bien que la Commission indique clairement que cette recommandation dépasse le cadre du dossier actuel, l'ajout de ce paragraphe permet déjà de satisfaire à cette recommandation de la Commission pour ce qui concerne les données énergétiques et une base légale est établie à cet effet pour le datamining » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/004, p. 9).

En ce qui concerne le deuxième paragraphe, il est dit :

« Dans ses avis des 17 juin 2015 et 3 février 2016, la Commission vie privée pose la question d'une durée de conservation des données adaptée, compte tenu de l'article 4, § 1er, 4°, de la loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (LVP). La Commission indique que la définition d'une durée de conservation peut avoir lieu d'une manière précise dans les autorisations d'échange de données. Au paragraphe 2, il est défini que ces autorisations doivent préciser des durées de conservation pour des données codées et décodées » (*ibid.*).

Le troisième paragraphe est commenté en ces termes :

« En ce qui concerne le ' datamining ' ' l'IPSS qui procède à l'analyse sur les données relationnelles ' est désignée comme responsable de traitement » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/004, p. 10).

B.7.3.1. L'article 4 de la loi attaquée remplace l'article 102 de la loi-programme (I) du 29 mars 2012 par ce qui suit :

« Les données visées à l'article 101 peuvent uniquement être utilisées comme indication supplémentaire afin de décider si un bénéficiaire utilise une adresse fictive ».

B.7.3.2. Les travaux préparatoires de cette disposition mentionnent :

« Cet article dispose que les données peuvent uniquement être utilisées comme indication supplémentaire afin de constater si un bénéficiaire utilise une adresse fictive.

En effet, il ne s'agit pas de conclure qu'il y a fraude en se basant uniquement sur les données de consommation. Ces données elles-mêmes ne sont pas suffisamment probantes à cet effet » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/001, p. 9).

B.7.4. Dans l'article 103 de la loi-programme (I) du 29 mars 2012, l'article 5 de la loi attaquée remplace le mot « demander » par le mot « utiliser ».

B.7.5.1. L'article 6 de la loi attaquée remplace l'article 105 de la loi-programme (I) du 29 mars 2012 par ce qui suit :

« Le comité de gestion de la Banque Carrefour de la Sécurité Sociale détermine les modalités, entre autres la structure et le contenu des messages avec lesquels les données sont transmises, la façon selon laquelle et le moment auquel les données de consommation et d'adresses sont transmises ».

B.7.5.2. Les travaux préparatoires de cette disposition mentionnent :

« Cet article prévoit une délégation au Comité de gestion de la Banque Carrefour de la Sécurité Sociale.

Le comité de gestion devra déterminer les modalités pratiques d'application de la mesure. Il s'agit, entre autres, de la structure et du contenu des messages, de la façon dont et le moment auquel les données de consommation et les adresses doivent être transmises. Une telle délégation au comité de gestion n'est pas neuve et est justifiée par le fait qu'il s'agit souvent d'aspects techniques pour lesquels une réaction rapide est nécessaire, compte tenu d'un environnement informatique qui évolue rapidement » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/001, pp. 9-10).

Quant à la recevabilité du recours

B.8.1. Les griefs soulevés par la partie requérante étant exclusivement dirigés contre les articles 2, 3 et 4 de la loi attaquée, le recours est seulement recevable en ce qu'il est dirigé contre ces articles.

B.8.2.1. Le Conseil des ministres conteste la recevabilité de la plupart des griefs formulés dans le moyen unique au motif qu'ils ne seraient pas suffisamment développés ou qu'ils seraient dénués de pertinence. En outre, il souligne à plusieurs reprises qu'un des griefs formulés serait totalement ou partiellement irrecevable parce que la Cour n'est pas compétente pour exercer un contrôle direct au regard de dispositions conventionnelles, de dispositions législatives (la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel; ci-après : la « loi relative à la protection de la vie privée »), d'actes législatifs de l'Union européenne (la 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 (ci-après : la « directive 95/46/CE ») et le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)) et des principes généraux de nécessité, de subsidiarité, de proportionnalité, de transparence, de limitation de conservation, d'obligation de justification, d'intégrité et de sécurité.

B.8.2.2. La Cour est compétente pour contrôler des normes de nature législative au regard des règles répartitrices de compétence entre l'Etat fédéral, les communautés et les régions, ainsi qu'au regard des articles du titre II (« Des Belges et de leurs droits ») et des articles 143, § 1er, 170, 172 et 191 de la Constitution.

Tous les griefs sont pris de la violation d'une ou de plusieurs règles dont la Cour garantit le respect.

Dans la mesure où la partie requérante invoque en outre des dispositions conventionnelles, des actes législatifs de l'Union européenne, des dispositions législatives et des principes généraux, la Cour ne les examine qu'en tant que la partie requérante dénonce la violation des dispositions constitutionnelles précitées, combinées avec les dispositions, actes et principes visés. Dans cette mesure, les griefs sont recevables.

B.8.3. Pour satisfaire aux exigences de l'article 6 de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, les moyens de la requête doivent faire connaître, parmi les règles dont la Cour garantit le respect, non seulement celles qui seraient violées, mais aussi les dispositions qui violeraient ces règles, et exposer en quoi ces règles auraient été transgressées par les dispositions visées.

La Cour examine les griefs formulés dans le moyen unique, dans la mesure où ils satisfont aux exigences précitées.

B.8.4. Les exceptions sont rejetées.

Quant au droit au respect de la vie privée

B.9. Le moyen unique est principalement pris, mais pas exclusivement, de la violation du droit au respect de la vie privée, tel qu'il est garanti par l'article 22 de la Constitution, combiné avec l'article 8 de la Convention européenne des droits de l'homme, avec l'article 17 du Pacte international relatif aux droits civils et politiques et avec les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.

B.10.1. L'article 22 de la Constitution dispose :

« Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi.

La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit ».

B.10.2. L'article 8 de la Convention européenne des droits de l'homme dispose :

« 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 ».

B.10.3. Le Constituant a recherché la plus grande concordance possible entre l'article 22 de la Constitution et l'article 8 de la Convention européenne précitée (*Doc. parl.*, Chambre, 1992-1993, nº 997/5, p. 2).

La portée de cet article 8 est analogue à celle de la disposition constitutionnelle précitée, de sorte que les garanties que fournissent ces deux dispositions forment un ensemble indissociable.

B.10.4. L'article 17 du Pacte international relatif aux droits civils et politiques dispose :

« 1. Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.

2. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ».

B.10.5. Les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne disposent :

« Art. 7. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications ».

« Art. 8. 1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».

Dans le contrôle qu'elle exerce au regard des articles 7 et 8 précités, la Cour doit prendre en compte l'article 52, paragraphe 1, de la Charte, qui dispose :

« Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui ».

B.11. Le droit au respect de la vie privée, tel qu'il est garanti par les dispositions constitutionnelles et conventionnelles précitées, a pour but essentiel de protéger les personnes contre les ingérences dans leur vie privée.

Ce droit a une portée étendue et englobe notamment la protection des données à caractère personnel et des informations personnelles. La jurisprudence de la Cour européenne des droits de l'homme fait apparaître que de la protection de ce droit relèvent notamment les données et informations personnelles suivantes : le nom, l'adresse, les activités professionnelles, les relations personnelles, les empreintes digitales, les images filmées, les photographies, les communications, les données ADN, les données judiciaires (condamnations ou inculpations), les données financières et les informations concernant des biens (voy. notamment CEDH, 23 mars 1987, *Leander* c. Suède, § § 47-48; grande chambre, 4 décembre 2008, *S. et Marper* c. Royaume-Uni, § § 66-68; 17 décembre 2009, *B.B.* c. France, § 57; 10 février 2011, *Dimitrov-Kazakov* c. Bulgarie, § § 29-31; 18 octobre 2011, *Khelili* c. Suisse, § § 55-57; 9 octobre 2012, *Alkaya* c. Turquie, § 29; 18 avril 2013, *M.K.* c. France, § 26; 18 septembre 2014, *Brunet* c. France, § 31).

B.12. Les droits que garantissent l'article 22 de la Constitution et l'article 8 de la Convention européenne des droits de l'homme ne sont toutefois pas absolus.

Ils n'excluent pas toute ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée mais exigent que cette ingérence soit prévue par une disposition législative suffisamment précise, qu'elle réponde à un besoin social impérieux dans une société démocratique et qu'elle soit proportionnée à l'objectif légitime qu'elle poursuit. Ces dispositions engendrent de surcroît l'obligation positive, pour l'autorité publique, de prendre des mesures qui assurent le respect effectif de la vie privée, même dans la sphère des relations entre les individus (CEDH, 27 octobre 1994, *Kroon et autres* c. Pays-Bas, § 31; grande chambre, 12 octobre 2013, *Söderman* c. Suède, § 78).

B.13.1. En réservant au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée, l'article 22 de la Constitution garantit à tout citoyen qu'aucune ingérence dans l'exercice de ce droit ne peut avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue.

Une délégation à un autre pouvoir n'est toutefois pas contraire au principe de légalité, pour autant que l'habilitation soit définie de manière suffisamment précise et porte sur l'exécution de mesures dont les éléments essentiels sont fixés préalablement par le législateur.

B.13.2. Outre l'exigence de légalité formelle, l'article 22 de la Constitution impose également que l'ingérence dans l'exercice du droit au respect de la vie privée soit définie en des termes clairs et suffisamment précis qui permettent d'appréhender de manière prévisible les hypothèses dans lesquelles le législateur autorise une pareille ingérence.

De même, l'exigence de prévisibilité à laquelle la loi doit satisfaire pour être jugée conforme à l'article 8 de la Convention européenne des droits de l'homme implique que sa formulation soit assez précise pour que chacun puisse - en s'entourant au besoin de conseils éclairés - prévoir, à un degré raisonnable, dans les circonstances de la cause, les conséquences d'un acte déterminé (CEDH, grande chambre, 4 mai 2000, *Rotaru* c. Roumanie, § 55; grande chambre, 17 février 2004, *Maestri* c. Italie, § 30). La législation doit donner à chacun une indication suffisante sur les circonstances dans lesquelles et à quelles conditions elle habilite la puissance publique à recourir à des mesures affectant les droits protégés par la Convention (CEDH, grande chambre, 12 juin 2014, *Fernández Martínez* c. Espagne, § 117).

Plus particulièrement, lorsque l'intervention de l'autorité présente un caractère secret, la loi doit offrir des garanties suffisantes contre les ingérences arbitraires dans l'exercice du droit au respect de la vie privée, en délimitant le pouvoir d'appréciation des autorités concernées avec une netteté suffisante, d'une part, et en prévoyant des procédures qui permettent un contrôle juridictionnel effectif, d'autre part (CEDH, grande chambre, 4 mai 2000, *Rotaru* c. Roumanie, § 55; 6 juin 2006, *Segerstedt-Wiberg* c. Suède, § 76; 4 juillet 2006, *Lupsa* c. Roumanie, § 34).

B.13.3. Il découle dès lors de l'article 8 de la Convention européenne des droits de l'homme et de l'article 22 de la Constitution qu'il doit être prévu de manière suffisamment précise dans quelles circonstances un traitement de données à caractère personnel est autorisé (CEDH, grande chambre, 4 mai 2000, *Rotaru* c. Roumanie, § 57; grande chambre, 12 janvier 2010, *S. et Marper* c. Royaume-Uni, § 99).

Le niveau requis de précision de la législation concernée - laquelle ne peut du reste parer à toute éventualité - dépend notamment, selon la Cour européenne des droits de l'homme, du domaine qu'elle est censée couvrir et du nombre et de la qualité de ses destinataires (CEDH, grande chambre, 12 janvier 2010, *S. et Marper* c. Royaume-Uni, §§ 95 et 96). Ainsi, la Cour européenne des droits de l'homme a jugé que l'exigence de prévisibilité dans des domaines liés à la sécurité nationale ne pouvait avoir la même portée que dans d'autres domaines (CEDH, 26 mars 1987, *Leander* c. Suède, § 51; 4 juillet 2006, *Lupsa* c. Roumanie, § 33).

B.14.1. Une ingérence des pouvoirs publics dans l'exercice du droit au respect de la vie privée doit non seulement reposer sur une disposition législative suffisamment précise mais aussi répondre à un besoin social impérieux dans une société démocratique et être proportionnée au but légitime poursuivi.

Le législateur dispose en la matière d'une marge d'appréciation. Cette marge n'est toutefois pas illimitée : pour qu'une norme soit compatible avec le droit au respect de la vie privée, il faut que le législateur ait établi un juste équilibre entre tous les droits et intérêts en cause.

B.14.2. Pour juger de cet équilibre, la Cour européenne des droits de l'homme tient compte notamment des dispositions de la Convention du Conseil de l'Europe du 28 janvier 1981 « pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel » (ci-après : la « Convention n° 108 »)(CEDH, 25 février 1997, *Z* c. Finlande, § 95; grande chambre, 12 janvier 2010, *S. et Marper* c. Royaume-Uni, § 103).

Cette Convention contient, entre autres, les principes relatifs au traitement de données à caractère personnel : licéité, loyauté, transparence, limitation des finalités, proportionnalité, exactitude, limitation de la conservation, intégrité et confidentialité, et responsabilité.

Pour interpréter ces principes, il y a lieu, en l'espèce, de tenir compte en particulier du contenu de la recommandation (2010)13.

B.14.3. Une ingérence dans l'exercice du droit au respect de la vie privée par un traitement de données à caractère personnel, en l'occurrence par un accès et par l'utilisation par les services publics de certaines données personnelles au moyen de techniques particulières (CEDH, 23 mars 1987, *Leander* c. Suède, § 48; grande chambre, 4 mai 2000, *Rotaru* c. Roumanie, § 46; CJUE, grande chambre, 8 avril 2014, C-293/12, *Digital Rights Ireland Ltd*, et C-594/12, *Kärntner Landesregierung e.a.*) doit donc reposer sur une justification raisonnable et être proportionnée aux buts poursuivis par le législateur.

B.14.4. En ce qui concerne la proportionnalité, la Cour européenne des droits de l'homme et la Cour de justice de l'Union européenne tiennent compte de l'existence ou non, dans la réglementation visée, des garanties matérielles et procédurales mentionnées en B.13.2.

Pour juger du caractère proportionné de mesures relatives au traitement de données à caractère personnel, il convient dès lors de tenir compte notamment de leur caractère automatisé, des techniques utilisées, de la précision, de la pertinence et du caractère excessif ou non des données traitées, de l'existence ou de l'absence de mesures qui limitent la durée de conservation des données, de l'existence ou de l'absence d'un système de contrôle indépendant permettant de vérifier si la conservation des données est encore requise, de la présence ou de l'absence de droits de contrôle et de voies de recours suffisants pour les personnes concernées, de la présence ou de l'absence de garanties visant à éviter la stigmatisation des personnes dont les données sont traitées, du caractère distinctif de la réglementation et de la présence ou de l'absence de garanties visant à éviter l'usage inapproprié et abusif, par les services publics, des données à caractère personnel traitées (CEDH, grande chambre, 4 mai 2000, *Rotaru* c. Roumanie, § 59; décision, 29 juin 2006, *Weber et Saravia* c. Allemagne, § 135; 28 avril 2009, *K.H. e.a.* c. Slovaquie, § § 60-69; grande chambre, 12 janvier 2010, *S. et Marper* c. Royaume-Uni, § § 101-103, 119, 122 et 124; 18 avril 2013, *M.K.* c. France, § § 37 et 42-44; 18 septembre 2014, *Brunet* c. France, § § 35-37; 12 janvier 2016, *Szabó et Vissy* c. Hongrie, § 68; CJUE, grande chambre, 8 avril 2014, C-293/12, *Digital Rights Ireland Ltd*, et C-594/12, *Kärntner Landesregierung e.a.*, points 56-66).

B.15.1. Les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne ont, en ce qui concerne le traitement des données à caractère personnel, une portée analogue à celle de l'article 8 de la Convention européenne des droits de l'homme (CJUE, grande chambre, C-92/09 et C-93/09, 9 novembre 2010, *Volker und Markus Schecke GbR et autres*) et de l'article 22 de la Constitution. Il en va de même de l'article 17 du Pacte international relatif aux droits civils et politiques.

B.15.2. La compatibilité de dispositions législatives avec les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, combinés avec des dispositions constitutionnelles analogues ou avec les articles 10 et 11 de la Constitution, ne peut être examinée par la Cour qu'en ce que les dispositions attaquées mettent en œuvre le droit de l'Union (CJUE, grande chambre, 26 février 2013, C-617/10, *Åklagaren*, points 17 et suivants).

En l'espèce, il convient de prendre en compte la directive 95/46/CE et le règlement général sur la protection des données.

B.15.3. Dès lors que les dispositions attaquées concernent le traitement de données à caractère personnel relevant de l'application de ces actes législatifs de l'Union européenne, les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne sont combinés avec les dispositions constitutionnelles analogues ou avec les articles 10 et 11 de la Constitution.

Quant au moyen unique

B.16. Les griefs formulés par la partie requérante concernent principalement la compatibilité, avec le droit au respect de la vie privée, de divers aspects du système « push » et du « data mining » envisagé.

En ce qui concerne la prévisibilité de la loi

B.17. La partie requérante demande l'annulation des articles 2, 3 et 4 de la loi attaquée parce que l'ingérence dans le droit au respect de la vie privée ne serait pas compatible avec les dispositions mentionnées en B.9, en ce qu'il n'existerait pas de fondement ou de fondement légal suffisamment précis pour justifier l'ingérence visée par le législateur et en ce que les articles 3 et 4 ne seraient pas suffisamment précis.

B.18. Toute personne doit savoir de manière suffisamment précise les circonstances et conditions dans lesquelles une ingérence dans sa vie privée est autorisée, en particulier en ce qui concerne le traitement automatisé de données à caractère personnel. Toute personne doit dès lors avoir une idée suffisamment claire des données traitées, des personnes concernées par ce traitement de données et des conditions et finalités dudit traitement.

Eu égard aux articles 5, *b)*, et 9, paragraphe 2, de la Convention n° 108 et au principe 3.4 de la Recommandation (2010)13, cette exigence s'applique d'autant plus lorsque les données à caractère personnel sont ensuite traitées par les services publics à d'autres fins que celles pour lesquelles elles ont initialement été obtenues.

B.19. Dans l'article 2, attaqué, le législateur a prévu que les sociétés de distribution et les gestionnaires de réseaux de distribution collectent et transmettent des données de consommation et des adresses obtenues à la Banque-carrefour de la sécurité sociale lorsque la consommation s'écarte du seuil de consommation moyenne correspondant à une composition de ménage déterminée, que ces données sont filtrées par la BCSS, croisées avec d'autres données, dans le but de vérifier si l'intéressé est connu comme bénéficiaire de prestations sociales, et enfin que ces données sont transmises aux IPSS et aux inspecteurs sociaux, afin que ces derniers puissent contrôler, sur la base des données obtenues, combinées avec les données disponibles dans le réseau, telles qu'elles sont visées dans la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale (ci-après : la « loi sur la BCSS »), après autorisation du comité sectoriel de la sécurité sociale et de la santé, si des prestations sociales ont été octroyées sur la base d'une adresse fictive. Dans l'article 4, attaqué, le législateur a clairement prévu que les données de consommation ne peuvent être considérées que comme un élément complémentaire et non comme un élément déterminant pour conclure à une fraude de la part d'un bénéficiaire de prestations sociales.

Dans l'article 3, attaqué, le législateur a ouvert la possibilité, pour les IPSS, de procéder au regroupement des données pour effectuer des analyses de ces données qui doivent permettre à ces services de réaliser des contrôles plus ciblés, sur la base d'indicateurs de risque de fraude sociale au domicile.

L'article 104 de la loi-programme (I) du 29 mars 2012 prévoit en outre que les dispositions de la loi relative à la protection de la vie privée restent d'application, de sorte que les conditions générales de traitement de données à caractère personnel, qui sont visées à l'article 4 de cette loi, s'appliquent également dans le cadre de l'ingérence attaquée en l'espèce.

B.20. Compte tenu, en particulier, des travaux préparatoires mentionnés en B.4, il découle de ce qui précède que l'ingérence a un fondement légal, de sorte que toute personne peut connaître de manière suffisamment précise les circonstances et les conditions relatives au traitement de ses données à caractère personnel. L'ingérence dans le droit à la protection de la vie privée satisfait donc aux conditions mentionnées en B.13.2.

B.21. Néanmoins, la référence à l'article 101, faite aux paragraphes 2 et 3 de cet article, est manifestement une erreur matérielle, eu égard à la formulation de l'article 3 attaqué, et en particulier à la référence à des données « codées » ou « décodées », et compte tenu des travaux préparatoires mentionnés en B.7.2.2 et de la volonté, qui en découle, de s'inspirer des règles de traitement des données à caractère personnel telles qu'elles sont appliquées par le SPF Finances.

A l'article 101/1, § § 2 et 3, de la loi-programme (I) du 29 mars 2012, inséré par l'article 3, attaqué, les mots « dans le cadre de l'article 101, § 1 » et « visées à l'article 101, § 1er, » doivent être annulés.

En ce qui concerne le principe de légalité

Le délai de conservation des données

B.22. La partie requérante fait valoir qu'en ce qui concerne l'ingérence prévue par les articles 2 et 3 attaqués, le législateur n'a pas fixé toutes les conditions auxquelles il peut être porté atteinte au droit au respect de la vie privée, en ce que le délai précis de conservation des données serait fixé par le comité sectoriel de la sécurité sociale et de la santé.

B.23. L'article 4, § 1er, 4° et 5°, de la loi relative à la protection de la vie privée prévoit que les données à caractère personnel ne peuvent être conservées pour une durée excédant la durée nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues et que ces données doivent être, le cas échéant, rectifiées ou effacées. Compte tenu du fait que le législateur ne peut prévoir des règles distinctes et précises pour tous les cas spécifiques, il pouvait régler de manière générale les conditions de conservation des données à caractère personnel, ainsi que la durée de cette conservation.

Il découle de ce qui précède que le législateur a réglé les éléments essentiels de la durée de conservation des données.

Le grief formulé en B.22 n'est pas fondé.

En ce qui concerne le principe de proportionnalité

Le système « push »

B.24. La partie requérante demande l'annulation de l'article 2 attaqué parce que le système « push » qu'il contient irait au-delà de ce qui est nécessaire pour lutter contre la fraude sociale au domicile et parce que les garanties relatives aux délais de conservation, à l'intervention du comité sectoriel de la sécurité sociale et de la santé, aux droits de contrôle des intéressés, à la procédure et à la sécurité seraient inexistantes ou insuffisantes.

B.25. Eu égard au fait que le système « push » prévoit une ingérence importante dans la vie privée du fait de l'ampleur et de la technique du traitement de données à caractère personnel, cette ingérence doit non seulement avoir un fondement légal, mais aussi satisfaire aux conditions mentionnées en B.14.

B.26. Comme il a déjà été dit en B.2, le législateur visait à lutter de manière plus performante et plus efficace contre la fraude sociale, qui est étroitement liée à l'utilisation d'un domicile fictif.

Le législateur poursuivait donc un objectif légitime en adoptant la mesure attaquée.

B.27. Le législateur doit également poursuivre cet objectif en prenant une mesure adéquate.

B.28. Le législateur a pu raisonnablement estimer que le système « push » était adéquat pour atteindre l'objectif poursuivi, en ce qu'il permet, sans qu'il y ait *a priori* une présomption de fraude à charge d'un bénéficiaire spécifique, d'utiliser des données de consommation fondées sur une consommation anormale comme un signal autonome d'une éventuelle fraude au domicile, ce qui permet de mieux détecter l'usage d'adresses potentiellement fictives et d'exercer aussi ensuite des contrôles ciblés, même avec des capacités en personnel réduites.

B.29. En ce qui concerne la nécessité de l'ingérence dans le droit au respect de la vie privée lors du traitement de données à caractère personnel, il convient de déterminer quelle est l'incidence de la réglementation attaquée sur cette vie privée, compte tenu des garanties existantes, et de vérifier si cette réglementation ne porte pas une atteinte disproportionnée aux garanties mentionnées en B.14.

B.30.1. Les autorités, services, organismes ou personnes qui sélectionnent, transmettent ou obtiennent ces données à caractère personnel par la méthode visée dans la loi attaquée sont tenus de respecter les dispositions applicables de la loi sur la protection de la vie privée.

B.30.2. En l'espèce, le législateur, par la loi relative à la protection de la vie privée, a choisi d'adopter un régime légal général, applicable à la fois au secteur public et au secteur privé (*Doc. parl.*, Chambre, 1990-1991, nr. 1610/1, p. 3), qui tienne néanmoins compte des particularités de certains secteurs et de la conciliation de toutes sortes d'intérêts. C'est pourquoi le législateur a expressément confirmé, dans l'article 104 de la loi-programme (I) du 29 mars 2012, l'application de la loi relative à la protection de la vie privée au système « push ».

B.30.3. La loi relative à la protection de la vie privée contient les règles qui sont essentielles à la protection du droit au respect de la vie privée : notamment des garanties individuelles (article 4) quant à l'enregistrement de données sensibles (articles 6 à 8); le droit d'accès et le droit de rectification (articles 10 et 12); la confidentialité et la sécurisation (article 16, § 4); la publicité des traitements et la large information des personnes concernées (articles 5 et 9); et le contrôle par un organe indépendant (article 31) et par les cours et tribunaux (article 14). Le responsable du traitement, désigné par le législateur, est donc soumis au respect de plusieurs obligations.

B.31. Néanmoins, l'importance, la nature et l'ampleur du traitement de données à caractère personnel instauré par le législateur requièrent des garanties spécifiques ou complémentaires.

Compte tenu du fait que le système attaqué consiste à signaler automatiquement - sans la moindre présomption préalable dans le chef des services publics à l'encontre de bénéficiaires individuels de prestations sociales - des soupçons de fraude au domicile, le législateur a choisi de soumettre les consommateurs de gaz, d'eau et d'électricité à un « profilage ». Cette technique a ceci de spécifique qu'elle se base sur le recours à certains paramètres pour repérer comme signal un comportement déterminé (fraude), à travers des données de consommation relatives à un nombre indifférencié de personnes ou pour prévoir un tel comportement sur la base d'une analyse de cette masse de données. Ce signal résulte en l'espèce de la comparaison entre la consommation réelle d'eau, de gaz et d'électricité à une adresse déterminée et la consommation moyenne correspondant à la composition de ménage officiellement communiquée à cette même adresse.

Cette technique de traitement comporte néanmoins des risques en ce qui concerne le droit à la protection de la vie privée dont jouissent les intéressés (voir le rapport explicatif de la recommandation (2010)13, points 50-64), en ce qu'elle peut notamment amener à établir de fausses corrélations entre les caractéristiques d'un comportement déterminé et des personnes. Le législateur doit donc prévoir des garanties suffisantes.

B.32.1. La partie requérante fait valoir que le législateur n'a pas désigné un responsable du traitement à chaque étape du système « push ».

B.32.2. Avant que le système « push » ne soit mis en application, le traitement des données de consommation et des adresses dans le cadre de l'exécution normale par les sociétés de distribution et par les gestionnaires de réseaux de distribution se fait conformément aux dispositions de la loi relative à la protection de la vie privée, ces sociétés et ces gestionnaires étant tenus de désigner pour ce faire un responsable au sens de l'article 1er, § 4, de la loi relative à la protection de la vie privée.

En ce qui concerne la sélection des données à transmettre et le flux de données à proprement parler dans le système attaqué, le législateur a cependant choisi de désigner la Banque-carrefour de la sécurité sociale comme responsable du traitement des données.

Le législateur a dès lors prévu que le respect des obligations mentionnées en B.30 dans le cadre du système « push » incombe d'abord à la Banque-carrefour de la sécurité sociale, qui est aussi responsable du respect de ces obligations par le sous-traitant, au sens de l'article 1er, § 5, de la loi relative à la protection de la vie privée, en l'occurrence les sociétés de distribution et les gestionnaires de réseaux de distribution.

Le grief formulé en B.32.1 n'est pas fondé.

B.33.1. La partie requérante fait valoir que le traitement des données à caractère personnel, tel qu'il est prévu dans le système attaqué, n'est pas minimal.

B.33.2. Dans le système attaqué, le législateur oblige les sociétés de distribution et les gestionnaires de réseaux de distribution à collecter les seules données de consommation et les adresses liées à ces données. L'obligation ainsi imposée est limitée à deux types de données qui sont utilisées pour l'exploitation normale.

Les sociétés de distribution et les gestionnaires de réseaux de distribution sont dès lors tenus de transmettre les données de consommation et les adresses à la Banque-carrefour de la sécurité sociale. Le législateur a toutefois fixé un seuil d'écart pour la transmission de ces données, en l'occurrence un écart de plus de 80 % par rapport à la consommation moyenne correspondant à la composition de ménage officiellement communiquée.

B.33.3. Il peut être admis qu'il existe un lien entre la composition du ménage et la consommation d'eau, de gaz et d'électricité. Il peut dès lors être déduit, sur la base des données de consommation, un écart par rapport à la consommation moyenne probable pour le type de ménage officiellement communiqué. Compte tenu de ce qui est dit en B.3.5 et de la marge d'appréciation dont dispose le législateur confronté à des évaluations complexes, il n'apparaît pas que le seuil précité soit manifestement déraisonnable.

B.34. Ce seuil permet en effet de limiter le nombre de personnes dont les données doivent être transmises à la Banque-carrefour de la sécurité sociale au nombre de personnes pour lesquelles il existe des motifs raisonnables qui justifient la poursuite de l'enquête, d'autant plus qu'il s'agit d'un écart significatif.

B.35. Avant de transmettre les données obtenues aux inspecteurs sociaux ou aux IPSS, la Banque-carrefour de la sécurité sociale vérifie, au moyen du répertoire des personnes (article 6 de la loi sur la Banque-carrefour de la sécurité sociale), après croisement avec les données du Registre national, si les données de consommation et les adresses obtenues concernent un bénéficiaire de prestations sociales, de sorte que, lors de la dernière étape, ne sont finalement transmises que les données relatives aux bénéficiaires à l'égard desquels il existe une présomption de fraude sociale au domicile.

B.36. Il découle de ce qui précède que le législateur a prévu de filtrer ce flux de données structurel et volumineux et de le limiter à ce qui est nécessaire pour lutter contre la fraude sociale au domicile.

Dans le système « push », les services publics ont donc seulement accès aux données dont ils ont besoin pour contrôler le caractère fictif ou non du domicile d'un bénéficiaire de prestations sociales. Ce traitement n'a dès lors pas d'effets disproportionnés.

Le grief formulé en B.33.1 n'est pas fondé.

B.37.1. La partie requérante fait valoir que le traitement des données personnelles des intéressés viole leurs droits de contrôle, en ce que l'exercice direct de ces droits est exclu.

B.37.2. L'article 3, § 5, 3°, de la loi relative à la protection de la vie privée prévoit que les articles 9, 10, § 1er, et 12 de la même loi (droit à l'information, droit d'accès, droit de rectification et droit d'effacement) ne s'appliquent pas aux autorités publiques désignées par arrêté royal en vue de l'exercice de leurs missions de police administrative. En exécution de l'article 3, § 5, 3°, de la loi relative à la protection de la vie privée, l'article 1er de l'arrêté royal du 11 mars 2015 dispose :

« § 1. Les articles 9, 10, § 1er, et 12 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 ne sont pas applicables aux inspecteurs sociaux et aux fonctionnaires des autorités publiques énumérées au § 2, dans le cadre de leurs missions de police administrative visées dans Livre 1er, Titre 2 et Titre 4, Chapitre 3 du Code pénal social.

§ 2. Ces autorités sont :

- Service public fédéral Emploi, Travail et Concertation sociale;

- Office national de l'Emploi;

- Office national de Sécurité sociale;

- Office national des Vacances Annuelles;

- Institut national d'Assurance Maladie-Invalidité;

- Agence fédérale pour les allocations familiales;

- Office des régimes particuliers de sécurité sociale;

- Fonds des Accidents du Travail;

- Fonds des Maladies professionnelles;

- Office de contrôle des Mutualités et des Unions nationales de mutualités;

- Office national des Pensions;

- Institut national des assurances sociales pour travailleurs indépendants ».

L'intéressé ne peut donc exercer directement ses droits de contrôle sur le traitement de données par les inspecteurs sociaux et par les IPSS, dans la mesure où ce traitement relève de l'exécution de leurs missions de police administrative.

B.37.3. L'article 13 de la loi relative à la protection de la vie privée dispose toutefois :

« Toute personne justifiant de son identité a le droit de s'adresser sans frais à la Commission de la protection de la vie privée pour exercer les droits visés aux articles 10 et 12 à l'égard des traitements de données à caractère personnel visés à l'article 3, § § 4, 5, 6 et 7.

Le Roi détermine, après avis de la Commission de la protection de la vie privée et par arrêté délibéré en Conseil des ministres, les modalités d'exercice de ces droits.

La Commission de la protection de la vie privée communique uniquement à l'intéressé qu'il a été procédé aux vérifications nécessaires.

Toutefois, le Roi détermine, après avis de la commission de la protection de la vie privée, par arrêté délibéré en Conseil des ministres, quelle information peut être communiquée à l'intéressé lorsque la demande de celui-ci porte sur un traitement de données à caractère personnel géré par des services de police en vue de contrôles d'identité ».

L'intéressé peut dès lors exercer ses droits de contrôle en s'adressant à la Commission de la protection de la vie privée.

B.38.1. En vertu de l'article 9, paragraphe 2, de la Convention n° 108, il est possible de déroger au droit de contrôle visé à l'article 8 de cette Convention, dans la mesure où une loi le prévoit et lorsque cette dérogation constitue, dans une société démocratique, une mesure nécessaire à la protection de la sécurité de l'Etat, à la sûreté publique, aux intérêts monétaires de l'Etat, à la répression des infractions pénales et à la protection de la personne concernée et des droits et libertés d'autrui.

B.38.2. L'effectivité et l'efficacité de la lutte contre la fraude - et donc de la protection des intérêts financiers de l'Etat et des droits d'autrui dans un système social - peuvent justifier la limitation des droits de contrôle des intéressés sur le traitement de leurs données personnelles, pour autant que cette limitation du droit d'accès en ce qui concerne les missions de police administrative porte uniquement sur les données relatives à des bénéficiaires de prestations sociales et que la durée de l'exclusion du droit d'accès direct n'excède pas les besoins de l'enquête.

Il découle de ce qui est dit en B.37 que la non-application des articles 9, 10 et 12 de la loi relative à la protection de la vie privée et le droit d'accès indirect, prévu par l'article 13 de la loi relative à la protection de la vie privée, sont limités aux données qui sont traitées par les douze instances visées et par les inspecteurs sociaux, dans le cadre de leurs missions de police administrative. En ce qui concerne les données qui sont traitées par ces institutions publiques et par ces inspecteurs sociaux, pour d'autres missions et à d'autres fins, ces derniers sont tenus au respect des articles 9, 10 et 12 de la loi relative à la protection de la vie privée.

Toutefois, lorsque les besoins d'une enquête ne le justifient plus, il n'est pas raisonnablement justifié de refuser à l'intéressé l'accès direct à ses données personnelles et le contrôle de ces dernières.

B.38.3. Sous réserve de ce qui est mentionné en B.38.2, dernier alinéa, le grief formulé en B.37.1 n'est pas fondé.

B.39.1. La partie requérante fait valoir l'absence de garanties suffisantes en termes de sécurité et de confidentialité.

B.39.2. L'article 16, § 4, de la loi relative à la protection de la vie privée prévoit que le responsable du traitement ainsi que le sous-traitant lui-même doivent prendre les mesures organisationnelles et techniques requises pour protéger les données à caractère personnel, compte tenu de l'état de la technique en la matière, de la nature des données à protéger et des risques potentiels. Le législateur a explicitement désigné les risques à prendre en compte lors de la mise en œuvre de ces mesures de sécurité (destruction accidentelle de données, perte accidentelle de données, modification non autorisée des données, etc.).

B.39.3. Outre les garanties contenues dans la loi relative à la protection de la vie privée, le législateur a également prévu, dans la loi relative à la Banque-carrefour de la sécurité sociale, des garanties concernant le secret professionnel, la désignation d'un conseiller en sécurité et les mesures de sécurité (articles 22, 23, 24, 25 et 28 de la loi sur la Banque-carrefour de la sécurité sociale). En ce qui concerne l'inspection sociale également, l'article 58 du Code pénal social garantit la confidentialité des données sociales mises à disposition des inspecteurs sociaux. Aux articles 213 à 215 du Code pénal social, le législateur a également prévu des sanctions en cas de non-respect de la confidentialité des données ou en cas d'absence des mesures de sécurité requises.

B.39.4. Il ressort de ce qui précède que le législateur a prévu des garanties pour assurer la sécurité et la confidentialité des données à caractère personnel qui sont traitées.

Le grief formulé en B.39.1 n'est pas fondé.

B.40. La partie requérante invoque l'absence de garanties procédurales, telles qu'elles sont par exemple contenues dans la loi du 3 août 2012 portant dispositions relatives aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances dans le cadre de ses missions.

B.41. Les données traitées selon le système « push » peuvent uniquement être utilisées par les services publics comme indication supplémentaire en vue de déterminer si un bénéficiaire de prestations sociales a commis une fraude au domicile (article 102 de la loi-programme (I) du 29 mars 2012, tel qu'il a été remplacé par l'article 4 de la loi attaquée), ce qui exclut tout effet défavorable immédiat pour l'intéressé. En effet, les instances publiques compétentes doivent, le cas échéant, disposer d'autres éléments pour prendre une décision défavorable (par exemple des sanctions en cas de fraude) à l'encontre d'un bénéficiaire de prestations sociales. Dans l'article 103 de la loi-programme (I) du 29 mars 2012, tel qu'il a été modifié par l'article 5 de la loi attaquée, le législateur a prévu que les inspecteurs sociaux informent le bénéficiaire ou, le cas échéant, un tiers, du fait qu'ils peuvent utiliser des données de consommation le concernant, pour les besoins de l'enquête administrative. En vertu de l'article 79 du Code pénal social, les intéressés ont également accès au dossier administratif.

B.42. Si, finalement, l'enquête donne lieu à un « constat » de fraude au domicile repérée au moyen du système « push », le bénéficiaire de prestations sociales concerné peut en outre démontrer en fait ou en droit qu'il n'y a pas eu fraude au domicile. En vertu des principes généraux de bonne administration ou des règles relatives à la procédure pénale, l'intéressé bénéficie de garanties en ce qui concerne ses droits de défense.

B.43. L'article 14 de la loi relative à la protection de la vie privée prévoit que le président du tribunal de première instance, siégeant comme en référé, connaît de toute demande relative au droit accordé par ou en vertu de la loi, d'obtenir communication de données à caractère personnel, et de toute demande tendant à faire rectifier, supprimer ou interdire d'utiliser toute donnée à caractère personnel inexacte ou, compte tenu du but du traitement, incomplète ou non pertinente, dont l'enregistrement, la communication ou la conservation sont interdits, au traitement de laquelle la personne concernée s'est opposée ou encore qui a été conservée au-delà de la période autorisée. En vertu de l'article 32, § 3, de la loi relative à la protection de la vie privée, le président de la Commission de la protection de la vie privée peut, le cas échéant après une plainte de l'intéressé, soumettre au tribunal de première instance tout litige concernant l'application de cette loi et de ses mesures d'exécution.

L'intéressé dispose dès lors de voies de recours pour soumettre au contrôle du juge l'ingérence dans son droit au respect de la vie privée résultant du traitement de ses données personnelles.

B.44. Il ressort de ce qui précède que la loi attaquée offre des garanties procédurales suffisantes.

Le grief formulé en B.40 n'est pas fondé.

B.45. La partie requérante fait valoir que le législateur n'a pas fixé de délais de conservation suffisamment spécifiques.

B.46. En vertu de l'article 4, § 1er, 3°, 4° et 5°, de la loi relative à la protection de la vie privée, eu égard à l'objectif spécifique poursuivi, l'obligation s'applique, lors de chaque phase, de ne plus traiter les données à caractère personnel qui ne sont pas (ou qui ne sont plus) pertinentes ou qui sont erronées, de les rectifier ou de les supprimer, et en tout cas de ne pas les conserver plus longtemps que nécessaire pour atteindre l'objectif poursuivi, en l'occurrence la collecte et la transmission de données de consommation à la BCSS, le recoupement et le transfert de ces données par la BCSS aux services publics intéressés. Les IPSS et les inspecteurs sociaux sont également soumis à l'interdiction de conserver les données au-delà de la période nécessaire pour contrôler l'utilisation d'une adresse fictive à des fins de fraude aux allocations, de sorte qu'en tout état de cause, ces données ne peuvent être conservées au-delà du délai de prescription prévu en cas de fraude.

Le grief formulé en B.45 n'est pas fondé.

B.47. La partie requérante fait encore valoir que le législateur n'a pas choisi la mesure la moins extrême pour renforcer la lutte contre la fraude sociale au domicile.

B.48. Il ressort des travaux préparatoires mentionnés en B.2 que, pour lutter contre la fraude sociale au domicile, le législateur a envisagé deux façons d'utiliser les données de consommation : le système « pull » (*statu quo*) et le système « push » (nouvel instrument).

B.49. Dans les deux systèmes, en cas de suspicion de fraude, les services publics reçoivent uniquement, en vue du contrôle de la fraude sociale au domicile, les données de consommation de bénéficiaires de prestations sociales.

La différence essentielle entre les deux systèmes porte sur la façon dont l'autorité publique arrive à la présomption de fraude précitée. Dans le système attaqué, la présomption est alimentée par des procédés techniques permettant une analyse automatique et structurelle des données de consommation de tous les consommateurs en vue de déclencher des signaux d'alerte sur la base d'un profil, alors que le système « pull » n'utilise aucune donnée concernant des tiers.

B.50. Eu égard au fait que la lutte contre la fraude sociale au domicile est une lutte permanente nécessitant des efforts continus, et que la fraude et la lutte contre celle-ci sont sujettes à des changements de comportement social, notamment eu égard aux moyens techniques disponibles, le législateur a pu raisonnablement estimer que le système « push » permet de lutter de manière plus effective et efficace contre la fraude sociale.

B.51. De l'explication du système « pull » donnée en B.1.3, il ressort que ce système requiert un investissement énorme en personnel et en moyens pour permettre de lutter efficacement contre la fraude sociale au domicile. Eu égard au rayon d'action limité de ce système, ce dernier ne semble pas permettre de soumettre le même nombre de bénéficiaires sociaux à une enquête et ne permet donc pas non plus de détecter le même nombre de cas présumés de fraude que le système « push » attaqué. Ceci vaut également *mutatis mutandis* pour les instruments de recherche évoqués par la partie requérante, tels que la visite domiciliaire, la collecte d'informations et l'audition de personnes (articles 24, 26 et 27 du Code pénal social). En ce qui concerne la réclamation spécifique et individualisée de données, le système « pull » est également de nature à stigmatiser les intéressés - d'une part, en tant que bénéficiaires de prestations sociales et, d'autre part, en tant que fraudeurs présumés - et donc à avoir des conséquences néfastes sur la vie privée.

B.52. Du fait du rôle de la BCSS, le système « push » empêche les sociétés de distribution et les gestionnaires de réseaux de distribution de connaître, parmi leurs consommateurs, ceux qui bénéficient de prestations sociales, ce qui réduit au strict nécessaire l'ingérence dans la vie privée des bénéficiaires de prestations sociales. Il ressort également de ce qui est dit en B.29 à B.44 que le législateur a prévu les conditions et garanties matérielles et procédurales nécessaires en termes d'ingérence dans la vie privée.

B.53. Il ressort de ce qui précède, et en particulier compte tenu de ce qui est mentionné en B.1.2 et B.52 et des différences entre les deux systèmes, que le législateur pouvait raisonnablement considérer que le système « push », tel qu'il est instauré par l'article 2 de la loi attaquée, ne va pas au-delà de ce qui est nécessaire pour détecter, décourager et combattre la fraude sociale au domicile de manière performante et efficace.

Le grief mentionné en B.47 n'est pas fondé.

B.54. La Cour doit encore vérifier si le système « push » attaqué, qui, tel qu'il est exposé en B.3, implique le « profilage » et la technique de traitement « data mining », n'engendre pas des effets disproportionnés.

B.55. Eu égard à l'objectif poursuivi, qui consiste notamment à détecter des cas présumés de fraude au domicile jusque-là impossibles ou très difficiles à détecter, et compte tenu du caractère dissuasif du système « push », des changements dans le comportement de personnes du groupe-cible, et de l'imprévisibilité des agissements frauduleux et du nombre de cas, il n'est pas sans justification raisonnable qu'en fixant la mesure, le législateur ne puisse faire aucune estimation globale et définitive des recettes et coûts liés au système et donc à l'efficacité de celui-ci.

Le grief mentionné en B.54 n'est pas fondé.

Le « datawarehouse » et le « data mining »

B.56. La partie requérante demande l'annulation de l'article 3 parce que le regroupement et l'analyse de données disponibles par les IPSS iraient au-delà de ce qui est nécessaire pour lutter contre la fraude sociale au domicile et parce que les garanties telles que la condition d'une autorisation décernée par le comité sectoriel de la sécurité sociale et de la santé et les conditions d'intégrité et de confidentialité seraient inexistantes ou insuffisantes.

B.57. Le regroupement des données dont peuvent disposer les IPSS et les inspecteurs sociaux qui en relèvent le cas échéant, ainsi que la recherche, dans ces données, d'éventuels corrélations et indicateurs concernant le risque d'utilisation d'une adresse fictive peuvent raisonnablement être considérés comme un moyen approprié pour renforcer la lutte contre la fraude sociale au domicile.

B.58. Ainsi qu'il ressort de ce qui a été mentionné en B.30, les garanties offertes par la loi relative à la protection de la vie privée s'appliquent également au traitement qui découle de l'article 3 attaqué.

B.59. La partie requérante fait valoir que l'article 3 attaqué ne requiert aucune autorisation de la part d'un comité sectoriel de la sécurité sociale et de la santé, en ce qui concerne la transmission de données aux inspecteurs sociaux.

B.60. Compte tenu de l'annulation mentionnée en B.21 et de la portée, limitée aux IPSS, de l'article attaqué, le grief formulé en B.59 n'est pas fondé.

B.61. Enfin, la partie requérante fait valoir que l'article 3 attaqué viole les principes d'intégrité et de confidentialité, en ce qu'il ne prévoit pas de garanties suffisantes.

B.62. L'article 16, § 4, de la loi relative à la protection de la vie privée impose aux IPSS, en leur qualité de responsables du traitement des données, de prendre des mesures organisationnelles et techniques adéquates, qui sont nécessaires pour garantir la protection des données à caractère personnel, compte tenu de l'état de la technique et de la nature des données à protéger, ainsi que des risques potentiels. A cet égard, le législateur a explicitement désigné les risques à prendre en compte lors de la mise en œuvre de ces mesures de sécurité (destruction accidentelle de données, perte accidentelle de données, modification non autorisée des données, etc.).

Le grief mentionné en B.61 n'est pas fondé.

B.63. Il ressort de ce qui précède, compte tenu également du caractère initialement codé des analyses visées, que l'article 3 de la loi attaquée ne va pas au-delà de ce qui est nécessaire pour renforcer la lutte contre la fraude sociale au domicile. La détection de corrélations et de nouveaux indices est en outre nécessaire pour suivre les évolutions des actes frauduleux et traquer d'éventuels cas de fraude.

Les griefs mentionnés en B.56 ne sont pas fondés.

Par ces motifs,

la Cour

- annule les mots « dans le cadre de l'article 101, § 1er, » et « visées à l'article 101, § 1er », contenus respectivement dans les paragraphes 2 et 3 de l'article 101/1 de la loi-programme (I) du 29 mars 2012, tels qu'ils ont été insérés par l'article 3 de la loi du 13 mai 2016 « modifiant la loi-programme (I) du 29 mars 2012 concernant le contrôle de l'abus d'adresses fictives par les bénéficiaires de prestations sociales, en vue d'introduire la transmission systématique de certaines données de consommation de sociétés de distribution et de gestionnaire de réseaux de distribution vers la BCSS améliorant le datamining et le datamatching dans la lutte contre la fraude sociale »;

- rejette le recours pour le surplus, sous réserve de ce qui est dit en B.38.2, dernier alinéa.

Ainsi rendu en langue néerlandaise, en langue française et en langue allemande, conformément à l'article 65 de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, le 15 mars 2018.

Le greffier,
P.-Y. Dutilleux

Le président,
E. De Groot

VERFASSUNGSGERICHTSHOF

[2018/201410]

Auszug aus dem Entscheid Nr. 29/2018 vom 15. März 2018

Geschäftsverzeichnisnummer 6552

In Sachen: Klage auf teilweise Nichtigerklärung des Gesetzes vom 13. Mai 2016 « zur Abänderung des Programmgesetzes (I) vom 29. März 2012 in Bezug auf die Kontrolle des Missbrauchs fiktiver Adressen durch die Anspruchsberechtigten von Sozialleistungen im Hinblick auf die Einführung der systematischen Übermittlung bestimmter Verbrauchsdaten durch Verteilungsunternehmen und Verteilernetzbetreiber an die ZDSS zur Verbesserung des Data-Mining und Data-Matching im Rahmen der Bekämpfung des Sozialbetrugs », erhoben von der VoG « Ligue des Droits de l'Homme ».

Der Verfassungsgerichtshof,

zusammengesetzt aus den Präsidenten A. Alen und J. Spreutels, den Richtern L. Lavrysen, J.-P. Moerman, E. Derycke und F. Daoût, und dem emeritierten Präsidenten E. De Groot gemäß Artikel 60*bis* des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof, unter Assistenz des Kanzlers P.-Y. Dutilleux, unter dem Vorsitz des emeritierten Präsidenten E. De Groot,

erlässt nach Beratung folgenden Entscheid:

I. *Gegenstand der Klage und Verfahren*

Mit einer Klageschrift, die dem Gerichtshof mit am 28. November 2016 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 29. November 2016 in der Kanzlei eingegangen ist, erhob die VoG « Ligue des Droits de l'Homme », unterstützt und vertreten durch RA R. Jespers, in Antwerpen zugelassen, Klage auf teilweise Nichtigerklärung des Gesetzes vom 13. Mai 2016 « zur Abänderung des Programmgesetzes (I) vom 29. März 2012 in Bezug auf die Kontrolle des Missbrauchs fiktiver Adressen durch die Anspruchsberechtigten von Sozialleistungen im Hinblick auf die Einführung der systematischen Übermittlung bestimmter Verbrauchsdaten durch Verteilungsunternehmen und Verteilernetzbetreiber an die ZDSS zur Verbesserung des Data-Mining und Data-Matching im Rahmen der Bekämpfung des Sozialbetrugs » (veröffentlicht im *Belgischen Staatsblatt* vom 27. Mai 2016).

(...)

II. *Rechtliche Würdigung*

(...)

Zum Kontext der beanstandeten Bestimmungen

B.1.1. Das beanstandete Gesetz vom 13. Mai 2016 « zur Abänderung des Programmgesetzes (I) vom 29. März 2012 in Bezug auf die Kontrolle des Missbrauchs fiktiver Adressen durch die Anspruchsberechtigten von Sozialleistungen im Hinblick auf die Einführung der systematischen Übermittlung bestimmter Verbrauchsdaten durch Verteilungsunternehmen und Verteilernetzbetreiber an die ZDSS zur Verbesserung des Data-Mining und Data-Matching im Rahmen der Bekämpfung des Sozialbetrugs » (nachfolgend: Programmgesetz (I) vom 29. März 2012) regelt, im Rahmen der Bekämpfung des sozialen Wohnsitzbetrugs, zum einen den Datenaustausch zwischen Verteilungsunternehmen und Verteilernetzbetreibern einerseits und öffentlichen Behörden andererseits und zum anderen die Analyse einer großen Menge an Sozialdaten. ZDSS steht für Zentrale Datenbank der sozialen Sicherheit.

B.1.2. Mit dem beanstandeten Gesetz wollte der Gesetzgeber eine klare Vorgabe in der Koalitionsvereinbarung und späteren politischen Programmen zum Ergreifen neuer Maßnahmen bei der Bekämpfung von Sozialbetrug umsetzen. Der Gesetzgeber beabsichtigte, die Bekämpfung von sozialem Wohnsitzbetrug sukzessiv in mehreren Schritten zu verschärfen und durch neue Instrumente im Rahmen der Kontrolle von Missbräuchen effizienter zu gestalten (*Parl. Dok.*, Kammer, 2011-2012, DOK 53-2081/017, S. 22; *Parl. Dok.*, Kammer, 2015-2016, DOK 54-1554/001, S. 8; *Parl. Dok.*, Kammer, 2015-2016, DOK 54-1554/005, S. 54).

B.1.3. Das Programmgesetz (I) vom 29. März 2012 sah vor, dass Anspruchsberechtigte von Sozialleistungen im Rahmen einer Kontrolle aufgefordert wurden, ihre Verbrauchsdaten bezüglich Wasser, Gas und Strom gegebenenfalls vorzulegen. Durch vorgenanntes Programmgesetz wurde die gesetzliche Möglichkeit für die Sozialinspektion geschaffen, diese Verbrauchsdaten bei Verteilungsunternehmen oder Verteilernetzbetreibern zu beantragen (das sogenannte « Pull »-System).

Artikel 101 des Programmgesetzes (I) vom 29. März 2012, vor dessen Änderung durch den beanstandeten Artikel 2, legte fest:

« Wenn die Sozialinspektoren im Rahmen einer Untersuchung auf der Grundlage anderer Elemente vermuten, dass ein Anspruchsberechtigter eine fiktive Adresse nutzt, um Anspruch zu erheben auf Sozialleistungen, auf die er keinen Anspruch erheben kann, können sie die Daten des Wasser-, Strom- und Gasverbrauchs bei den Verteilungsunternehmen und den Verteilernetzbetreibern beantragen.

Diese Verbrauchsdaten können als zusätzlicher Hinweis gebraucht werden, um nachzuweisen, dass es sich um eine fiktive Adresse handelt ».

Dieser Artikel wurde bei der parlamentarischen Vorbereitung wie folgt kommentiert:

« Deze afdeling beoogt, in uitvoering van de notificatie van de begrotingsopmaak 2012, enkele nieuwe instrumenten aan te reiken aan de controle-instanties om de fraudebestrijding bij uitkeringen vanwege de overheid aan te scherpen. Het wil een aanzet vormen voor een betere handhaving van de uitkeringen. Het doel is te bewerkstelligen dat aan elke sociaal verzekerde de correcte uitkering wordt betaald.

In concreto krijgen de sociale inspecteurs de mogelijkheid om de verbruiksgegevens van water, elektriciteit en gas van personen die recht hebben op een sociale prestatie op te vragen bij de nutsbedrijven en de distributiebeheerders.

Deze laatste zijn verplicht om op een dergelijk verzoek in te gaan en de gegevens te verschaffen » (*Parl. St.*, Kamer, 2011-2012, DOC 53-2081/001, p. 71).

« Sociale inspecteurs krijgen het recht om de verbruiksgegevens van nutsvoorzieningen (water, elektriciteit en gas) op te vragen bij nutsbedrijven en distributienetbeheerders indien zij op basis van andere elementen vermoeden dat een gerechtigde van sociale prestaties domiciliefraude pleegt. Voor de nutsbedrijven en distributienetbeheerders, die tot nu toe niet in alle gevallen op een informatieverzoek ingaan, zal een verplichting gelden om op dergelijk verzoek in te gaan en de gegevens te verschaffen. De aangereikte informatie kan een bijkomende indicatie van misbruik, doch geen sluitend bewijs opleveren.

Deze maatregel is een eerste stap, maar zorgt niet voor een integrale oplossing van het probleem. Andere hervormingen zijn in de toekomst nodig om domiciliefraude te beteugelen » (*Parl. St.*, Kamer, 2011-2012, DOC 53-2081/017, p. 22).

B.1.4. Dieses sogenannte « Pull »-System wurde in der Praxis nie angewandt (*Parl. Dok.*, Kammer, 2015-2016, DOK 54-0020/063, S. 14).

B.2.1. Das beanstandete Gesetz ersetzt das vorgenannte « Pull »-System durch das sogenannte « Push »-System und sieht neue Möglichkeiten bei « Data-Mining » im Rahmen der Bekämpfung von sozialem Wohnsitzbetrug vor.

B.2.2. Hinsichtlich der Einführung des « Push »-Datenaustauschsystems erwähnt die parlamentarische Vorbereitung:

« Het bestaande zogenaamde ' pull ' systeem, waarbij nutsbedrijven en de distributienetbeheerders deze verbruiksgegevens op vraag van de inspectiediensten moeten overmaken, wordt omgezet in een ' push ' systeem. Dit betekent dat de nutsbedrijven en distributienetbeheerders de bedoelde verbruiksgegevens voortaan automatisch elektronisch sturen naar de [Kruispuntbank van de Sociale Zekerheid; hierna : KSZ]. Deze gegevens zullen dienen als bijkomende indicatoren om de sociale inspectiediensten toe te laten domiciliefraude beter te detecteren. *In concreto* zullen de verbruiksgegevens door de KSZ aangewend worden bij datamatching en, in een latere fase, als extra indicatoren bij de datamining. Op deze manier komt de regering tegemoet aan punt 31 van het advies van de Commissie ter bescherming van de persoonlijke levenssfeer (CBPL) dat geen bijkomende gegevens noch over het sociaal statuut van de betrokkene, noch over de gezinssamenstelling, worden doorgegeven aan de nutsbedrijven en distributienetbeheerders » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/001, pp. 5-6).

Bezüglich der Einführung des neuen Systems wird außerdem Folgendes erwähnt:

« Het in 2012 ingevoerde *pull*-systeem was een stap in de goede richting. Nu is het nodig om over te gaan naar het meer doeltreffende *push*-systeem, in eerste instantie in het kader van een testfase die toelaat om de methode te verbeteren » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/005, p. 54).

Im Rahmen der parlamentarischen Vorbereitung wird daraufhin der Mehrwert des « Push »-Systems erläutert:

« De meerwaarde van deze beleidsverschuiving ligt in het feit dat de push van extreem laag of extreem hoog verbruik ten opzichte van het gemiddelde verbruik, afhankelijk van de gezinssamenstelling, een knipperlicht activeert in de gevallen waar er nog geen vermoeden van fraude is. Daar ligt ook de toegevoegde waarde van de datamining: de controles meer efficiënt en gerichter maken. Bij het ' pull ' systeem is deze toegevoegde waarde zeer beperkt aangezien men op basis van een concreet dossier met een vermoeden van fraude bijkomende gegevens opvraagt » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/001, p. 6).

B.2.3.1. In Bezug auf die vom Gesetzgeber verfolgten Ziele erwähnt die parlamentarische Vorbereitung:

« Overeenkomstig de begrotingsnotificatie die door de Ministerraad op 3 april 2015 (blz. 39-40) goedgekeurd werd, is het doel van dit ontwerp van wet om het mogelijk te maken verbruiksgegevens van particulieren systematisch door te zenden van nutsbedrijven naar de Kruispuntbank van de sociale zekerheid. Dit moet de controle op de correcte toekenning van sociale prestaties versterken.

Meer en meer groeit het bewustzijn dat uitkeringsfraude een hypotheek legt op onze sociale zekerheid. Deze kan maar bestaan in zoverre zij een breed draagvlak heeft dat wordt gedragen door de solidariteit.

Uitkeringsfraude treft onze sociale zekerheid in het hart. Zij ondermijnt immers één van haar basisbeginselen, met name de solidariteit. Dit principe vormt één van de grondslagen van ons stelsel.

Tal van burgers betalen hun bijdragen eerlijk en ontvangen hun uitkeringen rechtmatig. Slechts een bepaalde groep respecteert de regels niet en benadeelt zo de andere burgers die wel correct bijdragen aan het regime van de sociale zekerheid en die er van genieten wanneer ze er recht op hebben.

In verschillende takken van de sociale zekerheid, zoals de werkloosheid en de ziekte- en invaliditeitsverzekering, worden sommige prestaties met een verhoging/toeslag immers toegekend in functie van de familiale situatie van de sociaal verzekerde.

Fictieve domiciliëring is een fraudemechanisme dat hierop inspeelt doordat de sociaal verzekerde bewust zijn werkelijke domicilie en/of familiale situatie niet aangeeft om op ongeoorloofde wijze een hogere uitkering te krijgen dan diegene waarop hij recht heeft.

Rekening houdende met de impact hiervan, is de aan de fictieve domiciliëring verbonden sociale fraude een fenomeen waaraan de inspectiediensten bijzondere aandacht besteden.

In het kader van een versterking van de strijd tegen de sociale fraude, werden externe maatregelen (versterking van de samenwerking met de magistraten, de politie en de andere openbare instellingen van sociale zekerheid) alsook interne maatregelen (invoering van nieuwe administratieve procedures) uitgewerkt en ingevoerd.

Er werd eveneens beslist om een globale strategie voor de bestrijding van fictieve domiciliëring te voorzien waarbij alle instellingen van sociale zekerheid en de organismen voor toekenning van sociale voordelen zijn betrokken en dit door opsporings- en vervolgingsrichtlijnen voor te schrijven met respect voor de privacy.

Het College van Procureurs-generaal heeft een omzendbrief uitgevaardigd over dit sociaal fraudefenomeen bestaande uit fictieve inschrijvingen. Deze omzendbrief van het College (COL PG 17/2013) en het bijhorend vademecum zijn in voege getreden op 2 september 2013 » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/001, pp. 4-5).

B.2.3.2. Daraus ergibt sich, dass der Gesetzgeber, unter Zugrundelegung des Standpunkts, dass Leistungsbetrug die Solidarität als Grundpfeiler der sozialen Sicherheit untergräbt, die Bekämpfung von Sozialbetrug als gewichtige gesellschaftliche Angelegenheit angesehen hat. Im Hinblick auf diese Bekämpfung wurden bereits mehrere Maßnahmen ergriffen. Mit der beanstandeten Regelung wird insbesondere sozialer Wohnsitzbetrug unter Berücksichtigung der engen Beziehung zwischen der Höhe der Sozialleistungen, der Wohnsitz- und der Haushaltssituation in den Blick genommen.

B.3.1. Mithin hat der Gesetzgeber vor, die Bekämpfung von sozialem Wohnsitzbetrug durch den Einsatz von modernen Verarbeitungstechniken zu verschärfen, ohne dass die ausgewählten und übermittelten Verbrauchsdaten, die sogenannten Betrugswarnleuchten, bei der Feststellung bestimmend sind, ob ein Anspruchsberechtigter von Sozialleistungen eine fiktive Adresse nutzt.

Das beanstandete Gesetz bezweckt somit, den öffentlichen Behörden, d. h. den Sozialinspektoren und den öffentlichen Einrichtungen für soziale Sicherheit (nachfolgend: OESSs), effektivere und effizientere Instrumente zur Erfüllung ihrer gesetzlichen Aufgaben in der sozialen Sicherheit an die Hand zu geben. Sozialinspektoren sind diejenigen Beamten, die unter der Autorität der Minister stehen, zu deren Zuständigkeitsbereich die Beschäftigung und die Arbeit, die soziale Sicherheit, die sozialen Angelegenheiten und die Volksgesundheit gehören, oder die den davon abhängenden öffentlichen Einrichtungen unterstehen und die beauftragt sind mit der Überwachung der Einhaltung der Bestimmungen der Sozialgesetze (Artikel 16 Nr. 1 des Sozialstrafgesetzbuchs). OESSs sind diejenigen öffentlichen Dienste, denen die Anwendung der Gesetze zur sozialen Sicherheit obliegt.

B.3.2. Der Gesetzgeber hat u. a. infolge der Möglichkeiten von « Profiling »-Techniken, die auf « Data-Warehousing », « Data-Matching » und « Data-Mining » beruhen, geurteilt, dass das automatische und systematische Bereitstellen von ausgewählten Adressdaten und Daten zum Wasser-, Gas- und Stromverbrauch an die in B.3.1 erwähnten öffentlichen Behörden einerseits sowie die Analyse der verfügbaren aggregierten Daten und die Suche in diesen Daten nach Risikoindikatoren durch diese Behörden andererseits nützliche Instrumente bei der Bekämpfung von sozialem Wohnsitzbetrug sind.

B.3.3. Das « Profiling » verläuft in drei unterschiedlichen Phasen, bei denen nach oder auf Grundlage von Mustern und Modellen (sogenannten Profilen) gesucht wird. In der ersten Phase geht es um die Erfassung und Speicherung von Informationen über Verhaltensweisen oder Eigenschaften von Personen in großem Rahmen (« Data-Warehousing »),

in der zweiten und dritten Phase um die Analyse und eingehende Untersuchung dieser Daten, um Zusammenhänge zwischen Verhaltensweisen und Eigenschaften festzustellen, und so auf Grundlage der derart festgestellten Zusammenhänge bis jetzt unbekannte oder verborgene (bestehende, zukünftige bzw. vergangene) Eigenschaften und Verhaltensweisen über Personen aus den Daten abzuleiten (« Data-Mining »).

B.3.4. Die « Profiling »-Technik bezweckt daher, auf Grundlage eines Profils, eine Gesamtheit an Eigenschaften, die eine Kategorie von Personen charakterisiert (z. B. Betrüger), eine individuelle Person mit dem Ziel zu erkennen, um Entscheidungen (z. B. Einleiten einer Untersuchung) in Bezug auf diese Person zu treffen sowie ihre persönlichen Vorlieben, Verhaltensweisen und Einstellungen zu analysieren oder vorherzusagen (Punkt 1 d. und e. der Empfehlung Nr. (2010)13 des Ministerkomitees an die Mitgliedstaaten vom 23. November 2010 über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten im Zusammenhang mit « Profiling » (nachfolgend: Empfehlung (2010)13).

B.3.5. Es ist gleichwohl sehr wichtig, dass bei dieser Technik die richtigen Auswahlkriterien (Gesamtheit an Eigenschaften) verwendet werden, um die Bekämpfung von Sozialbetrug zu verschärfen (die sogenannte Betrugswarnleuchte oder die sogenannten Risikoindikatoren). Die Technik weist ja, *a fortiori* in der Anfangsphase des Vorhabens, schwerwiegende Mängel auf, nämlich falsche positive und falsche negative Ergebnisse, was eine dauerhafte Überwachung und Evaluation der Kriterien erforderlich macht (siehe Datenschutzkommission Empfehlung 24/2015, S. 7; Empfehlung 05/2016, S. 6).

B.4. Aus der parlamentarischen Vorbereitung des beanstandeten Gesetzes geht hervor, dass das vom Gesetzgeber verfolgte Ziel implementiert wird, indem eine gesetzliche Grundlage für die verschärfte Kontrolle von sozialem Wohnsitzbetrug über automatischen Datenaustausch zwischen Dienstleistern und öffentlichen Behörden und für die modernen Techniken der Untersuchung in umfangreichen Datenbanken (« Data-Warehousing »), wie « Data-Matching » und « Data-Mining », geschaffen wird, unbeschadet der Anforderungen im Rahmen des Schutzes der Privatsphäre (siehe Artikel 104 des Programmgesetzes (I) vom 29. März 2012):

« Het ontwerp voorziet daarom in een wettelijke basis om bepaalde verbruiksgegevens van water, gas en elektriciteit en adresgegevens van bepaalde particulieren elektronisch over te maken aan de Kruispuntbank van de sociale zekerheid (KSZ) » (*Parl. St*., Kamer, 2015-2016, DOC 54-1554/001, p. 5).

« De Commissie [voor de bescherming van de persoonlijke levenssfeer] adviseerde een gelijkaardige algemene wettelijke basis voor het gebruik van ' *datamining* ' en ' *datamatching* ' aan de hand van de relevante databanken, zoals gebruikt door onder meer het platform OASIS. Hoewel de Commissie duidelijk stelt dat deze aanbeveling het huidige dossier overstijgt, wordt met de toevoeging van deze paragraaf reeds tegemoetgekomen aan deze aanbeveling van de Commissie voor wat betreft de energiegegevens en wordt hiervoor een wettelijke basis voor datamining ingesteld » (*Parl. St*., Kamer, 2015-2016, DOC 54-1554/004, p. 9).

« Met respect voor de privacy zal er zodoende, zoals dit reeds in Nederland het geval is, op automatische wijze kunnen worden nagegaan of de opgegeven verbruiksgegevens al dan niet matchen met domiciliegegevens. Deze gegevenskruising kan knipperlichten doen branden waardoor verder onderzoek noodzakelijk is. De energiegegevens worden vandaag al effectief aangewend in de strijd tegen woningleegstand in Brussel, bijvoorbeeld.

Om dit alles te realiseren wordt de bestaande wetgeving, opgenomen in de artikelen 100 tot en met 105 van de programmawet van 29 maart 2012, aangepast. Deze wet bevat reeds een bepaling die de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens van toepassing maakt. Deze bepaling blijft uiteraard behouden in het nieuwe systeem » (*Parl. St*., Kamer, 2015-2016, DOC 54-1554/001, p. 6).

B.5.1. Die Maßnahmen, durch welche der Gesetzgeber sein Ziel verwirklichen möchte, sind in den Artikeln 2 und 3 des beanstandeten Gesetzes genannt.

B.5.2. Artikel 2 des beanstandeten Gesetzes führt ein « Push »-System ein - das über verschiedene Phasen mit einem sehr spezifischen Ziel verläuft -, bei dem Daten zum Wasser-, Gas- und Stromverbrauch und zur Adresse bestimmter Privatkunden elektronisch an die ZDSS übermittelt werden, die sie filtert und mit anderen Daten abgleicht (« Data-Matching »), um sie den zuständigen OESSs und Sozialinspektoren zwecks Verschärfung und Steigerung der Effizienz der Bekämpfung von Leistungsbetrug bereitzustellen (*Parl. Dok.*, Kammer, 2015-2016, DOK 54-1554/001, S. 5).

In der ersten Phase werden die Verteilungsunternehmen und Verteilungsnetzbetreiber verpflichtet, die Verbrauchs- und Adressdaten zu erfassen. Anschließend haben sie bestimmte Daten wenigstens einmal pro Jahr an die ZDSS zu übermitteln. Diese Daten werden ausgewählt, weil der Verbrauch unter Berücksichtigung der offiziell mitgeteilten Haushaltszusammensetzung mindestens 80 Prozent vom durchschnittlichen Verbrauch abweicht (Artikel 101 § 1 Absatz 1 des Programmgesetzes (I) vom 29. März 2012 in der Fassung der Änderung durch Artikel 2 des beanstandeten Gesetzes). Die Familienmodelle und der durchschnittliche Verbrauch pro Familienmodell werden jährlich vom Geschäftsführenden Ausschuss der ZDSS in Absprache mit den Verteilungsunternehmen und den Verteilernetzbetreibern festgelegt (Artikel 101 § 1 Absatz 2 des Programmgesetzes (I) vom 29. März 2012 in der Fassung der Änderung durch Artikel 2 des beanstandeten Gesetzes).

In der zweiten Phase werden die so erfassten und empfangenen Daten durch die ZDSS, nach Abgleich mit dem Nationalregister zwecks Feststellung, wer unter den übermittelten Adressen wohnt, den OESSs und Sozialinspektoren bereitgestellt, soweit sie dem Anspruchsberechtigten, auf den sich die Daten beziehen, eine Sozialleistung gewähren oder eine Überwachungsfunktion wahrnehmen hinsichtlich der Einhaltung von Gesetzen, die einen Vorteil gewähren (« Data-Matching »; Artikel 101 § 1 Absatz 3 des Programmgesetzes (I) vom 29. März 2012 in der Fassung der Änderung durch Artikel 2 des beanstandeten Gesetzes).

Die Sozialinspektion oder eine OESS kann daraufhin nach Ermächtigung seitens des Sektoriellen Ausschusses der sozialen Sicherheit und der Gesundheit auf Grundlage der empfangenen Daten, in Verbindung mit anderen (personenbezogenen) Daten aus den Sozialdatenbanken, der ZDSS und dem Nationalregister, überprüfen, ob eine Sozialleistung aufgrund einer fiktiven Adresse gewährt wird (« Data-Mining »; Artikel 101 § 1 Absatz 3 des Programmgesetzes (I) vom 29. März 2012 in der Fassung der Änderung durch Artikel 2 des beanstandeten Gesetzes).

Gleichwohl kann aus den übermittelten Verbrauchs- und Adressdaten allein nicht abgeleitet werden, dass der betreffende Anspruchsberechtigte einen sozialen Wohnsitzbetrug begangen hat (Artikel 102 des Programmgesetzes (I) vom 29. März 2012 in der Fassung der Änderung durch Artikel 4 des beanstandeten Gesetzes).

B.5.3. Ferner erlaubt Artikel 3 eine Untersuchung zu den Zusammenhängen und Risikoindikatoren in Bezug auf sozialen Wohnsitzbetrug in aggregierten Daten aus relevanten Sozialdatenbanken (« Data-Mining ») durch eine OESS.

In dieser dritten Phase kann eine OESS, zu der auch die Sozialinspektion gehört, die empfangenen Verbrauchs- und Adressdaten mit anderen ihr verfügbaren Daten aggregieren, um Analysen relationaler Daten durchzuführen, damit den Diensten ermöglicht wird, gezielte Betrugskontrollen auf der Grundlage von Risikoindikatoren in Bezug auf die Gewährung einer Unterstützung aufgrund einer fiktiven Adresse vorzunehmen (Artikel 101/1 des Programmgesetzes (I) vom 29. März 2012 in der Fassung der Einfügung durch Artikel 3 des beanstandeten Gesetzes). Die Analyse erfolgt anhand verschlüsselter Daten, die nur entschlüsselt werden, nachdem sie getrennt wurden, wenn aus der Analyse ein Risiko für die Benutzung einer fiktiven Adresse hervorgeht.

B.6. Der Gesetzgeber hat sich darüber hinaus dafür entschieden, die Ausführungsregeln in Bezug auf das eingeführte System dem Geschäftsführenden Ausschuss der ZDSS zu überlassen. Dieser Ausschuss wird in der parlamentarischen Vorbereitung wie folgt erläutert:

« Er wordt tevens voorzien dat niet de Koning, maar wel het beheerscomité van de Kruispuntbank van de sociale zekerheid het gemiddelde verbruik per gezinstype zal moeten bepalen. Het beheerscomité moet dit doen in overleg met de actoren op het terrein, namelijk de nutsbedrijven en distributienetbeheerders. Deze aanpak maakt het volgens de regering mogelijk om de meest adequate grenswaarden vast te leggen en deze, indien nodig, snel aan te passen aan de veranderende omstandigheden op het terrein om domiciliefraude efficiënt te kunnen bestrijden. Domiciliefraude is immers een evolutief gegeven en bovendien wenst de regering uiteraard in geen geval bonafide gerechtigden te treffen. Aan deze bekommernis wordt tegemoetgekomen door de voorziene delegatie aan het beheerscomité » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/001, pp. 7-8).

Hinsichtlich der beanstandeten Bestimmungen

B.7.1.1. Artikel 2 des beanstandeten Gesetzes ersetzt Artikel 101 des Programmgesetzes (I) vom 29. März 2012 wie folgt:

« § 1. Entsprechend der Regelmäßigkeit ihrer Datenerfassung und mindestens einmal pro Kalenderjahr übermitteln Verteilungsunternehmen und Verteilernetzbetreiber der Zentralen Datenbank der sozialen Sicherheit in elektronischer Form bestimmte Verbrauchsdaten und die Adressen einiger ihrer Privatkunden. Es handelt sich um Daten, die von Verteilungsunternehmen und Verteilernetzbetreibern ausgewählt werden, weil der Verbrauch des Privatkunden den durchschnittlichen Verbrauch, der unter Berücksichtigung der offiziell mitgeteilten Haushaltszusammensetzung bestimmt wird, um mindestens 80 Prozent über-beziehungsweise unterschreitet.

Die Familienmodelle und der durchschnittliche Verbrauch pro Familienmodell werden jährlich vom Geschäftsführenden Ausschuss der Zentralen Datenbank der sozialen Sicherheit in Absprache mit Verteilungsunternehmen und Verteilernetzbetreibern festgelegt.

Die Zentrale Datenbank der sozialen Sicherheit übermittelt den öffentlichen Einrichtungen für soziale Sicherheit und den Sozialinspektoren die in Absatz 1 erwähnten Daten nach Abgleich mit den Daten des Nationalregisters, wie im Gesetz vom 8. August 1983 zur Organisation eines Nationalregisters der natürlichen Personen erwähnt, unter der Bedingung, dass die erwähnten Einrichtungen dem Anspruchsberechtigten, auf den diese Daten sich beziehen, eine Sozialleistung gewähren, entweder aufgrund der sozialen Sicherheit oder aufgrund eines Sozialhilfesystems oder aufgrund anderer Vorteile, die durch die Vorschriften gewährt werden, deren Einhaltung die Sozialinspektoren überwachen. Nach Ermächtigung seitens des Sektoriellen Ausschusses der sozialen Sicherheit und der Gesundheit müssen sie in Verbindung mit anderen im Netzwerk verfügbaren Sozialdaten und personenbezogenen Sozialdaten, so wie sie im Gesetz vom 15. Januar 1990 über die Errichtung und Organisation einer Zentralen Datenbank der sozialen Sicherheit erwähnt sind, überprüfen können, ob die Sozialleistung aufgrund einer fiktiven Adresse gewährt wird.

§ 2. Was die in § 1 erwähnte Datenverarbeitung betrifft, wird als für die Verarbeitung Verantwortliche, so wie in Artikel 1 § 4 des Gesetzes vom 8. Dezember 1992 über den Schutz des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten erwähnt, die Zentrale Datenbank der sozialen Sicherheit angewiesen ».

B.7.1.2. Die parlamentarische Vorbereitung erwähnt zum ersten Paragraphen der neuen Bestimmung:

« Dit artikel verplicht de nutsbedrijven en distributienetbeheerders om in functie van de periodiciteit van hun eigen gegevensinzameling, maar minstens één maal per kalenderjaar bepaalde verbruiks- en adresgegevens van bepaalde van hun particuliere klanten op elektronische wijze aan de Kruispuntbank van de sociale zekerheid te bezorgen. Dit betekent dus dat de gegevens voortaan ' gepusht ' worden. Dit moet dus minstens één maal per jaar, maar indien het voor bepaalde nutsbedrijven en distributienetbeheerders mogelijk is, kunnen de gegevens ook meermaals per jaar doorgestuurd worden. Het gaat om de gegevens die door de nutsbedrijven en distributienetbeheerders geselecteerd worden omdat ze minstens 80 % in neerwaartse of opwaartse zin afwijken van een gemiddeld verbruik waarbij rekening gehouden wordt met [de] officieel meegedeelde gezinssamenstelling De gezinstypes en het gemiddeld verbruik per gezinstype worden jaarlijks bepaald door het beheerscomité van de Kruispuntbank van de sociale zekerheid in overleg met de nutsbedrijven en distributienetbeheerders.

In het voorontwerp van wet was voorzien dat de mededeling van verbruiksgegevens zou gebeuren op basis van bepaalde grenswaarden die kunnen wijzen op een te laag of te hoog verbruik in functie van de officieel meegedeelde gezinssamenstelling. Deze grenswaarden zouden worden vastgesteld door de Koning bij een besluit vastgesteld na overleg in de Ministerraad. De Raad van State heeft in punt 8.2. van zijn advies echter opgemerkt dat deze delegatie aan de Koning te uitgebreid is. Gelet op deze opmerking heeft de regering geoordeeld dat het raadzaam is om inderdaad reeds in de wet zelf een beperking te voorzien. Daarom wordt de 80 % regel in de wet zelf ingeschreven. Er wordt tevens voorzien dat niet de Koning, maar wel het beheerscomité van de Kruispuntbank van de sociale zekerheid het gemiddelde verbruik per gezinstype zal moeten bepalen. Het beheerscomité moet dit doen in overleg met de actoren op het terrein, namelijk de nutsbedrijven en distributienetbeheerders. Deze aanpak maakt het volgens de regering mogelijk om de meest adequate grenswaarden vast te leggen en deze, indien nodig, snel aan te passen aan de veranderende omstandigheden op het terrein om domiciliefraude efficiënt te kunnen bestrijden. Domiciliefraude is immers een evolutief gegeven en bovendien wenst de regering uiteraard in geen geval bonafide gerechtigden te treffen. Aan deze bekommernis wordt tegemoetgekomen door de voorziene delegatie aan het beheerscomité.

Daarnaast moet volgens de CBPL beter verantwoord worden waarom wordt overgestapt van een ' pull ' naar een ' push ' model. Aangezien verschillende openbare instellingen van sociale zekerheid (OISZ) uitkeringen toekennen die variëren in functie van de gezinssamenstelling, is het voor hen van belang om zo goed mogelijk te kunnen controleren of de opgegeven gezinssamenstelling wel correct is. Momenteel doen de inspectiediensten dit onder andere door middel van controles ter plaatse in het opgegeven domicilie of door het opvragen van de verbruiksgegevens bij de sociaal verzekerde zelf of bij de nutsbedrijven of distributienetbeheerders. Het voorgestelde push model dient deze bestaande instrumenten te versterken en de controle dus meer sluitend en performanter te maken. Tijdens de bespreking in de Nationale Arbeidsraad heeft de Rijksdienst voor Arbeidsvoorziening bijvoorbeeld aangegeven dat dit systeem hun sociale inspecteurs inderdaad beter in staat zal stellen om de naleving van de regels van de werkloosheidsreglementering gerichter en doeltreffender te controleren.

Bovendien vraagt de CBPL ook waarom zowel een te laag als te hoog verbruik geviseerd wordt. Gelet op het voorgaande is het logisch dat beide uitersten in aanmerking genomen worden. Het is immers mogelijk dat beide partners van een koppel een uitkering genieten. Om hun beider uitkeringen te verhogen verklaren ze beide alleenstaande te zijn. Om dit te staven hebben ze een apart domicilie. Hierdoor kunnen ze beide een uitkering als alleenstaande genieten. Deze bedraagt uiteraard meer dan een uitkering als samenwonende. In de feiten wonen ze echter nog steeds samen. In het ene domicilie zal het werkelijk verbruik dus in principe lager zijn dan het gemiddelde verbruik van een alleenstaande. In het andere domicilie in principe te hoog. Dankzij deze maatregel kunnen beide vormen van uitkeringsfraude gedetecteerd worden.

Tevens wordt de finaliteit van deze verplichting vastgelegd. Deze gegevens moeten de bevoegde sociaal inspecteurs in staat stellen om na te gaan of de betaalde sociale zekerheids- of bijstandsuitkeringen terecht toegekend werden.

Om dit te kunnen doen moeten deze gegevens gecombineerd worden met andere gegevens waar de bevoegde diensten over beschikken of toegang toe hebben.

Om toegang te krijgen tot de verbruiksgegevens en om ze te mogen combineren met de andere gegevens moeten de geïnteresseerde diensten, zoals steeds, een machtiging vragen van het sectoraal comité van de sociale zekerheid en van de gezondheid.

Ingevolge opmerking 9.4 van de Raad van State werd de tekst aangepast om duidelijker tot uiting te laten komen dat de afwijkende verbruiksgegevens enkel worden meegedeeld door de KSZ indien de betrokken personen uitkeringen ontvangen van de betrokken instellingen.

Deze aanpassing biedt meteen ook een antwoord op de bemerking van de CBPL dat de private bedrijven (nutsbedrijven en distributienetbeheerders) geen aanvullende informatie over de sociaal verzekerde mogen krijgen van de sociale inspectie of het rijksregister. Het gaat zeer duidelijk om éénrichtingsverkeer. De private bedrijven moeten informatie verschaffen. Ze krijgen er geen » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/001, pp. 7-9).

Zum zweiten Paragraphen erwähnt die parlamentarische Vorbereitung:

« In de adviezen van 17 juni 2015 en 3 februari 2016 wijst de Privacycommissie erop dat de verantwoordelijke voor de verwerking niet uitdrukkelijk is aangewezen in het ontwerp. Daar er bij de door het wetsontwerp beoogde aanpak van sociale fraude een groot aantal spelers betrokken zal zijn (distributienetbeheerders, KSZ, sociale inspectie, eventuele verwerkers,...) zal vroeg of laat de vraag rijzen wie de verantwoordelijke is of de verwerker voor de diverse bewerking(en) die het wetsontwerp beoogt. Omdat voor al deze verwerkingen de actuele en toekomstige rechten en plichten moeten worden nageleefd door elke verantwoordelijke onder de WVP en de GDPR, is het belangrijk dat dienaangaande verduidelijking wordt verschaft. Het advies van de Privacycommissie stelt zelf dat deze aanduiding ook op een precieze wijze kan geschieden in de machtigingen tot gegevensuitwisseling. Om de transparantie te verhogen zal de verantwoordelijke voor de verwerking ook duidelijk in de wet worden vermeld. Voor wat betreft de ' *datamatching* ' wordt de ' Kruispuntbank van de Sociale Zekerheid ' aangewezen als de verantwoordelijke voor de verwerking » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/004, p. 7).

B.7.2.1. Artikel 3 des beanstandeten Gesetzes fügt einen neuen Artikel 101/1 in das Programmgesetz (I) vom 29. März 2012 ein, der bestimmt:

« § 1. Öffentliche Einrichtungen für soziale Sicherheit (OESS) können die gemäß Artikel 101 erfassten Daten mit anderen Daten, über die die OESS verfügen, aggregieren, um Analysen relationaler Daten durchzuführen, mit denen ihre Dienste gezielte Kontrollen auf der Grundlage von Risikoindikatoren in Bezug auf die Gewährung einer Unterstützung, die aufgrund einer fiktiven Adresse berechnet wird, vornehmen können. Die Analyse erfolgt anhand verschlüsselter Daten. Daten, aus denen ein Risiko für die Benutzung einer fiktiven Adresse hervorgeht, werden getrennt und entschlüsselt.

§ 2. Damit Datenkategorien im Rahmen von Artikel 101 § 1 einer OESS übermittelt werden können, ist eine Ermächtigung seitens eines sektoriellen Ausschusses, der beim Ausschuss für den Schutz des Privatlebens eingerichtet ist, erforderlich. In der Ermächtigung werden die Bedingungen in Bezug auf die Aufbewahrungsfrist verschlüsselter und entschlüsselter Daten festgelegt.

§ 3. Für die in Artikel 101 § 1 erwähnten Analysen relationaler Daten wird als für die Verarbeitung Verantwortliche, so wie in Artikel 1 § 4 des Gesetzes vom 8. Dezember 1992 über den Schutz des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten erwähnt, die OESS angewiesen, die die Analyse relationaler Daten durchführt ».

B.7.2.2. Die parlamentarische Vorbereitung zum ersten Paragraphen dieser Bestimmung erwähnt:

« Het advies van 3 februari 2016 van de Privacycommissie verwijst naar artikel 5, § 1, van de wet van 3 augustus 2012 houdende bepalingen betreffende de verwerking van persoonsgegevens door de Federale Overheidsdienst Financiën in het kader van zijn opdrachten, die stelt :

' § 1. De Federale Overheidsdienst Financiën kan de overeenkomstig artikel 3 ingezamelde gegevens samenvoegen met het oog op de oprichting van een datawarehouse waarmee zijn diensten enerzijds in staat worden gesteld om gerichte controles uit te voeren op basis van risico-indicatoren en anderzijds analyses kunnen uitvoeren op relationele gegevens afkomstig van verschillende administraties en, of diensten van de Federale Overheidsdienst Financiën. ' De Commissie adviseerde een gelijkaardige algemene wettelijke basis voor het gebruik van ' *datamining* ' en ' *datamatching* ' aan de hand van de relevante databanken, zoals gebruikt door onder meer het platform OASIS. Hoewel de Commissie duidelijk stelt dat deze aanbeveling het huidige dossier overstijgt, wordt met de toevoeging van deze paragraaf reeds tegemoetgekomen aan deze aanbeveling van de Commissie voor wat betreft de energiegegevens en wordt hiervoor een wettelijke basis voor datamining ingesteld » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/004, p. 9).

In Bezug auf den zweiten Paragraphen heißt es:

« In de adviezen van 17 juni 2015 en 3 februari 2016 stelt de Privacycommissie de vraag naar een gepaste bewaringstermijn voor de gegevens, rekening houdend met artikel 4, § 1, 4°, van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (WVP). De Commissie stelt dat de vaststelling van een bewaringstermijn op precieze wijze kan geschieden in de machtigingen tot gegevensuitwisseling. In paragraaf 2 wordt vastgelegd dat deze machtigingen bewaringstermijnen moeten bevatten voor gecodeerde en gedecodeerde gegevens » (*ibid.*).

Der dritte Paragraph wird wie folgt erläutert:

« Voor wat betreft de ' datamining ' wordt de ' OISZ die de analyse op relationele gegevens uitvoert ' aangewezen als de verantwoordelijke voor de verwerking » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/004, p. 10).

B.7.3.1. Artikel 4 des beanstandeten Gesetzes ersetzt Artikel 102 des Programmgesetzes (I) vom 29. März 2012 wie folgt:

« Die in Artikel 101 erwähnten Daten können nur als zusätzlicher Hinweis gebraucht werden, um festzustellen, ob ein Anspruchsberechtigter eine fiktive Adresse nutzt ».

B.7.3.2. Die parlamentarische Vorbereitung erwähnt zu dieser Bestimmung:

« Dit artikel bepaalt dat de gegevens enkel als bijkomend element gebruikt kunnen worden om uit te maken of een gerechtigde gebruik maakt van een fictief adres.

Het is inderdaad niet de bedoeling om louter op basis van verbruiksgegevens te besluiten dat er fraude in het spel is. Daarvoor zijn deze gegevens op zichzelf genomen niet voldoende doorslaggevend » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/001, p. 9).

B.7.4. Artikel 5 des beanstandeten Gesetzes ersetzt das Wort « beantragen » in Artikel 103 des Programmgesetzes (I) vom 29. März 2012 durch das Wort « verwenden ».

B.7.5.1. Artikel 6 des beanstandeten Gesetzes ersetzt Artikel 105 des Programmgesetzes (I) vom 29. März 2012 wie folgt:

« Der Geschäftsführende Ausschuss der Zentralen Datenbank der sozialen Sicherheit bestimmt die Modalitäten, unter anderem die Struktur und den Inhalt der Mitteilungen, mit denen die Daten übermittelt werden, die Art und den Zeitpunkt der Übermittlung der Verbrauchsdaten und Adressen ».

B.7.5.2. Die parlamentarische Vorbereitung erwähnt zu dieser Bestimmung:

« Dit artikel voorziet in een delegatie aan het beheerscomité van de Kruispuntbank van de sociale zekerheid.

Het beheerscomité dient de nadere regels te bepalen om de maatregel in de praktijk te implementeren. Het gaat onder meer om de structuur en inhoud van de berichten en de wijze en het tijdstip waarop de verbruiks- en adresgegevens moeten worden overgemaakt. Dergelijke delegatie aan het beheerscomité is niet nieuw en wordt verantwoord door het feit dat het gaat om vaak technische aspecten waarvoor het noodzakelijk is om in een snel veranderende informatica-omgeving kort op de bal te kunnen spelen » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1554/001, pp. 9-10).

Zur Zulässigkeit der Klage

B.8.1. Soweit die antragstellende Partei ausschließlich Einwände in Bezug auf Artikel 2, 3 und 4 des beanstandeten Gesetzes geltend macht, ist die Klage zulässig, wenn sie sich gegen diese Artikel richtet.

B.8.2.1. Der Ministerrat bestreitet die Zulässigkeit der meisten mit dem einzigen Klagegrund geltend gemachten Einwände, weil sie nicht hinreichend dargelegt oder irrelevant seien. Außerdem trägt er mehrfach vor, dass ein Einwand ganz oder teilweise unzulässig sei, weil der Gerichtshof keine Befugnis habe, unmittelbar zu prüfen, ob völkerrechtliche Vertragsbestimmungen, Rechtsnormen mit Gesetzeskraft (Gesetz vom 8. Dezember 1992 über den Schutz des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten, nachfolgend: Datenschutzgesetz), Rechtsakte der Europäischen Union (Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (nachfolgend: Richtlinie 95/46/EG) und Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)) und die allgemeinen Grundsätze der Notwendigkeit, der Subsidiarität, der Verhältnismäßigkeit, der Transparenz, der Speicherbegrenzung, der Rechenschaftspflicht, der Integrität und der Sicherheit eingehalten worden seien.

B.8.2.2. Der Gerichtshof ist befugt, Rechtsnormen mit Gesetzeskraft auf ihre Rechtmäßigkeit vor dem Hintergrund der Regeln, die die Zuständigkeiten zwischen dem Föderalstaat, den Gemeinschaften und den Regionen verteilen, sowie der Artikel von Titel II (« Die Belgier und ihre Rechte ») und der Artikel 143 § 1, 170, 172 und 191 der Verfassung zu prüfen.

Alle Einwände beziehen sich auf einen Verstoß gegen eine oder mehrere dieser Regeln, deren Einhaltung der Gerichtshof gewährleistet.

Soweit die antragstellende Partei ferner auch völkerrechtliche Vertragsbestimmungen, Rechtsakte der Europäischen Union, Rechtsnormen mit Gesetzeskraft und allgemeine Grundsätze erwähnt, prüft der Gerichtshof diese nur insoweit, als ein Verstoß gegen die vorgenannten Verfassungsbestimmungen in Verbindung mit den vorgenannten Bestimmungen, Akten und Grundsätzen geltend gemacht wird. In diesem Umfang sind die Einwände zulässig.

B.8.3. Um den Anforderungen von Artikel 6 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof zu entsprechen, müssen die im Antrag aufgeführten Klagegründe nicht nur erkennen lassen, welche der Regeln, deren Einhaltung der Gerichtshof gewährleistet, verletzt worden seien, sondern auch bei welchen Bestimmungen ein Verstoß gegen diese Regeln vorliege, und darlegen, in welcher Hinsicht diese Regeln durch die genannten Bestimmungen verletzt seien.

Der Gerichtshof prüft die Einwände des einzigen Klagegrundes, soweit sie die vorgenannten Anforderungen erfüllen.

B.8.4. Die Einreden werden verworfen.

Zum Recht auf Achtung des Privatlebens

B.9. Der einzige Klagegrund beruht hauptsächlich, wenn auch nicht ausschließlich, auf einem Verstoß gegen das Recht auf Achtung des Privatlebens, das durch Artikel 22 der Verfassung in Verbindung mit Artikel 8 der Europäischen Menschenrechtskonvention, Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte und den Artikeln 7 und 8 der Charta der Grundrechte der Europäischen Union geschützt ist.

B.10.1. Artikel 22 der Verfassung bestimmt:

« Jeder hat ein Recht auf Achtung vor seinem Privat- und Familienleben, außer in den Fällen und unter den Bedingungen, die durch Gesetz festgelegt sind.

Das Gesetz, das Dekret oder die in Artikel 134 erwähnte Regel gewährleistet den Schutz dieses Rechtes ».

B.10.2. Artikel 8 der Europäischen Menschenrechtskonvention bestimmt:

« 1. Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.

2. Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer ».

B.10.3. Der Verfassungsgeber wollte eine möglichst große Übereinstimmung zwischen Artikel 22 der Verfassung und Artikel 8 der Europäischen Menschenrechtskonvention erreichen (*Parl. Dok.*, Kammer, 1992-1993, Nr. 997/5, S. 2).

Die Tragweite dieses Artikels 8 entspricht derjenigen der vorgenannten Verfassungsbestimmung, sodass die durch die beiden Bestimmungen gewährleisteten Garantien eine untrennbare Einheit bilden.

B.10.4. Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte bestimmt:

« 1. Niemand darf willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden.

2. Jede Person hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen ».

B.10.5. Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union (GRC) bestimmen:

« Art. 7. Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation ».

« Art. 8. 1. Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

2. Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

3. Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht ».

Bei der Prüfung im Rahmen vorgenannter Artikel 7 und 8 ist Artikel 52 Absatz 1 der GRC zu berücksichtigen, in dem es heißt:

« Jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten muss gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie notwendig sind und den von der Union anerkannten, dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen ».

B.11. Das Recht auf Achtung des Privatlebens, wie in den vorerwähnten Verfassungs- und Vertragsbestimmungen gewährleistet, hat als wesentliches Ziel, jede Person vor Eingriffen in ihr Privatleben zu schützen.

Dieses Recht hat eine weitreichende Tragweite und umfasst, u. a., den Schutz personenbezogener Daten und persönlicher Informationen. Die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte zeigt, dass, u. a., folgende personenbezogene Daten und Informationen unter den Schutzbereich dieses Rechts fallen: der Name, die Adresse, die professionellen Aktivitäten, die persönlichen Beziehungen, digitale Fingerabdrücke, Kamerabilder, Fotos, Kommunikationsdaten, DNA-Daten, gerichtliche Daten (Verurteilung oder Verdacht), finanzielle Daten und Informationen über Eigentum (vgl. u. a. EGMR, 23. März 1987, *Leander* gg. Schweden, Rn. 47-48; Große Kammer, 4. Dezember 2008, *S. und Marper* gg. Vereinigtes Königreich, Rn. 66-68; 17. Dezember 2009, *B.B.* gg. Frankreich, Rn. 57; 10. Februar 2011, *Dimitrov-Kazakov* gg. Bulgarien, Rn. 29-31; 18. Oktober 2011, *Khelili* gg. Schweiz, Rn. 55-57; 9. Oktober 2012, *Alkaya* gg. Türkei, Rn. 29; 18. April 2013, *M.K.* gg. Frankreich, Rn. 26; 18. September 2014, *Brunet* gg. Frankreich, Rn. 31).

B.12. Die durch Artikel 22 der Verfassung und Artikel 8 der Europäischen Menschenrechtskonvention gewährleisteten Rechte werden jedoch nicht absolut gewährleistet.

Sie schließen einen staatlichen Eingriff in das Recht auf Achtung des Privatlebens nicht aus, sondern schreiben vor, dass ein solcher Eingriff durch eine hinreichend genaue Gesetzesbestimmung erlaubt wird und dass dieser einem zwingenden gesellschaftlichen Bedürfnis in einer demokratischen Gesellschaft sowie dem damit verfolgten gesetzlichen Ziel entspricht. Die Bestimmungen beinhalten für den Staat außerdem in positiver Hinsicht die Verpflichtung zum Ergreifen von Maßnahmen, die eine tatsächliche Achtung des Privatlebens sicherstellen, und zwar auch im Rahmen der Sphäre der gegenseitigen Beziehungen zwischen Einzelpersonen (vgl. EGMR, 27. Oktober 1994, *Kroon u. a.* gg. Niederlande, Rn. 31; Große Kammer, 12. Oktober 2013, *Söderman* gg. Schweden, Rn. 78).

B.13.1. Indem Artikel 22 der Verfassung dem zuständigen Gesetzgeber die Befugnis zur Festlegung vorbehält, in welchen Fällen und unter welchen Bedingungen ein Eingriff in das Recht auf Achtung des Privatlebens erfolgen darf, gewährleistet er jedem Bürger, dass ein Eingriff in dieses Recht ausschließlich nach Regeln stattfinden darf, die durch eine demokratisch gewählte beratende Versammlung angenommen wurden.

Eine Übertragung auf eine andere Gewalt widerspricht ebenfalls nicht dem Gesetzmäßigkeitsgrundsatz, soweit die Ermächtigung hinreichend präzise umschrieben ist und sich auf die Umsetzung von Maßnahmen bezieht, deren wesentliche Elemente vorher durch den Gesetzgeber festgelegt wurden.

B.13.2. Neben dem formellen Gesetzmäßigkeitsgrundsatz ergibt sich aus Artikel 22 der Verfassung ebenso die Verpflichtung, dass der Eingriff in das Recht auf Achtung des Privatlebens durch eine eindeutige und hinreichend genaue Wortwahl formuliert wird, die es ermöglicht, die Fälle vorherzusehen, in denen der Gesetzgeber einen solchen Eingriff in das Recht auf Achtung des Privatlebens erlaubt.

Genauso beinhaltet das Erfordernis der Vorhersehbarkeit, welches das Gesetz erfüllen muss, damit es im Einklang mit Artikel 8 der Europäischen Menschenrechtskonvention steht, dass die entsprechende Formulierung hinreichend genau ist, sodass jede Person - gegebenenfalls nach angemessener Beratung - unter Zugrundelegung der jeweiligen Umstände in hinreichendem Maße die Folgen einer bestimmten Handlung vorhersehen kann (vgl. EGMR, Große Kammer, 4. Mai 2000, *Rotaru* gg. Rumänien, Rn. 55; Große Kammer, 17. Februar 2004, *Maestri* gg. Italien, Rn. 30). Die Gesetzgebung muss jede Person hinreichend auf die Umstände und Bedingungen hinweisen, die von den Behörden zu beachten sind bei Maßnahmen, die in die von der Konvention gewährleisteten Rechte eingreifen (vgl. EGMR, Große Kammer, 12. Juni 2014 *Fernández Martínez* gg. Spanien, Rn. 117).

Insbesondere dann, wenn das Auftreten des Staates geheimen Charakter hat, muss das Gesetz hinreichenden Schutz vor willkürlichen Eingriffen in das Recht auf Achtung des Privatlebens bieten, nämlich indem die Ermessensbefugnis der betreffenden Behörden hinreichend präzise umgrenzt wird und durch Sicherstellung von Verfahren, die eine effektive gerichtliche Kontrolle erlauben (EGMR, Große Kammer, 4. Mai 2000, *Rotaru* gg. Rumänien, Rn. 55; 6. Juni 2006, *Segerstedt-Wiberg* gg. Schweden, Rn. 76; 4. Juli 2006, *Lupsa* gg. Rumänien, Rn. 34).

B.13.3. Aus Artikel 8 der Europäischen Menschenrechtskonvention und Artikel 22 der Verfassung ergibt sich dementsprechend, dass hinreichend genau festgelegt werden muss, unter welchen Umständen eine Verarbeitung von personenbezogenen Daten erlaubt ist (EGMR, Große Kammer, 4. Mai 2000, *Rotaru* gg. Rumänien, Rn. 57; Große Kammer, 12. Januar 2010, *S. und Marper* gg. Vereinigtes Königreich, Rn. 99).

Der geforderte Genauigkeitsgrad für das betreffende Gesetz - das nicht jeden erdenklichen Fall regeln kann - hängt, laut dem Europäischen Gerichtshof für Menschenrechte, u. a. vom zu regelnden Bereich und von der Anzahl und der Eigenschaft der Personen, an die sich das Gesetz richtet, ab (EGMR, Große Kammer, 12. Januar 2010, *S. und Marper* gg. Vereinigtes Königreich, Rn. 95 und 96). So hat der Europäische Gerichtshof für Menschenrechte entschieden, dass das Erfordernis der Vorhersehbarkeit in Bereichen der nationalen Sicherheit nicht die gleiche Tragweite haben kann wie in anderen Bereichen (vgl. EGMR, 26. März 1987, *Leander* gg. Schweden, Rn. 51; 4. Juli 2006, *Lupsa* gg. Rumänien, Rn. 33).

B.14.1. Ein staatlicher Eingriff in das Recht auf Achtung des Privatlebens muss nicht nur eine hinreichend bestimmte Gesetzesbestimmung zur Grundlage haben, sondern auch einem zwingenden gesellschaftlichen Bedürfnis in einer demokratischen Gesellschaft entsprechen und im Verhältnis zum damit verfolgten gesetzlichen Ziel stehen.

Der Gesetzgeber verfügt in dem Zusammenhang über einen Ermessensspielraum. Dieser Ermessensspielraum ist gleichwohl nicht grenzenlos: Damit eine gesetzliche Regelung sich mit dem Recht auf Achtung des Privatlebens vereinbaren lässt, ist es erforderlich, dass der Gesetzgeber ein gerechtes Gleichgewicht zwischen allen betroffenen Rechten und Interessen schafft.

B.14.2. Bei der Beurteilung dieses Gleichgewichts berücksichtigt der Europäische Gerichtshof für Menschenrechte u. a. die Bestimmungen des Übereinkommens des Europarats vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (nachfolgend: Übereinkommen Nr. 108) (vgl. EGMR, 25. Februar 1997, *Z* gg. Finnland, Rn. 95; Große Kammer, 12. Januar 2010, *S. und Marper* gg. Vereinigtes Königreich, Rn. 103).

Dieses Übereinkommen beinhaltet u. a. die Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten: Rechtmäßigkeit, Ordnungsmäßigkeit, Transparenz, Zweckbindung, Verhältnismäßigkeit, Richtigkeit, Speicherbegrenzung, Integrität, Vertraulichkeit und Rechenschaftspflicht.

Hier ist bei der entsprechenden Auslegung insbesondere der Inhalt der Empfehlung Nr. (2010)13 zu beachten.

B.14.3. Ein Eingriff in das Recht auf Achtung des Privatlebens durch Verarbeitung von personenbezogenen Daten, hier durch Zugang seitens öffentlicher Behörden zu bestimmten personenbezogenen Daten und deren Nutzung mithilfe besonderer Techniken (EGMR, 23. März 1987, *Leander* gg. Schweden, Rn. 48; Große Kammer, 4. Mai 2000, *Rotaru* gg. Rumänien, Rn. 46; EuGH, Große Kammer, 8. April 2014, C-293/12, *Digital Rights Ireland Ltd*, und C-594/12, *Kärntner Landesregierung u. a.*), muss deshalb eine angemessene Rechtfertigungsgrundlage haben und den vom Gesetzgeber verfolgten Zielen entsprechen.

B.14.4. In Rahmen der Verhältnismäßigkeit berücksichtigen der Europäische Gerichtshof für Menschenrechte und der Gerichtshof der Europäischen Union das etwaige Vorhandensein der in B.13.2 erwähnten materiellen und prozessualen Garantien in der einschlägigen Regelung.

Bei der Beurteilung der Verhältnismäßigkeit von Maßnahmen in Bezug auf die Verarbeitung personenbezogener Daten sind mithin u. a. deren automatischer Charakter, die verwendeten Techniken, der Genauigkeitsgrad, die Relevanz, der gegebenenfalls außergewöhnliche Charakter der zu verarbeitenden Daten, das etwaige Vorhandensein von Maßnahmen zur Begrenzung der Datenspeicherfrist, das etwaige Vorhandensein eines unabhängigen Überwachungssystems, mit dem geprüft werden kann, ob eine Datenspeicherung weiterhin erforderlich ist, das etwaige Vorhandensein von ausreichenden Kontrollrechten und Rechtsbehelfen für die betroffenen Personen, das etwaige Vorhandensein von Garantien zur Vermeidung einer Stigmatisierung der Personen, deren Daten verarbeitet werden, der unterscheidende Charakter der Regelung und das etwaige Vorhandensein von Garantien zur Vermeidung einer falschen Nutzung und von Missbrauch der verarbeiteten personenbezogenen Daten durch öffentliche Behörden zu berücksichtigen (vgl. EGMR, Große Kammer, 4. Mai 2000, *Rotaru* gg. Rumänien, Rn. 59; Entscheidung, 29. Juni 2006, *Weber und Saravia* gg. Deutschland, Rn. 135; 28. April 2009, *K.H. u. a.* gg. Slowakei, Rn. 60-69; Große Kammer, 12. Januar 2010, *S. und Marper* gg. Vereinigtes Königreich, Rn. 101-103, 119, 122 und 124; 18. April 2013, *M.K.* gg. Frankreich, Rn. 37 und 42-44; 18. September 2014, *Brunet* gg. Frankreich, Rn. 35-37; 12. Januar 2016, *Szabó und Vissy* gg. Ungarn, Rn. 68; EuGH, Große Kammer, 8. April 2014, C-293/12, *Digital Rights Ireland Ltd*, und C-594/12, *Kärntner Landesregierung u. a.*, Rn. 56-66).

B.15.1. Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union haben, hinsichtlich der Verarbeitung personenbezogener Daten, eine Tragweite, die der von Artikel 8 der Europäischen Menschenrechtskonvention (vgl. EuGH, Große Kammer, 9. November 2010, C-92/09 und C-93/09, *Volker und Markus Schecke GbR u. a.*) und Artikel 22 der Verfassung entspricht. Gleiches gilt für Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte.

B.15.2. Die Vereinbarkeit von Rechtsnormen mit Gesetzeskraft mit den Artikeln 7 und 8 der Charta der Grundrechte der Europäischen Union in Verbindung mit analogen Verfassungsbestimmungen oder den Artikeln 10 und 11 der Verfassung kann vom Gerichtshof lediglich geprüft werden, soweit die beanstandeten Bestimmungen das Recht der Union umsetzen (EuGH, Große Kammer, 26. Januar 2013, C-617/10, *Åklagaren*, Rn. 17 ff.).

In diesem Fall sind Richtlinie 95/46/EG und die Datenschutz-Grundverordnung zu beachten.

B.15.3. Da sich die beanstandeten Bestimmungen auf die Verarbeitung personenbezogener Daten beziehen, die in den Anwendungsbereich dieser Rechtsakte der Union fallen, werden die Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union in Verbindung mit analogen Verfassungsbestimmungen oder den Artikeln 10 und 11 der Verfassung gelesen.

Zum einzigen Klagegrund

B.16. Die Einwände der antragstellenden Partei beziehen sich in erste Linie auf die Vereinbarkeit von verschiedenen Aspekten des « Push »-Systems und des vorausgesetzten « Data-Mining » mit dem Recht auf Achtung des Privatlebens.

Zur Vorhersehbarkeit des Gesetzes

B.17. Die antragstellende Partei fordert, dass die Artikel 2, 3 und 4 des beanstandeten Gesetzes für nichtig erklärt werden, weil der Eingriff in das Recht auf Achtung des Privatlebens mit den in B.9 genannten Bestimmungen nicht vereinbar sei, da es keine oder eine unzureichend bestimmte gesetzliche Grundlage für den seitens des Gesetzgebers beabsichtigten Eingriff gebe und die Artikel 3 und 4 nicht hinreichend genau seien.

B.18. Jeder Person muss hinreichend genau bekannt sein, in welchen Fällen und unter welchen Bedingungen ein Eingriff in ihr Privatleben, insbesondere durch die automatische Verarbeitung personenbezogener Daten, gestattet ist. Deshalb muss es jeder Person möglich sein, einen hinreichend deutlichen Einblick in die zu verarbeitenden Daten, in die von der Verarbeitung betroffenen Personen sowie die Bedingungen und die Ziele der Verarbeitung zu haben.

Unter Hinweis auf Artikel 5 *Buchst.* b und 9 Absatz 2 des Übereinkommens Nr. 108 und des Grundsatzes 3.4 der Empfehlung (2010)13 gilt dieses Erfordernis umso mehr, wenn personenbezogene Daten durch öffentliche Behörden für andere Zwecke weiterverarbeitet werden als für diejenigen, für welche sie ursprünglich erfasst wurden.

B.19. Der Gesetzgeber hat im beanstandeten Artikel 2 bestimmt, dass Verbrauchs- und Adressdaten durch die Verteilungsunternehmen und Verteilernetzbetreiber auf Grundlage der Überschreitung einer Abweichungsquote im Verhältnis zum durchschnittlichen Verbrauch einer bestimmten Haushaltszusammensetzung zu erfassen und an die ZDSS zu übermitteln sind, dass diese Daten durch die ZDSS gefiltert und mit anderen Daten abgeglichen werden, um festzustellen, ob die betroffene Person als Anspruchsberechtigter von Sozialleistungen bekannt ist, und dass sie schließlich an die OESSs und die Sozialinspektoren weitergeleitet werden, sodass die Letztgenannten auf Grundlage der empfangenen Daten in Kombination mit im Netzwerk verfügbaren Daten, so wie sie im Gesetz vom 15. Januar 1990 über die Errichtung und Organisation einer Zentralen Datenbank der sozialen Sicherheit erwähnt sind (nachfolgend: ZDSS-Gesetz), nach Ermächtigung seitens des Sektoriellen Ausschusses der sozialen Sicherheit und der Gesundheit, überprüfen können, ob eine Sozialleistung aufgrund einer fiktiven Adresse gewährt wird. Der Gesetzgeber hat im beanstandeten Artikel 4 eindeutig festgelegt, dass die Verbrauchsdaten bloß ein zusätzliches und kein determinierendes Element beim Nachweis eines Sozialbetrugs seitens eines Anspruchsberechtigten sein können.

Der Gesetzgeber hat im beanstandeten Artikel 3 die Möglichkeit für OESSs geschaffen, Daten zu aggregieren, um Analysen dieser Daten durchzuführen, damit so mehr gezielte Kontrollen auf der Grundlage von Risikoindikatoren in Bezug auf sozialen Wohnsitzbetrug vorgenommen werden können.

Artikel 104 des Programmgesetzes (I) vom 29. März 2012 sieht außerdem vor, dass die Bestimmungen des Datenschutzgesetzes anwendbar bleiben, sodass die allgemeinen Bedingungen für die Verarbeitung personenbezogener Daten des Artikels 4 dieses Gesetzes auch im Rahmen des vorliegend beanstandeten Eingriffs gelten.

B.20. Aus dem Vorgenannten, insbesondere unter Berücksichtigung der in B.4 erwähnten parlamentarischen Vorbereitung, ergibt sich, dass der Eingriff eine gesetzliche Grundlage hat, sodass jede Person auf hinreichend genaue Weise die Umstände und die Bedingungen hinsichtlich der Verarbeitung ihrer personenbezogenen Daten erfahren kann. Der Eingriff in das Recht auf Achtung des Privatlebens erfüllt daher die in B.13.2 genannten Anforderungen.

B.21. Unter Berücksichtigung sowohl der Wortwahl des beanstandeten Artikels 3, insbesondere der Bezugnahme auf « verschlüsselte » und « entschlüsselte » Daten, als auch der in B.7.2.2 genannten parlamentarischen Vorbereitung und des sich daraus ergebenden Willens, sich an der Regelung für die Verarbeitung personenbezogener Daten durch den FÖD Finanzen zu orientieren, stellt der Verweis auf Artikel 101 in den Paragraphen 2 und 3 dieses Artikels offensichtlich ein materielles Versehen dar.

In Artikel 101/1 § § 2 und 3 des Programmgesetzes (I) vom 29. März 2012, eingefügt durch den beanstandeten Artikel 3, sind die Worte « im Rahmen von Artikel 101 § 1 » bzw. « in Artikel 101 § 1 erwähnten » für nichtig zu erklären.

Zum Gesetzmäßigkeitsgrundsatz

Die Aufbewahrungsfristen für die Daten

B.22. Die antragstellende Partei trägt vor, dass der Gesetzgeber in Bezug auf den durch die beanstandeten Artikel 2 und 3 bewirkten Eingriff nicht alle Bedingungen, unter denen ein Eingriff in das Recht auf Achtung des Privatlebens erfolgen dürfe, geregelt habe, da die genaue Aufbewahrungsfrist durch den Sektoriellen Ausschuss der sozialen Sicherheit und der Gesundheit bestimmt werde.

B.23. Artikel 4 § 1 Nr. 4 und 5 des Datenschutzgesetzes bestimmt, dass die personenbezogenen Daten nicht länger aufbewahrt werden dürfen, als es für die Umsetzung des Zwecks erforderlich ist, und dass sie gegebenenfalls zu berichtigen oder zu löschen sind. Unter Berücksichtigung der Tatsache, dass der Gesetzgeber nicht für alle spezifischen Fälle gesonderte und präzise Regeln festlegen kann, konnte er die Anforderungen zur Aufbewahrung personenbezogener Daten und zur Aufbewahrungsfrist in allgemeiner Form regeln.

Aus dem Vorgenannten ergibt sich, dass der Gesetzgeber die wesentlichen Aspekte zur Aufbewahrungsfrist geregelt hat.

Der in B.22 geltend gemachte Einwand ist unbegründet.

Zum Verhältnismäßigkeitsgrundsatz

Das « Push »-System

B.24. Die antragstellende Partei fordert, dass der beanstandete Artikel 2 für nichtig erklärt wird, weil das darin vorgesehene « Push »-System weiter reiche, als es für die Bekämpfung von sozialem Wohnsitzbetrug erforderlich sei, und die Garantien hinsichtlich der Aufbewahrungsfristen, der Intervention seitens des Sektoriellen Ausschusses der sozialen Sicherheit und der Gesundheit, der Kontrollrechte der betroffenen Personen, des Verfahrens und der Sicherheit fehlten oder unzureichend seien.

B.25. Angesichts der Tatsache, dass das « Push »-System wegen des Umfangs und der Technik der Verarbeitung personenbezogener Daten einen schwerwiegenden Eingriff in das Privatleben darstellt, muss der Eingriff nicht nur eine gesetzliche Grundlage haben, sondern auch die in B.14 genannten Anforderungen erfüllen.

B.26. Wir bereits in B.2 erwähnt wurde, beabsichtigte der Gesetzgeber den Sozialbetrug, der eng mit der Nutzung einer fiktiven Adresse verbunden ist, effektiver und effizienter zu bekämpfen.

Somit verfolgte der Gesetzgeber mit der beanstandeten Maßnahme einen legitimen Zweck.

B.27. Der Gesetzgeber muss den Zweck auch durch eine geeignete Maßnahme verfolgen.

B.28. Der Gesetzgeber konnte redlicherweise zu dem Schluss gelangen, dass das « Push »-System zur Erreichung des verfolgten Zwecks geeignet ist, da es, ohne dass *a priori* ein Betrugsverdacht zulasten eines spezifischen Anspruchsberechtigten besteht, erlaubt, Verbrauchsdaten auf Grundlage eines abweichenden Verbrauchs als autonomes Signal für einen möglichen Wohnsitzbetrug zu benutzen, was die Möglichkeit bietet, die Nutzung von potenziellen fiktiven Adressen mit einer beschränkten Personalkapazität gleichwohl in höherem Maße zu ermitteln und anschließend auch gezielte Kontrollen vorzunehmen.

B.29. Hinsichtlich der Erforderlichkeit des Eingriffs in das Recht auf Achtung des Privatlebens bei der Verarbeitung personenbezogener Daten ist zu prüfen, wie sich die beanstandete Regelung unter Berücksichtigung der bestehenden Garantien auf das Privatleben auswirkt und ob die Regelung die in B.14 genannten Garantien unverhältnismäßig beschneidet.

B.30.1. Die Behörden, Dienste, Einrichtungen oder Personen, die personenbezogene Daten über das im beanstandeten Gesetz vorgesehene System auswählen, übermitteln oder empfangen, müssen die anwendbaren Bestimmungen des Datenschutzgesetzes beachten.

B.30.2. In dem Zusammenhang hat sich der Gesetzgeber mit dem Datenschutzgesetz für eine allgemeine gesetzliche Regelung entschieden, die sowohl für den öffentlichen als auch den privaten Sektor gilt (*Parl. Dok.*, Kammer, 1990-1991, Nr. 1610/1, S. 3), wobei trotzdem die Besonderheiten bestimmter Sektoren und der Ausgleich vieler Interessen berücksichtigt werden. Aus diesem Grunde hat der Gesetzgeber in Artikel 104 des Programmgesetzes (I) vom 29. März 2012 die Anwendbarkeit des Datenschutzgesetzes für das « Push »-System ausdrücklich bestätigt.

B.30.3. Das Datenschutzgesetz beinhaltet die Regeln, die für den Schutz des Rechts auf Achtung des Privatlebens wesentlich sind: u. a. individuelle Garantien (Artikel 4) bei der Speicherung sensibler Daten (Artikel 6 bis 8); Auskunfts- und Berichtigungsrecht (Artikel 10 und 12); Vertraulichkeit und Sicherheit (Artikel 16 § 4); Öffentlichkeit der Verarbeitungen und umfangreiches Bereitstellen von Informationen an die betroffenen Personen (Artikel 5 und 9); Kontrolle durch eine unabhängige Stelle (Artikel 31) und die Gerichtshöfe und Gerichte (Artikel 14). Den vom Gesetzgeber bestimmten Verantwortlichen für die Verarbeitung treffen mithin verschiedene Pflichten.

B.31. Trotzdem können die Schwere, die Art und der Umfang der vom Gesetzgeber beschlossenen Verarbeitung personenbezogener Daten spezifische oder zusätzliche Garantien erforderlich machen.

Unter Berücksichtigung der Tatsache, dass das beanstandete System darin besteht, Anhaltspunkte für einen Wohnsitzbetrug automatisch - d. h. ohne irgendeinen vorherigen Verdacht der öffentlichen Behörden hinsichtlich eines individuellen Anspruchsberechtigten von Sozialleistungen - zu signalisieren, hat der Gesetzgeber sich dafür entschieden, Verbraucher von Gas, Wasser oder Strom einem « Profiling » zu unterziehen. Es ist dieser Technik inhärent, dass bestimmte Parameter verwendet werden, um in Verbrauchsdaten einer unbestimmten Anzahl von Personen ein bestimmtes Verhalten (Betrug) als Signal zu ermitteln oder um ein solches Verhalten auf Grundlage einer Analyse dieser Massendaten vorherzusagen. Das vorgenannte Signal wird vorliegend durch einen Vergleich des tatsächlichen Wasser-, Gas- und Stromverbrauchs unter einer bestimmten Adresse mit dem durchschnittlichen Verbrauch bei Zugrundelegung der offiziell mitgeteilten Haushaltszusammensetzung unter derselben Adresse herausgefiltert.

Diese Verarbeitungstechnik birgt trotzdem Risiken für das Recht auf Schutz des Privatlebens der betroffenen Personen (siehe das Explanatory Memorandum zur Empfehlung (2010)13, Rn. 50-64), indem u. a. falsche Zusammenhänge zwischen Merkmalen eines bestimmten Verhaltens und Personen hergestellt werden können. Deshalb muss der Gesetzgeber hinreichende Garantien zur Verfügung stellen.

B.32.1. Die antragstellende Partei trägt vor, dass nicht für alle Phasen des « Push »-Systems ein für die Verarbeitung Verantwortlicher bestimmt worden sei.

B.32.2. Vor Anwendung des « Push »-Systems erfolgt die Verarbeitung der Verbrauchs- und Adressdaten im Rahmen der normalen geschäftlichen Tätigkeit durch die Verteilungsunternehmen und Verteilernetzbetreiber entsprechend den Bestimmungen des Datenschutzgesetzes, die dafür einen Verantwortlichen im Sinne von Artikel 1 § 4 des Datenschutzgesetzes zu bestimmen haben.

Was die Auswahl der zu übermittelnden Daten und den eigentlichen Datenstrom im Rahmen des beanstandeten Systems anbelangt, hat der Gesetzgeber sich allerdings dafür entschieden, die ZDSS als für die Verarbeitung Verantwortliche angewiesen.

Folglich hat der Gesetzgeber bestimmt, dass die in B.30 genannten Verpflichtungen im Rahmen des « Push »-Systems in erster Linie die ZDSS treffen, die auch für deren Einhaltung beim Auftragsverarbeiter im Sinne von Artikel 1 § 5 des Datenschutzgesetzes, hier bei den Verteilungsunternehmen und Verteilernetzbetreibern, verantwortlich ist.

Der in B.32.1 geltend gemachte Einwand ist unbegründet.

B.33.1. Die antragstellende Partei bringt vor, dass die Verarbeitung der personenbezogenen Daten mit dem beanstandeten System nicht minimal sei.

B.33.2. Der Gesetzgeber verpflichtet die Verteilungsunternehmen und Verteilernetzbetreiber, im Rahmen des beanstandeten Systems ausschließlich Verbrauchsdaten und damit zusammenhängende Adressen verpflichtend zu erfassen. Die so auferlegte Verpflichtung ist auf zwei Daten beschränkt, die im Rahmen der normalen geschäftlichen Tätigkeit verwendet werden.

Die Verteilungsunternehmen und Verteilernetzbetreiber trifft sodann die Verpflichtung, die Verbrauchs- und Adressdaten an die ZDSS zu übermitteln. Die Übermittlung hat der Gesetzgeber allerdings vom Vorliegen eines bestimmten Schweregrads abhängig gemacht, namentlich einer Abweichung von mehr als 80 Prozent gegenüber dem durchschnittlichen Verbrauch bei Zugrundelegung der offiziell mitgeteilten Haushaltszusammensetzung.

B.33.3. Es ist plausibel, dass es einen Zusammenhang zwischen der Haushaltszusammensetzung und dem Wasser-, Gas- und Stromverbrauch gibt. Folglich kann auf Grundlage der Verbrauchsdaten eine Abweichung gegenüber dem erwarteten durchschnittlichen Verbrauch bei dem offiziell mitgeteilten Familienmodell festgestellt werden. Unter Berücksichtigung der Ausführungen in B.3.5 und des Ermessensspielraums des Gesetzgebers bei komplexen Beurteilungen kann nicht angenommen werden, dass die vorgenannte Schwelle offensichtlich unangemessen ist.

B.34. Diese Schwelle erlaubt es schließlich, die Anzahl von Personen, deren Daten an die ZDSS zu übermitteln sind, auf die Personen zu beschränken, bei denen angemessene Gründe für eine weitere Untersuchung vorliegen, dies gilt erst recht vor dem Hintergrund, dass es um eine wesentliche Abweichung geht.

B.35. Bevor die empfangenen Daten an die Sozialinspektion oder eine OESS übermittelt werden, wird durch die ZDSS über das Personenverzeichnis (Artikel 6 des ZDSS-Gesetzes), nach Abgleich mit Daten aus dem Nationalregister, überprüft, ob sich die Verbrauchs- und Adressdaten auf einen Anspruchsberechtigten von Sozialleistungen beziehen, was dazu führt, dass in der letzten Phase schließlich nur die Daten der Anspruchsberechtigten, bei denen ein sozialer Wohnsitzbetrug vermutet wird, übermittelt werden.

B.36. Aus Vorgenanntem ergibt sich, dass der Gesetzgeber geregelt hat, dass der strukturelle und umfangreiche Datenstrom gefiltert und beschränkt wird auf dasjenige, was bei der Bekämpfung von sozialem Wohnsitzbetrug erforderlich ist.

So haben die öffentlichen Behörden über das « Push »-System lediglich Zugang zu den Daten, die sie für ihre Kontrolle hinsichtlich des gegebenenfalls fiktiven Charakters einer Adresse eines Anspruchsberechtigten von Sozialleistungen benötigen. Die Verarbeitung ist daher nicht mit unverhältnismäßigen Folgen verbunden.

Der in B.33.1 geltend gemachte Einwand ist unbegründet.

B.37.1. Die antragstellende Partei trägt vor, dass die Kontrollrechte der von der Verarbeitung ihrer personenbezogenen Daten betroffenen Personen missachtet würden, indem deren unmittelbare Ausübung ausgeschlossen werde.

B.37.2. Artikel 3 § 5 Nr. 3 des Datenschutzgesetzes bestimmt, dass die Artikel 9, 10 § 1 und 12 desselben Gesetzes (Recht auf Informationen, Auskunft, Berichtigung und Löschung) nicht auf die durch Königlichen Erlass im Hinblick auf die Ausführung ihrer verwaltungspolizeilichen Aufträge bestimmten öffentlichen Behörden anwendbar sind. In Umsetzung von Artikel 3 § 5 Nr. 3 des Datenschutzgesetzes bestimmt Artikel 1 des Königlichen Erlasses vom 11. März 2015:

« § 1. Die Artikel 9, 10 § 1 und 12 des Gesetzes vom 8. Dezember 1992 über den Schutz des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten sind nicht auf Sozialinspektoren und die Beamten der in § 2 genannten öffentlichen Behörden im Rahmen ihrer verwaltungspolizeilichen Aufträge im Sinne von Buch 1, Titel 2 und Titel 4, Kapitel 3 des Sozialstrafgesetzbuches anwendbar.

§ 2. Diese Behörden sind:

- Föderaler Öffentlicher Dienst Beschäftigung, Arbeit und Soziale Konzertierung;
- Landesamt für Arbeitsbeschaffung;
- Landesamt für soziale Sicherheit;
- Landesamt für den Jahresurlaub;
- Landesinstitut für Kranken- und Invalidenversicherung;
- Föderalagentur für Familienbeihilfen;
- Amt für das Sondersozialversicherungssystem;
- Fonds für Arbeitsunfälle;
- Fonds für Berufskrankheiten;
- Kontrollamt der Krankenkassen und Krankenkassenlandesverbände;
- Landespensionsamt;
- Landesinstitut der Sozialversicherungen für Selbständige ».

Daher kann eine betroffene Person ihre Kontrollrechte hinsichtlich der Verarbeitung durch Sozialinspektoren und die OESSs nicht unmittelbar ausüben, soweit die Verarbeitung im Rahmen der Ausübung der verwaltungspolizeilichen Aufgaben erfolgt.

B.37.3. Artikel 13 des Datenschutzgesetzes bestimmt allerdings:

« Personen, die ihre Identität nachweisen, haben das Recht, sich kostenlos an den Ausschuss für den Schutz des Privatlebens zu wenden, um die in den Artikeln 10 und 12 erwähnten Rechte in Bezug auf die in Artikel 3 § § 4, 5, 6 und 7 erwähnten Verarbeitungen personenbezogener Daten auszuüben.

Der König bestimmt nach Stellungnahme des Ausschusses für den Schutz des Privatlebens durch einen im Ministerrat beratenen Erlass die Modalitäten für die Ausübung dieser Rechte.

Der Ausschuss für den Schutz des Privatlebens teilt ausschließlich dem Betreffenden mit, dass die notwendigen Überprüfungen vorgenommen wurden.

Der König bestimmt jedoch nach Stellungnahme des Ausschusses für den Schutz des Privatlebens durch einen im Ministerrat beratenen Erlass, welche Information der Ausschuss der betroffenen Person mitteilen darf, wenn der Antrag der betroffenen Person eine Verarbeitung personenbezogener Daten betrifft, die von Polizeidiensten im Hinblick auf Identitätskontrollen verrichtet wird ».

Eine betroffene Person kann ihre Kontrollrechte mithin über den Datenschutzausschuss ausüben.

B.38.1. Gemäß Artikel 9 Absatz 2 des Übereinkommens Nr. 108 ist eine Abweichung von den in Artikel 8 des Übereinkommens genannten Kontrollrechten zulässig, soweit sie durch ein Gesetz vorgesehen und in einer demokratischen Gesellschaft zum Schutz der Sicherheit des Staates, der öffentlichen Sicherheit, der Währungsinteressen des Staates, zur Bekämpfung von Straftaten, zum Schutz des Betroffenen und zum Schutz der Rechte und Freiheiten Dritter notwendig ist.

B.38.2. Die Effektivität und die Effizienz im Rahmen der Bekämpfung von Betrug - und somit des Schutzes der Währungsinteressen des Staates und der Rechte Dritter in einem Sozialsystem - können es rechtfertigen, dass die Kontrollrechte der betroffenen Personen hinsichtlich der Verarbeitung ihrer personenbezogenen Daten insoweit eingeschränkt werden, sofern sich diese Auskunftseinschränkung im Zusammenhang mit der Verwaltungspolizei nur auf die Daten von Anspruchsberechtigten von Sozialleistungen bezieht und der Ausschluss einer unmittelbaren Auskunft nicht länger dauert, als er für die Untersuchung notwendig ist.

Aus den Ausführungen in B.37 ergibt sich, dass die Nichtanwendbarkeit der Artikel 9, 10 und 12 des Datenschutzgesetzes sowie das in Artikel 13 des Datenschutzgesetzes vorgesehene mittelbare Auskunftsrecht auf die Daten beschränkt sind, die durch die zwölf genannten Behörden und die Sozialinspektoren im Rahmen ihrer Aufträge als Verwaltungspolizei verarbeitet werden. In Bezug auf Daten, die durch diese öffentlichen Behörden und die Sozialinspektoren für andere Aufträge oder Zwecke verarbeitet werden, sind diese verpflichtet, die Artikel 9, 10 und 12 des Datenschutzgesetzes einzuhalten.

Falls der Untersuchungszweck es allerdings nicht mehr erforderlich macht, ist es nicht gerechtfertigt, der betroffenen Person das unmittelbare Auskunfts- und Kontrollrecht in Bezug auf ihre personenbezogenen Daten zu verwehren.

B.38.3. Unter dem Vorbehalt der Ausführungen in B.38.2 letzter Absatz ist der in B.37.1 geltend gemachte Einwand unbegründet.

B.39.1. Die antragstellende Partei bringt vor, dass die Garantien hinsichtlich der Sicherheit und der Vertraulichkeit nicht ausreichend seien.

B.39.2. Artikel 16 § 4 des Datenschutzgesetzes bestimmt, dass der für die Verarbeitung Verantwortliche sowie der Auftragsverarbeiter selbst passende organisatorische und technische Maßnahmen ergreifen müssen, die für den Schutz der personenbezogenen Daten unter Berücksichtigung des Standes der Technik und der Art der zu schützenden Daten und der möglichen Risiken erforderlich sind. Der Gesetzgeber hat ausdrücklich festgelegt, welche Risiken beim Ergreifen dieser Sicherheitsmaßnahmen zu berücksichtigen sind (zufällige Zerstörung von Daten, zufälliger Verlust von Daten, unberechtigte Änderung von Daten usw.).

B.39.3. Neben den Garantien im Datenschutzgesetz hat der Gesetzgeber auch Garantien im ZDSS-Gesetz betreffend das Berufsgeheimnis, die Einstellung eines Sicherheitsberaters und Sicherheitsmaßnahmen (Artikel 22, 23, 24, 25 und 28 des ZDSS-Gesetzes) vorgesehen. Auch in Bezug auf die Sozialinspektion gewährleistet Artikel 58 des Sozialstrafgesetzbuches die Vertraulichkeit der Sozialdaten, mit denen die Sozialinspektion in Berührung kommt. Der Gesetzgeber hat ebenfalls Sanktionen in den Artikeln 213 bis 215 des Sozialstrafgesetzbuches bei Missachtung der Vertraulichkeit von Daten oder bei Unterlassen der erforderlichen Sicherheitsmaßnahmen vorgesehen.

B.39.4. Aus Vorgenanntem ergibt sich, dass der Gesetzgeber Garantien zur Gewährleistung der Sicherheit und der Vertraulichkeit der verarbeiteten personenbezogenen Daten vorgesehen hat.

Der in B.39.1 geltend gemachte Einwand ist unbegründet.

B.40. Die antragstellende Partei macht geltend, dass prozessuale Garantien wie z. B. solche im Gesetz vom 3. August 2012 zur Festlegung von Bestimmungen in Bezug auf die Verarbeitung personenbezogener Daten durch den Föderalen Öffentlichen Dienst Finanzen im Rahmen seiner Aufträge fehlen würden.

B.41. Die Daten, die im Rahmen des "Push"-Systems verarbeitet werden, können durch die öffentlichen Behörden nur als zusätzlicher Hinweis gebraucht werden, um festzustellen, ob ein Anspruchsberechtigter von Sozialleistungen einen Wohnsitzbetrug begangen hat (Artikel 102 des Programmgesetzes (I) vom 29. März 2012 in der Fassung der Änderung durch Artikel 4 des beanstandeten Gesetzes), was einer unmittelbaren nachteiligen Auswirkung zulasten der betroffenen Person vorbeugt. Die zuständigen öffentlichen Behörden müssen schließlich im gegebenen Fall über andere Hinweise verfügen, um eine nachteilige Entscheidung (z. B. Sanktionen im Falle von Betrug) gegenüber einem Anspruchsberechtigten von Sozialleistungen zu treffen. Der Gesetzgeber hat in Artikel 103 des Programmgesetzes (I) vom 29. März 2012 in der Fassung der Änderung durch Artikel 5 des beanstandeten Gesetzes bestimmt, dass die Sozialinspektoren die betroffene Person oder einen Dritten über die Tatsache informieren, dass ihre Verbrauchsdaten im Rahmen einer behördlichen Untersuchung verwendet werden können. Gemäß Artikel 79 des Sozialstrafgesetzbuches haben die betroffenen Personen auch das Recht zur Einsichtnahme in die behördliche Akte.

B.42. Falls schließlich als Ergebnis des « Push »-Systems die « Feststellung » eines Wohnsitzbetruges folgen sollte, kann der betroffene Anspruchsberechtigte von Sozialleistungen alle tatsächlichen und rechtlichen Nachweise erbringen, dass kein Wohnsitzbetrug vorliegt. Die betroffene Person genießt kraft der allgemeinen Grundsätze einer ordnungsgemäßen Verwaltung oder der Regeln im Strafverfahren Garantien in Bezug auf ihre Verteidigungsrechte.

B.43. Artikel 14 des Datenschutzgesetzes schreibt vor, dass der wie im Verfahren für einstweilige Verfügungen tagende Präsident des Gerichts Erster Instanz erkennt über alle Ersuchen in Bezug auf das durch oder aufgrund des Gesetzes gewährte Recht auf Mitteilung personenbezogener Daten und über alle Ersuchen auf Berichtigung, Löschung oder Verbot der Verwendung personenbezogener Daten, die fehlerhaft oder unter Berücksichtigung des Verarbeitungszwecks unvollständig oder nicht sachdienlich sind, deren Speicherung, Mitteilung oder Aufbewahrung verboten ist, gegen deren Verarbeitung die betroffene Person sich widersetzt hat oder die über den erlaubten Zeitraum hinaus aufbewahrt worden sind. Gemäß Artikel 32 § 3 des Datenschutzgesetzes kann der Präsident des Ausschusses für den Schutz des Privatlebens, im gegebenen Fall nach einer Beschwerde seitens einer betroffenen Person, jede Streitsache in Bezug auf die Anwendung dieses Gesetzes und seiner Ausführungsmaßnahmen dem Gericht Erster Instanz vorlegen.

Eine betroffene Person verfügt deshalb über Rechtsbehelfe, die es ihr ermöglichen, den Eingriff in ihr Recht auf Schutz des Privatlebens durch die Verarbeitung personenbezogener Daten dem Richter zwecks Überprüfung vorzulegen.

B.44. Aus Vorgenanntem geht hervor, dass das beanstandete Gesetz hinreichende prozessuale Garantien bietet.

Der in B.40 geltend gemachte Einwand ist unbegründet.

B.45. Die antragstellende Partei trägt vor, dass der Gesetzgeber in einem unzureichenden Umfang spezifische Aufbewahrungsfristen festgelegt habe.

B.46. Gemäß Artikel 4 § 1 Nr. 3, 4 und 5 des Datenschutzgesetzes gilt für jede Phase in Anbetracht des spezifischen Zwecks die Verpflichtung, nicht (mehr) relevante oder fehlerhafte personenbezogene Daten nicht länger zu verarbeiten, sie zu berichtigen bzw. zu löschen und sie jedenfalls nicht länger aufzubewahren, als es für den verfolgten spezifischen Zweck, d. h. hier die Erfassung und die Übermittlung von Verbrauchsdaten an die ZDSS, die Aggregation und die Übermittlung dieser Daten durch die ZDSS an die zuständigen öffentlichen Behörden, erforderlich ist. Für die OESSs und die Sozialinspektoren gilt ebenfalls, dass sie die Daten nicht länger aufbewahren dürfen, als es für die Vornahme der Kontrollen hinsichtlich der Nutzung einer fiktiven Adresse im Rahmen von Leistungsbetrug erforderlich ist, was impliziert, dass sie jedenfalls nicht länger als die für einen Betrug geltende Verjährungsfrist aufbewahrt werden dürfen.

Der in B.45 geltend gemachte Einwand ist unbegründet.

B.47. Die antragstellende Partei bringt außerdem vor, dass der Gesetzgeber sich nicht für die am wenigsten einschneidende Maßnahme im Rahmen der Verschärfung der Bekämpfung von sozialem Wohnsitzbetrug entschieden habe.

B.48. Aus der in B.2 genannten parlamentarischen Vorbereitung ergibt sich, dass der Gesetzgeber zwei Alternativen betreffend die Art der Erlangung von Verbrauchsdaten bei der Bekämpfung von sozialem Wohnsitzbetrug erwogen hat: das « Pull »-System (*Status quo*) und das « Push »-System (neues Instrument).

B.49. Beide Systeme gewähren den öffentlichen Behörden, vor dem Hintergrund der Vornahme von Kontrollen in Bezug auf sozialen Wohnsitzbetrug, im Falle eines vermuteten Betrugs ausschließlich Einblick in die Verbrauchsdaten von Anspruchsberechtigten von Sozialleistungen.

Der wesentliche Unterschied zwischen beiden System besteht darin, auf welche Weise die Behörde zu einem solchen Betrugsverdacht gelangt. Beim beanstandeten System hat der Verdacht seine Grundlage in technologischen Prozessen, bei denen Verbrauchsdaten aller Verbraucher strukturell und automatisch gescreent werden, damit anhand eines Profils Betrugswarnleuchten ausgelöst werden, während beim « Pull »-System keine Daten von Dritten einbezogen werden.

B.50. In Anbetracht der Tatsache, dass die Bekämpfung von sozialem Wohnsitzbetrug einen Dauerkampf darstellt, der ständige Anstrengungen erfordert, und dass das Betrugsverhalten und dessen Bekämpfung mit Änderungen beim Sozialverhalten verbunden sind, insbesondere im Hinblick auf die vorhandenen technischen Hilfsmittel, konnte der Gesetzgeber redlicherweise urteilen, dass der Sozialbetrug effektiver und effizienter im Rahmen des « Push »-Systems bekämpft werden kann.

B.51. Aus den Ausführungen zum « Pull »-System in B.1.3 geht hervor, dass dieses System den Einsatz von außerordentlich viel Personal und Mitteln erforderlich macht, um eine gewisse Schlagkraft bei der Bekämpfung von sozialem Wohnsitzbetrug zu entfalten. Angesichts seines beschränkten Wirkungskreises scheint dieses System nicht in der Lage, die gleiche Anzahl an Anspruchsberechtigten von Sozialleistungen einer Untersuchung zu unterziehen, und folglich auch nicht, die gleiche Anzahl an mutmaßlichen Betrugsfällen wie im Rahmen des beanstandeten « Push »-Systems aufzudecken. Gleiches gilt *mutatis mutandis* auch für die durch die antragstellende Partei genannten Untersuchungsinstrumente wie den Hausbesuch, die Informationssammlung und die Vernehmung (Artikel 24, 26 und 27 des Sozialstrafgesetzbuches). Angesichts der spezifischen und individuellen Beantragung von Daten ist das « Pull »-System auch so beschaffen, dass es eine stigmatisierende Wirkung hinsichtlich der betroffenen Personen - einerseits als Anspruchsberechtigter von Sozialleistungen und andererseits als mutmaßlicher Betrüger - hat und sich somit nachteilig auf das Privatleben auszuwirkt.

B.52. Das « Push »-System verhindert durch die Rolle der ZDSS, dass die Verteilungsunternehmen und Verteilernetzbetreiber davon Kenntnis haben, welche Verbraucher Anspruchsberechtigte von Sozialleistungen sind, wodurch der Eingriff in das Privatleben des Anspruchsberechtigten von Sozialleistungen auf das absolut Notwendige beschränkt wird. Aus den Ausführungen in B.29 bis B.44 ergibt sich auch, dass der Gesetzgeber die notwendigen materiellen und prozessualen Bedingungen und Garantien im Zusammenhang mit dem Eingriff in das Privatleben geregelt hat.

B.53. Aus Vorgenanntem und insbesondere angesichts der Ausführungen in B.1.2 und B.52 und der Unterschiede zwischen den beiden Systemen geht hervor, dass der Gesetzgeber redlicherweise zu dem Schluss gelangen konnte, dass das « Push »-System, wie es durch den beanstandeten Artikel 2 eingeführt wurde, nicht weiter geht, als es für eine effektive und effiziente Ermittlung, Abschreckung und Bekämpfung von sozialem Wohnsitzbetrug erforderlich ist.

Der in B.47 erwähnte Einwand ist unbegründet.

B.54. Der Gerichtshof hat noch zu prüfen, ob das beanstandete « Push »-System, welches, wie in B.3 erläutert, « Profiling » und die Verarbeitungstechnik « Data-Mining » impliziert, gegebenenfalls mit unverhältnismäßigen Folgen einhergeht.

B.55. In Anbetracht des verfolgten Zwecks, u. a. die bis dahin nicht oder sehr schwierig feststellbaren Fälle von mutmaßlichem Wohnsitzbetrug zu ermitteln, und unter Berücksichtigung des abschreckenden Charakters des « Push »-Systems, der Änderungen beim Verhalten von Personen der Zielgruppe und der Unvorhersehbarkeit des Betrugsverhaltens und der Anzahl der Fälle ist es nicht ungerechtfertigt, dass der Gesetzgeber bei der Festlegung der Maßnahme keine allumfassenden und endgültigen Aussagen über die mit dem System verbundenen Erträge und Kosten und mithin über dessen Effizienz treffen kann.

Der in B.54 erwähnte Einwand ist unbegründet.

« Data-Warehouse » und « Data-Mining »

B.56. Die antragstellende Partei fordert, dass Artikel 3 für nichtig erklärt wird, weil die Aggregation und die Analyse der verfügbaren Daten durch die OESSs weitreichender seien, als es für die Bekämpfung von sozialem Wohnsitzbetrug erforderlich sei, und weil Garantien wie das Erfordernis einer Ermächtigung seitens des Sektoriellen Ausschusses der sozialen Sicherheit und der Gesundheit sowie Garantien zur Integrität und Vertraulichkeit fehlten oder unzureichend seien.

B.57. Die Aggregation von Daten, über welche die OESSs und die gegebenenfalls dazugehörige Sozialinspektion verfügen können, sowie die Suche in diesen Daten nach möglichen Zusammenhängen und Indikatoren in Bezug auf das Risiko für die Nutzung einer fiktiven Adresse können redlicherweise als ein geeignetes Mittel zur Verschärfung der Bekämpfung von sozialem Wohnsitzbetrug angesehen werden.

B.58. Entsprechend den Ausführungen in B.30 gelten die Garantien des Datenschutzgesetzes auch im Rahmen einer solchen Verarbeitung, die sich aus dem beanstandeten Artikel 3 ergibt.

B.59. Die antragstellende Partei trägt vor, dass im beanstandeten Artikel 3 keine Ermächtigung seitens eines Sektoriellen Ausschusses der sozialen Sicherheit und der Gesundheit im Hinblick auf die Übermittlung von Daten an die Sozialinspektoren gefordert werde.

B.60. Unter Berücksichtigung der in B.21 erwähnten Nichtigkeit und der auf die OESSs beschränkten Tragweite des beanstandeten Artikels ist der in B.59 erwähnte Einwand unbegründet.

B.61. Die antragstellende Partei macht schließlich geltend, dass der beanstandete Artikel 3 die Integrität und die Vertraulichkeit verletze, weil es keine ausreichenden Garantien gebe.

B.62. Artikel 16 § 4 des Datenschutzgesetzes verpflichtet die OESSs als für die Verarbeitung Verantwortliche, passende organisatorische und technische Maßnahmen zu ergreifen, die für den Schutz der personenbezogenen Daten unter Berücksichtigung des Standes der Technik und der Art der zu schützenden Daten und der möglichen Risiken erforderlich sind. Der Gesetzgeber hat dabei ausdrücklich festgelegt, welche Risiken beim Ergreifen dieser Sicherheitsmaßnahmen zu berücksichtigen sind (zufällige Zerstörung von Daten, zufälliger Verlust von Daten, unberechtigte Änderung von Daten usw.).

Der in B.61 erwähnte Einwand ist unbegründet.

B.63. Aus Vorgenanntem geht hervor, dass Artikel 3 des beanstandeten Gesetzes, auch unter Berücksichtigung des zunächst verschlüsselten Charakters der vorgesehenen Analysen, keine weitreichenderen Eingriffe gestattet, als es für die Verschärfung der Bekämpfung von sozialem Wohnsitzbetrug erforderlich ist. Das Ermitteln der Zusammenhänge und neuer Indikatoren ist außerdem für das Verfolgen von Entwicklungen im Betrugsverhalten und das Aufdecken von möglichen Betrugsfällen erforderlich.

Die in B.56 erwähnten Einwände sind unbegründet.

Aus diesen Gründen:

Der Gerichtshof

- erklärt in den Paragraphen 2 und 3 von Artikel 101/1 des Programmgesetzes (I) vom 29. März 2012 in der Fassung der Einfügung durch Artikel 3 des Gesetzes vom 13. Mai 2016 « zur Abänderung des Programmgesetzes (I) vom 29. März 2012 in Bezug auf die Kontrolle des Missbrauchs fiktiver Adressen durch die Anspruchsberechtigten von Sozialleistungen im Hinblick auf die Einführung der systematischen Übermittlung bestimmter Verbrauchsdaten durch Verteilungsunternehmen und Verteilernetzbetreiber an die ZDSS zur Verbesserung des Data-Mining und Data-Matching im Rahmen der Bekämpfung des Sozialbetrugs » die Worte « im Rahmen von Artikel 101 § 1 » bzw. « in Artikel 101 § 1 erwähnten » für nichtig;

- weist die Klage im Übrigen unter Vorbehalt der Ausführungen in B.38.2 letzter Absatz ab.

Erlassen in niederländischer, französischer und deutscher Sprache, gemäß Artikel 65 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof, am 15. März 2018.

Der Kanzler,
P.-Y. Dutilleux

Der Präsident,
E. De Groot

FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN

[C − 2018/12750]

3 JUNI 2018. — Wet tot wijziging van de wet van 21 december 1998 betreffende de veiligheid bij voetbalwedstrijden

FILIP, Koning der Belgen,

Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

De Kamer van volksvertegenwoordigers heeft aangenomen en Wij bekrachtigen hetgeen volgt :

Artikel 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

Art. 2. In artikel 2 van de wet van 21 december 1998 betreffende de veiligheid bij voetbalwedstrijden, laatstelijk gewijzigd bij de wet van 27 juni 2016, worden de volgende wijzigingen aangebracht:

1° de bepaling onder 1° wordt vervangen als volgt:

"1° voetbalwedstrijd: de variant van het voetbalspel die met twee ploegen van elf spelers op een grasveld of op een veld in synthetisch materiaal wordt gespeeld; deze voetbalwedstrijden situeren zich onder de koepel van een overkoepelende sportbond;";

2° er wordt de bepaling 2°/1 ingevoegd, luidende:

"2°/1. nationale afdeling: alle voetbalwedstrijden die worden gespeeld op andere niveaus dan die gespeeld op provinciaal niveau, met uitzondering van de wedstrijden van een damescategorie of een bepaalde leeftijdscategorie. De eerste afdeling is de hoogste in het klassement, de vijfde de laagste;";

3° de bepaling onder 3° wordt vervangen als volgt:

"3° internationale wedstrijd: de in de bepaling onder 1° bepaalde voetbalwedstrijd waaraan ten minste één niet-Belgische ploeg deelneemt en die deelneemt aan een buitenlands kampioenschap of representatief is voor een vreemde natie. Indien een Belgische club deelneemt, behoort deze tot de nationale afdeling zoals bepaald in de bepaling onder 2°/1;";

4° in de bepaling onder 4° worden de woorden "of iedere andere voetbalwedstrijd zoals hierna vermeld" ingevoegd tussen de woorden "internationale voetbalwedstrijd" en de woorden "geheel of ten dele";

5° in de bepaling onder 7° worden de woorden "voor zover het speelveld grenst aan ten minste een tribune" opgeheven en wordt deze bepaling aangevuld met de woorden "; bij afwezigheid van een buitenomheining doet de binnenomheining dienst als afbakening;";

6° de bepaling onder 9° wordt vervangen als volgt:

"9° perimeter: de ruimte aansluitend bij de buitenomheining van het stadion, of bij gebreke van een buitenomheining, bij de binnenomheining rond het speelveld, waarvan de geografische grenzen vastgesteld worden door de Koning, na raadpleging van de betrokken

SERVICE PUBLIC FEDERAL INTERIEUR

[C − 2018/12750]

3 JUIN 2018. — Loi modifiant la loi du 21 décembre 1998 relative à la sécurité lors des matches de football

PHILIPPE, Roi des Belges,

A tous, présents et à venir, Salut.

La Chambre des représentants a adopté et Nous sanctionnons ce qui suit :

Article 1er. La présente loi règle une matière visée à l'article 74 de la Constitution.

Art. 2. À l'article 2 de la loi du 21 décembre 1998 relative à la sécurité lors des matches de football, modifié en dernier lieu par la loi du 27 juin 2016, les modifications suivantes sont apportées:

1° le 1° est remplacé par ce qui suit:

"1° match de football: la variante du football qui est jouée par deux équipes de onze joueurs sur du gazon ou un revêtement synthétique; ces matches de football se déroulent sous l'égide d'une fédération sportive coordinatrice;";

2° il est inséré un 2°/1 rédigé comme suit:

"2°/1. division nationale: tous les matches de football joués à un autre niveau que le niveau provincial, à l'exclusion des matches destinés à une catégorie féminine ou à une catégorie d'âge déterminée. La première division est la plus élevée du classement, la cinquième est la plus basse;";

3° le 3° est remplacé par ce qui suit:

"3° match international: le match de football défini au 1° auquel participe au moins une équipe d'une nationalité autre que belge et qui participe à un championnat étranger ou est représentative d'une nation étrangère. Si un club belge participe, il relèvera de la division nationale visée au 2°/1;";

4° dans le 4°, les mots ", ou tout autre match de football tel que décrit ci-après" sont insérés entre les mots "ou un match international de football" et les mots ", à son initiative";

5° dans le 7°, les mots ", pour autant que le terrain de jeu soit jouxté d'au moins une tribune" sont abrogés et la disposition est complétée par les mots "; en l'absence de clôture extérieure, la clôture intérieure servira à le délimiter;";

6° le 9° est remplacé par ce qui suit:

"9° périmètre: espace jouxtant la clôture extérieure du stade ou, à défaut de clôture extérieure, la clôture intérieure entourant le terrain de jeu, dont les limites géographiques sont dans les deux cas fixées par le Roi, après consultation du bourgmestre, des services de police et de