Geschäftsverzeichnisnr. 6552
Entscheid Nr. 29/2018 vom 15. März 2018

E N T S C H E I D

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).

Der Ministerrat, unterstützt und vertreten durch RÄin V. Pertry, in Brüssel zugelassen, hat einen Schriftsatz eingereicht, die klagende Partei hat einen Erwiderungsschriftsatz eingereicht, und der Ministerrat hat auch einen Gegenerwiderungsschriftsatz eingereicht.

Durch Anordnung vom 26. September 2017 hat der Gerichtshof nach Anhörung der referierenden Richter A. Alen und J.-P. Moerman beschlossen, dass die Rechtssache verhandlungsreif ist, dass keine Sitzung abgehalten wird, außer wenn eine Partei innerhalb von sieben Tagen nach Erhalt der Notifizierung dieser Anordnung einen Antrag auf Anhörung eingereicht hat, und dass vorbehaltlich eines solchen Antrags die Verhandlung am 18. Oktober 2017 geschlossen und die Rechtssache zur Beratung gestellt wird.

Da keine Sitzung beantragt wurde, wurde die Rechtssache am 18. Oktober 2017 zur Beratung gestellt.

Die Vorschriften des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof, die sich auf das Verfahren und den Sprachengebrauch beziehen, wurden zur Anwendung gebracht.

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, 26. 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, 4. Dezember 2008, *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, 4. Dezember 2008, *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,

26. 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, 4. Dezember 2008, *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, Der Präsident,

P.-Y. Dutilleux E. De Groot