Geschäftsverzeichnisnrn. 7125, 7150, 7202, 7203 und 7211
Entscheid Nr. 2/2021 vom 14. Januar 2021

E N T S C H E I D

In Sachen: Klagen auf Nichtigerklärung von Artikel 27 des Gesetzes vom 25. November 2018 « zur Festlegung verschiedener Bestimmungen in Bezug auf das Nationalregister und die Bevölkerungsregister », erhoben von der « Parti Libertarien » und Baudoin Collard, von Matthias Dobbelaere-Welvaert und anderen, von der VoG « Liga voor Mensenrechten », von der VoG « Ligue des droits humains » und von Siham Najmi und John Pitseys in ihrer Eigenschaft als gesetzliche Vertreter ihres Sohnes Samuel Pitseys Najmi.

Der Verfassungsgerichtshof,

zusammengesetzt aus den Präsidenten F. Daoût und L. Lavrysen, und den Richtern T. Merckx-Van Goey, P. Nihoul, T. Giet, R. Leysen, J. Moerman, M. Pâques, Y. Kherbache und T. Detienne, unter Assistenz des Kanzlers P.-Y. Dutilleux, unter dem Vorsitz des Präsidenten F. Daoût,

erlässt nach Beratung folgenden Entscheid:

*

* *

I. *Gegenstand der Klagen und Verfahren*

a. Mit einer Klageschrift, die dem Gerichtshof mit am 11. Februar 2019 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 12. Februar 2019 in der Kanzlei eingegangen ist, erhoben Klage auf Nichtigerklärung von Artikel 27 des Gesetzes vom 25. November 2018 « zur Festlegung verschiedener Bestimmungen in Bezug auf das Nationalregister und die Bevölkerungsregister » (veröffentlicht im *Belgischen Staatsblatt* vom 13. Dezember 2018): die « Parti Libertarien » und Baudoin Collard, unterstützt und vertreten durch RA R. Fonteyn, in Brüssel zugelassen.

b. Mit einer Klageschrift, die dem Gerichtshof mit am 22. März 2019 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 25. März 2019 in der Kanzlei eingegangen ist, erhoben Klage auf Nichtigerklärung derselben Gesetzesbestimmung: Matthias Dobbelaere-Welvaert, Bert Cattoor, Johan Gielen und Antoon Lowette, unterstützt und vertreten durch RA G. Lenssens, in Brüssel zugelassen.

c. Mit einer Klageschrift, die dem Gerichtshof mit am 12. Juni 2019 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 13. Juni 2019 in der Kanzlei eingegangen ist, erhob die VoG « Liga voor Mensenrechten », unterstützt und vertreten durch RA D. Pattyn, in Ostflandern zugelassen, und RA R. Fonteyn, Klage auf Nichtigerklärung derselben Gesetzesbestimmung.

d. Mit einer Klageschrift, die dem Gerichtshof mit am 12. Juni 2019 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 13. Juni 2019 in der Kanzlei eingegangen ist, erhob die VoG « Ligue des droits humains », unterstützt und vertreten durch RA D. Pattyn und RA R. Fonteyn, Klage auf Nichtigerklärung derselben Gesetzesbestimmung.

e. Mit einer Klageschrift, die dem Gerichtshof mit am 12. Juni 2019 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 17. Juni 2019 in der Kanzlei eingegangen ist, erhoben Klage auf Nichtigerklärung derselben Gesetzesbestimmung: Siham Najmi und John Pitseys in ihrer Eigenschaft als gesetzliche Vertreter ihres Sohnes Samuel Pitseys Najmi, unterstützt und vertreten durch RA R. Fonteyn.

Diese unter den Nummern 7125, 7150, 7202, 7203 und 7211 ins Geschäftsverzeichnis des Gerichtshofes eingetragenen Rechtssachen wurden verbunden.

Schriftsätze wurden eingereicht von

- der « Parti Libertarien » und Baudoin Collard, unterstützt und vertreten durch RA R. Fonteyn (intervenierende Parteien in der Rechtssache Nr. 7150),

- der VoG « Ligue des droits humains », unterstützt und vertreten durch RA R. Fonteyn (intervenierende Partei in der Rechtssache Nr. 7150),

- dem Ministerrat, unterstützt und vertreten durch RA P. Goffaux, RA D. D'Hooghe und RÄin M. Van Den Langenbergh, in Brüssel zugelassen (in allen Rechtssachen).

Die klagenden Parteien haben Erwiderungsschriftsätze eingereicht.

Der Ministerrat hat auch Gegenerwiderungsschriftsätze eingereicht.

Durch Anordnung vom 23. September 2020 hat der Gerichtshof nach Anhörung der referierenden Richter M. Pâques und Y. Kherbache beschlossen, dass die Rechtssachen verhandlungsreif sind, 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 7. Oktober 2020 geschlossen und die Rechtssachen zur Beratung gestellt werden.

Infolge der Anträge der klagenden Parteien in den Rechtssachen Nrn. 7150 und 7202 auf Anhörung hat der Gerichtshof durch Anordnung vom 7. Oktober 2020 den Sitzungstermin auf den 12. November 2020 anberaumt.

Auf der öffentlichen Sitzung vom 12. November 2020

- erschienen

. RA D. Pattyn *loco* RA R. Fonteyn, für die klagenden Parteien in den Rechtssachen Nrn. 7125 und 7211 und für die intervenierenden Parteien in der Rechtssache Nr. 7150,

. RA D. Pattyn, für die klagenden Parteien in den Rechtssachen Nrn. 7202 und 7203,

. RA G. Lenssens, für die klagenden Parteien in der Rechtssache Nr. 7150,

. RA P. Goffaux und RÄin M. Van Den Langenbergh, für den Ministerrat,

- haben die referierenden Richter M. Pâques und Y. Kherbache Bericht erstattet,

- wurden die vorgenannten Rechtsanwälte angehört,

- wurden die Rechtssachen 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*

(...)

In Bezug auf die angefochtene Bestimmung und deren Kontext

B.1.1. Artikel 27 des Gesetzes vom 25. November 2018 « zur Festlegung verschiedener Bestimmungen in Bezug auf das Nationalregister und die Bevölkerungsregister » (nachstehend: Gesetz vom 25. November 2018) bestimmt:

« Artikel 6 [des Gesetzes vom 19. Juli 1991 über die Bevölkerungsregister, die Personalausweise, die Ausländerkarten und die Aufenthaltsdokumente und zur Abänderung des Gesetzes vom 8. August 1983 zur Organisation eines Nationalregisters der natürlichen Personen], zuletzt abgeändert durch das Gesetz vom 9. November 2015, wird wie folgt abgeändert:

1. Paragraph 2 Absatz 3 wird durch eine Nr. 8 mit folgendem Wortlaut ergänzt:

‘ 8. das digitale Bild der Fingerabdrücke des Zeigefingers der linken und der rechten Hand des Inhabers oder - bei Invalidität oder Untauglichkeit - eines anderen Fingers jeder Hand; der König bestimmt nach Stellungnahme der Datenschutzbehörde durch einen im Ministerrat beratenen Erlass die Bedingungen und Modalitäten für die Erfassung des digitalen Bildes der Fingerabdrücke. ’

2. Paragraph 2 wird durch folgende Absätze ergänzt:

‘ Die in Absatz 3 Nr. 8 erwähnte Information darf nur während der Zeit, die für die Herstellung und Ausstellung des Personalausweises erforderlich ist, und in jedem Fall während eines Zeitraums von höchstens drei Monaten aufbewahrt werden, wobei die Daten nach Ablauf dieser Frist von drei Monaten unbedingt vernichtet und gelöscht werden müssen.

Ist beziehungsweise sind ermächtigt, die in Absatz 3 Nr. 8 erwähnte Information zu lesen:

- das Gemeindepersonal, das mit der Ausstellung der Personalausweise beauftragt ist,

- die Polizeidienste, sofern dies für die Erfüllung ihrer verwaltungs- und gerichtspolizeilichen gesetzlichen Aufträge im Rahmen der Betrugsbekämpfung erforderlich ist, insbesondere der Bekämpfung des Menschenhandels und -schmuggels, des Betrugs und der Untreue, der Geldwäsche, des Terrorismus, der Fälschung und des Gebrauchs gefälschter Urkunden, der Namensanmaßung und des Gebrauchs eines falschen Namens, der Verstöße gegen das Gesetz vom 15. Dezember 1980 über die Einreise ins Staatsgebiet, den Aufenthalt, die Niederlassung und das Entfernen von Ausländern und der Behinderungen der verwaltungspolizeilichen Aufträge,

- das Personal, das mit der Grenzkontrolle beauftragt ist, sowohl in Belgien als auch im Ausland,

- die Personalmitglieder des Ausländeramtes, sofern dies im Rahmen der Ermittlung und Feststellung von Verstößen gegen das Gesetz vom 15. Dezember 1980 über die Einreise ins Staatsgebiet, den Aufenthalt, die Niederlassung und das Entfernen von Ausländern und das Gesetz vom 30. April 1999 über die Beschäftigung ausländischer Arbeitnehmer erforderlich ist,

- die Personalmitglieder des Föderalen Öffentlichen Dienstes Auswärtige Angelegenheiten und die diplomatischen und konsularischen Personalmitglieder, die vom Botschafter oder Konsul individuell dazu ermächtigt worden sind, sofern dies im Rahmen der Betrugsbekämpfung erforderlich ist,

- das Unternehmen, das mit der Herstellung der Personalausweise beauftragt ist, und die Personen, die in diesem Unternehmen strikt dazu ermächtigt worden sind, und zwar ausschließlich für die Herstellung und Ausstellung der Personalausweise. ’

3. Paragraph 3 Absatz 2 Nr. 1 wird wie folgt ersetzt:

‘ 1. die ihn betreffenden Informationen im Nationalregister der natürlichen Personen, in den Bevölkerungsregistern und im Fremdenregister sowie im Register der Personalausweise und im Register der Ausländerkarten, die in Artikel 6*bis* erwähnt sind, einzusehen, ’.

4. Paragraph 4 wird wie folgt ersetzt:

‘ § 4. Auf dem elektronischen Personalausweis befindliche Daten, die sowohl mit bloßem Auge erkennbar als auch anhand eines Kartenlesers lesbar sind, mit Ausnahme des Lichtbildes des Inhabers, der Nationalregisternummer und des digitalen Bildes der Fingerabdrücke, können gemäß den Gesetzes- und Verordnungsbestimmungen in Bezug auf den Schutz des Privatlebens und den Schutz personenbezogener Daten gelesen und/oder registriert werden.

Die Nationalregisternummer und das Lichtbild des Inhabers dürfen nur benutzt werden, wenn diese Benutzung durch oder aufgrund eines Gesetzes, eines Dekrets oder einer Ordonnanz erlaubt ist. Der elektronische Personalausweis darf nur mit der freiwilligen und spezifischen Einwilligung seines Inhabers nach dessen Aufklärung gelesen oder benutzt werden.

Wird einem Bürger im Rahmen einer EDV-Anwendung ein Vorteil oder Dienst über seinen elektronischen Personalausweis angeboten, muss der betreffenden Person ebenfalls eine Alternative vorgeschlagen werden, bei der die Benutzung des elektronischen Personalausweises nicht erforderlich ist.

Unbeschadet des Artikels 1 des Königlichen Erlasses vom 25. März 2003 über die Personalausweise darf der Inhaber des elektronischen Personalausweises außer in Fällen, die vom König durch einen im Ministerrat beratenen Erlass festgelegt sind, sich weigern, dass seine Daten gelesen und/oder registriert werden. ’

5. Paragraph 7 Absatz 1 wird wie folgt ersetzt:

‘ Der König bestimmt nach Stellungnahme der Datenschutzbehörde Form und Modalitäten der Herstellung, Ausstellung und Verwendung des Ausweises beziehungsweise der Karte. ’

6. Paragraph 7 wird durch einen Absatz mit folgendem Wortlaut ergänzt:

‘ Das qualifizierte Signaturzertifikat wird auf dem Personalausweis minderjähriger Personen nicht aktiviert ».

B.1.2. Infolge dieser Abänderung bestimmt Artikel 6 des Gesetzes vom 19. Juli 1991 « über die Bevölkerungsregister, die Personalausweise, die Ausländerkarten und die Aufenthaltsdokumente » (nachstehend: Gesetz vom 19. Juli 1991) nunmehr:

« Die Gemeinde stellt Belgiern einen Personalausweis aus, Ausländern, denen der Aufenthalt im Königreich für länger als drei Monate gestattet oder erlaubt ist oder deren Niederlassung erlaubt ist, eine Ausländerkarte und Ausländern, die gemäß der Bestimmungen des Gesetzes vom 15. Dezember 1980 über die Einreise ins Staatsgebiet, den Aufenthalt, die Niederlassung und das Entfernen von Ausländern aus einem anderen Grund eingetragen sind, ein Aufenthaltsdokument. Personalausweis, Ausländerkarte und Aufenthaltsdokument gelten als Bescheinigung über die Eintragung in den Bevölkerungsregistern.

[…]

§ 2. Auf dem Personalausweis und der Ausländerkarte wird neben der Unterschrift des Inhabers entweder die Unterschrift des Gemeindebeamten, der den Ausweis beziehungsweise die Karte ausstellt, oder, bei Aushändigung des Ausweises beziehungsweise der Karte durch Die Post, AG öffentlichen Rechts, die Unterschrift der Person dieses Unternehmens vermerkt, die zu diesem Zweck ermächtigt worden ist gemäß den Modalitäten, die durch den im § 1 Absatz 2 erwähnten Königlichen Erlass festgelegt werden. Personenbezogene Daten, die mit bloßem Auge sichtbar und auf elektronische Weise lesbar sind, werden ebenfalls auf dem Ausweis beziehungsweise der Karte vermerkt.

Die mit bloßem Auge sichtbaren und auf elektronische Weise lesbaren personenbezogen Daten betreffen:

1. Name,

2. die ersten zwei Vornamen,

3. den ersten Buchstaben des dritten Vornamen,

4. Staatsangehörigkeit,

5. Geburtsort und -datum,

6. Geschlecht,

7. Ausstellungsort des Ausweises beziehungsweise der Karte,

8. Anfangs- und Enddatum der Gültigkeit des Ausweises beziehungsweise der Karte,

9. Bezeichnung und Nummer des Ausweises beziehungsweise der Karte,

10. Bild des Inhabers,

11. [...]

12. Erkennungsnummer des Nationalregisters.

Die auf elektronische Weise lesbaren personenbezogenen Daten betreffen:

1. Identitäts- und Signaturschlüssel,

2. Identitäts- und Signaturzertifikate,

3. den Zertifizierungsdiensteanbieter,

4. die erforderliche Information zur Authentifizierung des Ausweises beziehungsweise der Karte und zum Schutz der auf elektronische Weise lesbaren Daten auf dem Ausweis beziehungsweise der Karte und zur Benutzung der diesbezüglichen qualifizierten Zertifikate,

5. andere durch das Gesetz vorgesehene oder zugelassene Vermerke und durch die europäischen Rechtsvorschriften auferlegte Vermerke,

6. Hauptwohnort des Inhabers,

7. den in Artikel 374/1 des Zivilgesetzbuches erwähnten Vermerk,

8. das digitale Bild der Fingerabdrücke des Zeigefingers der linken und der rechten Hand des Inhabers oder - bei Invalidität oder Untauglichkeit - eines anderen Fingers jeder Hand; der König bestimmt nach Stellungnahme der Datenschutzbehörde durch einen im Ministerrat beratenen Erlass die Bedingungen und Modalitäten für die Erfassung des digitalen Bildes der Fingerabdrücke.

Der Inhaber des Ausweises beziehungsweise der Karte kann auf die Aktivierung der im vorhergehenden Absatz Nr. 1 bis 3 erwähnten Daten verzichten, wenn er dies wünscht.

Die in Absatz 3 Nr. 8 erwähnte Information darf nur während der Zeit, die für die Herstellung und Ausstellung des Personalausweises erforderlich ist, und in jedem Fall während eines Zeitraums von höchstens drei Monaten aufbewahrt werden, wobei die Daten nach Ablauf dieser Frist von drei Monaten unbedingt vernichtet und gelöscht werden müssen.

Ist beziehungsweise sind ermächtigt, die in Absatz 3 Nr. 8 erwähnte Information zu lesen:

- das Gemeindepersonal, das mit der Ausstellung der Personalausweise beauftragt ist,

- die Polizeidienste, sofern dies für die Erfüllung ihrer verwaltungs- und gerichtspolizeilichen gesetzlichen Aufträge im Rahmen der Betrugsbekämpfung erforderlich ist, insbesondere der Bekämpfung des Menschenhandels und -schmuggels, des Betrugs und der Untreue, der Geldwäsche, des Terrorismus, der Fälschung und des Gebrauchs gefälschter Urkunden, der Namensanmaßung und des Gebrauchs eines falschen Namens, der Verstöße

gegen das Gesetz vom 15. Dezember 1980 über die Einreise ins Staatsgebiet, den Aufenthalt, die Niederlassung und das Entfernen von Ausländern und der Behinderungen der verwaltungspolizeilichen Aufträge,

- das Personal, das mit der Grenzkontrolle beauftragt ist, sowohl in Belgien als auch im Ausland,

- die Personalmitglieder des Ausländeramtes, sofern dies im Rahmen der Ermittlung und Feststellung von Verstößen gegen das Gesetz vom 15. Dezember 1980 über die Einreise ins Staatsgebiet, den Aufenthalt, die Niederlassung und das Entfernen von Ausländern und das Gesetz vom 30. April 1999 über die Beschäftigung ausländischer Arbeitnehmer erforderlich ist,

- die Personalmitglieder des Föderalen Öffentlichen Dienstes Auswärtige Angelegenheiten und die diplomatischen und konsularischen Personalmitglieder, die vom Botschafter oder Konsul individuell dazu ermächtigt worden sind, sofern dies im Rahmen der Betrugsbekämpfung erforderlich ist,

- das Unternehmen, das mit der Herstellung der Personalausweise beauftragt ist, und die Personen, die in diesem Unternehmen strikt dazu ermächtigt worden sind, und zwar ausschließlich für die Herstellung und Ausstellung der Personalausweise.

[…]

§ 3. Der Inhaber des Ausweises beziehungsweise der Karte kann jederzeit anhand dieses Ausweises beziehungsweise dieser Karte oder bei der Gemeinde, in der er in den Bevölkerungsregistern eingetragen ist, beantragen, die elektronischen Daten, die im Ausweis beziehungsweise in der Karte gespeichert sind oder anhand dieses Ausweises beziehungsweise dieser Karte zugänglich sind, einzusehen, und hat das Recht, die Berichtigung seiner personenbezogenen Daten, die nicht präzise, vollständig und genau auf dem Ausweis beziehungsweise der Karte wiedergegeben sind, zu beantragen.

Der Inhaber des Ausweises beziehungsweise der Karte hat das Recht, anhand dieses Ausweises beziehungsweise dieser Karte oder bei der Gemeinde, in der er in den Bevölkerungsregistern eingetragen ist:

1. die ihn betreffenden Informationen im Nationalregister der natürlichen Personen, in den Bevölkerungsregistern und im Fremdenregister sowie im Register der Personalausweise und im Register der Ausländerkarten, die in Artikel 6*bis* erwähnt sind, einzusehen,

2. diese Daten, wenn sie nicht präzise, vollständig und genau wiedergegeben sind, berichtigen zu lassen,

3. alle Behörden, Einrichtungen oder Personen, die im Laufe der letzten sechs Monate seine Daten im Bevölkerungsregister oder im Nationalregister der natürlichen Personen eingesehen oder fortgeschrieben haben, zur Kenntnis zu nehmen, mit Ausnahme der Verwaltungs- und Gerichtsbehörden, die mit der Ermittlung und Ahndung von Delikten beauftragt sind, der Staatssicherheit und des Allgemeinen Nachrichten- und Sicherheitsdienstes der Streitkräfte.

Der König bestimmt das Datum des Inkrafttretens des im vorhergehenden Absatz Nr. 3 erwähnten Rechts auf Kenntnisnahme und die Regelung, der das Recht auf Einsichtnahme und Berichtigung und die Kenntnisnahme, die in den vorhergehenden Nummern erwähnt sind, unterliegen.

§ 4. Auf dem elektronischen Personalausweis befindliche Daten, die sowohl mit bloßem Auge erkennbar als auch anhand eines Kartenlesers lesbar sind, mit Ausnahme des Lichtbildes des Inhabers, der Nationalregisternummer und des digitalen Bildes der Fingerabdrücke, können gemäß den Gesetzes- und Verordnungsbestimmungen in Bezug auf den Schutz des Privatlebens und den Schutz personenbezogener Daten gelesen und/oder registriert werden.

Die Nationalregisternummer und das Lichtbild des Inhabers dürfen nur benutzt werden, wenn diese Benutzung durch oder aufgrund eines Gesetzes, eines Dekrets oder einer Ordonnanz erlaubt ist. Der elektronische Personalausweis darf nur mit der freiwilligen und spezifischen Einwilligung seines Inhabers nach dessen Aufklärung gelesen oder benutzt werden.

Wird einem Bürger im Rahmen einer EDV-Anwendung ein Vorteil oder Dienst über seinen elektronischen Personalausweis angeboten, muss der betreffenden Person ebenfalls eine Alternative vorgeschlagen werden, bei der die Benutzung des elektronischen Personalausweises nicht erforderlich ist.

Unbeschadet des Artikels 1 des Königlichen Erlasses vom 25. März 2003 über die Personalausweise darf der Inhaber des elektronischen Personalausweises außer in Fällen, die vom König durch einen im Ministerrat beratenen Erlass festgelegt sind, sich weigern, dass seine Daten gelesen und/oder registriert werden.

[...]

§ 7. Der König bestimmt nach Stellungnahme der Datenschutzbehörde Form und Modalitäten der Herstellung, Ausstellung und Verwendung des Ausweises beziehungsweise der Karte.

[…]

Das qualifizierte Signaturzertifikat wird auf dem Personalausweis minderjähriger Personen nicht aktiviert.

[…] ».

B.1.3. Nach der Begründung bezweckt die angefochtene Bestimmung, « Personen möglichst effizient zu identifizieren », um « die Bekämpfung des Identitätsbetrugs zu verstärken » (*Parl. Dok.*, Kammer, 2017-2018, DOC 54-3256/001, S. 34).

Zu diesem Zweck sieht die angefochtene Bestimmung vor, dass der Personalausweis von nun an das digitale Bild der Fingerabdrücke des Zeigefingers der linken und der rechten Hand des Inhabers oder – bei Invalidität oder Untauglichkeit – eines anderen Fingers jeder Hand

enthält (Artikel 6 § 2 Absatz 3 Nr. 8 des Gesetzes vom 19. Juli 1991). Diese persönlichen Informationen sind nur elektronisch lesbar und nicht mit bloßem Auge erkennbar.

Das digitale Bild der Fingerabdrücke darf nur während der Zeit, die für die Herstellung und Ausstellung des Personalausweises erforderlich ist, und in jedem Fall während eines Zeitraums von höchstens drei Monaten aufbewahrt werden. Nach Ablauf dieser Frist von drei Monaten müssen die Daten unbedingt vernichtet und gelöscht werden (Artikel 6 § 2 Absatz 5).

Nach einer Bemerkung der Datenschutzbehörde, die der Ansicht war, dass « es anstatt dem König die Aufgabe zur Bestimmung der Behörden zu übertragen, die ermächtigt sind, die digitalen Fingerabdrücke zu lesen, Aufgabe des Gesetzgebers im formellen Sinn des Begriffes ist, dies zu tun » (Stellungnahme Nr. 106/2018 vom 17. Oktober 2018, *Parl. Dok.*, Kammer, 2018-2019, DOC 54-3256/003, S. 121), werden in der angefochtenen Bestimmung die Stellen aufgezählt, die ermächtigt sind, das digitale Bild der Fingerabdrücke zu lesen (Artikel 6 § 2 Absatz 6).

Es handelt sich um das Gemeindepersonal, das mit der Ausstellung der Personalausweise beauftragt ist, die Polizeidienste, « sofern dies für die Erfüllung ihrer verwaltungs- und gerichtspolizeilichen gesetzlichen Aufträge im Rahmen der Betrugsbekämpfung erforderlich ist, insbesondere der Bekämpfung des Menschenhandels und -schmuggels, des Betrugs und der Untreue, der Geldwäsche, des Terrorismus, der Fälschung und des Gebrauchs gefälschter Urkunden, der Namensanmaßung und des Gebrauchs eines falschen Namens, der Verstöße gegen das Gesetz vom 15. Dezember 1980 ‘ über die Einreise ins Staatsgebiet, den Aufenthalt, die Niederlassung und das Entfernen von Ausländern ’ » und der Behinderungen der verwaltungspolizeilichen Aufträge, das Personal, das mit der Grenzkontrolle beauftragt ist, sowohl in Belgien als auch im Ausland, die Personalmitglieder des Ausländeramtes, « sofern dies im Rahmen der Ermittlung und Feststellung von Verstößen gegen das vorerwähnte Gesetz vom 15. Dezember 1980 und das Gesetz vom 30. April 1999 ‘ über die Beschäftigung ausländischer Arbeitnehmer ’ erforderlich ist », die Personalmitglieder des Föderalen Öffentlichen Dienstes Auswärtige Angelegenheiten und die diplomatischen und konsularischen Personalmitglieder, die vom Botschafter oder Konsul individuell dazu ermächtigt worden sind, « sofern dies im Rahmen der Betrugsbekämpfung erforderlich ist » und schließlich um das Unternehmen, das mit der Herstellung der Personalausweise beauftragt

ist, und die Personen, die in diesem Unternehmen strikt dazu ermächtigt worden sind, und zwar « ausschließlich für die Herstellung und Ausstellung der Personalausweise ».

Der Gesetzgeber ermächtigt den König, einerseits durch einen im Ministerrat beratenen Erlass die Bedingungen und Modalitäten für die Erfassung des digitalen Bildes der Fingerabdrücke und andererseits die Form und die Modalitäten der Herstellung, Ausstellung und Verwendung des Ausweises beziehungsweise der Karte, in beiden Fällen nach Stellungnahme der Datenschutzbehörde, zu bestimmen (Artikel 6 § 2 Absatz 3 Nr. 8 und § 7).

B.1.4. In der Begründung heißt es, dass die damals im Entwurf befindliche angefochtene Bestimmung « im Einklang mit den Empfehlungen der Europäischen Kommission » steht (*Parl. Dok.*, Kammer, 2017-2018, DOC 54-3256/001, S. 35).

Diese hatte zuvor, am 17. April 2018, einen Vorschlag für eine Verordnung vorgelegt, die die obligatorische Speicherung von digitalen Fingerabdrücken auf den Personalausweisen für die Mitgliedstaaten, die Personalausweise ausstellen, vorsah, « um die Verwendung von gefälschten Dokumenten, derer sich Terroristen und Kriminelle bedienen können, um aus einem Drittland in die EU einzureisen, einzudämmen » (ebenda; siehe auch *Parl. Dok.*, Kammer, 2018-2019, DOC 54-3256/003, SS. 5 und 17).

Aus den Erläuterungen des Ministers der Sicherheit und des Innern im Ausschuss für Inneres, Allgemeine Angelegenheiten und öffentlichen Dienst der Kammer geht hervor, dass die angefochtene Bestimmung das gleiche Ziel wie das verfolgt, das « in der Begründung der Europäischen Kommission zum Vorschlag für eine Verordnung KOM (2018) 212 zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern und der Aufenthaltsdokumente, die Unionsbürgern und deren Familienangehörigen ausgestellt werden, die ihr Recht auf Freizügigkeit ausüben » angegeben ist (*Parl. Dok.*, Kammer, 2018-2019, DOC 54-3256/003, S. 30).

B.1.5. Die angefochtene Bestimmung ist am 23. Dezember 2018 in Kraft getreten.

B.2.1. Nach der Annahme des Gesetzes vom 25. November 2018 wurde im Amtsblatt der Europäischen Union vom 12. Juli 2019 die Verordnung (EU) 2019/1157 des Europäischen Parlaments und des Rates vom 20. Juni 2019 « zur Erhöhung der Sicherheit der

Personalausweise von Unionsbürgern und der Aufenthaltsdokumente, die Unionsbürgern und deren Familienangehörigen ausgestellt werden, die ihr Recht auf Freizügigkeit ausüben » (nachstehend: Verordnung (EU) 2019/1157) veröffentlicht.

Diese Verordnung bezweckt « die Erhöhung der Sicherheit und die Erleichterung der Ausübung des Rechts auf Freizügigkeit von Unionsbürgern und ihren Familienangehörigen » (Erwägungsgrund 46). Durch die Speicherung eines Gesichtsbilds und zweier digitaler Fingerabdrücke auf Personalausweisen und Aufenthaltskarten soll das Risiko des Identitätsbetrugs verringert und « die Sicherheit von Personalausweisen und Aufenthaltskarten […] verbesser[t] » werden (Erwägungsgrund 18).

B.2.2. Nach ihrem Artikel 1 werden mit der Verordnung (EU) 2019/1157 « die Sicherheitsstandards für Personalausweise verschärft, die die Mitgliedstaaten ihren Staatsangehörigen ausstellen, und für Aufenthaltsdokumente, die die Mitgliedstaaten Unionsbürgern und deren Familienangehörigen ausstellen, die ihr Recht auf Freizügigkeit in der Union ausüben ».

Die Verordnung gilt unter anderem für « Personalausweise, die die Mitgliedstaaten gemäß Artikel 4 Absatz 3 der Richtlinie 2004/38/EG eigenen Staatsangehörigen ausstellen » (Artikel 2 Buchstabe a).

Artikel 3 der Verordnung (EG) 2019/1157 bezieht sich auf die « Sicherheitsstandards/Gestaltung/Spezifikationen », welche auf die nationalen Personalausweise anwendbar sind:

« 1. Die von den Mitgliedstaaten ausgestellten Personalausweise werden im ID-1-Format hergestellt und sind mit einem maschinenlesbaren Bereich ausgestattet. Diese Personalausweise orientieren sich an den Spezifikationen und Mindestsicherheitsstandards des ICAO-Dokuments 9303 und entsprechen den Anforderungen der Buchstaben c, d, f und g des Anhangs der Verordnung (EG) Nr. 1030/2002, geändert durch die Verordnung (EU) 2017/1954.

2. Die Datenelemente von Personalausweisen entsprechen den Spezifikationen des Teils 5 des ICAO-Dokuments 9303.

Abweichend von Unterabsatz 1 kann die Dokumentennummer in Zone I erfasst werden, und die Angabe des Geschlechts ist optional.

3. Auf dem Dokument erscheint der Titel ‘ Personalausweis ’ oder eine andere bereits etablierte nationale Bezeichnung in der Amtssprache oder den Amtssprachen des ausstellenden Mitgliedstaats sowie das Wort ‘ Personalausweis ’ in mindestens einer weiteren Amtssprache der Organe der Union.

4. Auf der Vorderseite des Personalausweises erscheint der zwei Buchstaben umfassende Ländercode des ausstellenden Mitgliedstaats im Negativdruck in einem blauen Rechteck, umgeben von zwölf gelben Sternen.

5. Die Personalausweise werden mit einem hochsicheren Speichermedium versehen, das ein Gesichtsbild des Personalausweisinhabers und zwei Fingerabdrücke in interoperablen digitalen Formaten enthält. Bei der Erfassung der biometrischen Identifikatoren wenden die Mitgliedstaaten die technischen Spezifikationen gemäß dem Durchführungsbeschluss der Kommission C(2018)7767 an.

6. Das Speichermedium weist eine ausreichende Kapazität auf und ist geeignet, die Integrität, die Authentizität und die Vertraulichkeit der Daten sicherzustellen. Auf die gespeicherten Daten kann kontaktlos zugegriffen werden, und sie werden nach Maßgabe des Durchführungsbeschlusses C(2018)7767 gesichert. Die Mitgliedstaaten tauschen untereinander die Informationen aus, die für die Authentifizierung des Speichermediums und den Zugriff auf und die Überprüfung der in Absatz 5 genannten biometrischen Datennotwendig sind.

7. Kinder unter zwölf Jahren können von der Pflicht zur Abgabe von Fingerabdrücken befreit werden.

Kinder unter sechs Jahren sind von der Pflicht zur Abgabe von Fingerabdrücken befreit.

Personen, bei denen eine Abnahme von Fingerabdrücken physisch nicht möglich ist, sind von der Pflicht zur Abgabe von Fingerabdrücken befreit.

8. Sofern zur Erreichung des angestrebten Ziels erforderlich und angemessen, können die Mitgliedstaaten für den innerstaatlichen Gebrauch nach dem nationalen Recht vorgeschriebene Hinweise und Bemerkungen eintragen. Die Wirksamkeit der Mindestsicherheitsstandards und die grenzübergreifende Interoperabilität der Personalausweise dürfen dadurch nicht beeinträchtigt werden.

9. Nehmen die Mitgliedstaaten ein Dual Interface oder ein gesondertes Speichermedium in den Personalausweis auf, so muss das zusätzliche Speichermedium den einschlägigen ISO-Normen entsprechen und darf keine Interferenzen mit dem in Absatz 5 genannten Speichermedium bewirken.

10. Speichern die Mitgliedstaaten im Personalausweis Daten für elektronische Dienste wie elektronische Behördendienste und den elektronischen Geschäftsverkehr, so müssen diese nationalen Daten von den in Absatz 5 genannten biometrischen Daten physisch oder logisch getrennt sein.

11. Versehen die Mitgliedstaaten den Personalausweis mit zusätzlichen Sicherheitsmerkmalen, so darf das die grenzübergreifende Kompatibilität dieser

Personalausweise und die Wirksamkeit der Mindestsicherheitsstandards nicht beeinträchtigen ».

Artikel 10 derselben Verordnung bezieht sich auf die Erfassung biometrischer Identifikatoren:

« 1. Biometrische Identifikatoren werden ausschließlich durch qualifiziertes und ordnungsgemäß befugtes Personal erfasst, das von den für die Ausstellung der Personalausweise oder Aufenthaltskarten zuständigen Behörden benannt wird; diese Erfassung erfolgt zum Zwecke der Aufnahme in ein hochsicheres Speichermedium gemäß Artikel 3 Absatz 5 bei Personalausweisen bzw. gemäß Artikel 7 Absatz 1 bei Aufenthaltskarten. Abweichend von Satz 1 werden Fingerabdrücke ausschließlich von qualifiziertem und ordnungsgemäß befugtem Personal dieser Behörden erfasst, es sei denn, es handelt sich um Anträge, die bei den diplomatischen und konsularischen Behörden des Mitgliedstaats eingereicht wurden.

Um die Übereinstimmung der biometrischen Identifikatoren mit der Identität des Antragstellers zu gewährleisten, muss der Antragsteller während des Ausstellungsverfahrens für jeden Antrag mindestens einmal persönlich erscheinen.

2. Die Mitgliedstaaten stellen sicher, dass angemessene und wirksame Verfahren für die Erfassung biometrischer Identifikatoren bestehen, und dass diese Verfahren den in der Charta, in der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten und im Übereinkommen der Vereinten Nationen über die Rechte des Kindes verankerten Rechten und Grundsätzen entsprechen.

Treten bei der Erfassung der biometrischen Identifikatoren Schwierigkeiten auf, stellen die Mitgliedstaaten sicher, dass geeignete Verfahren zur Wahrung der Würde der betroffenen Person vorhanden sind.

3. Vorbehaltlich anderer Verarbeitungszwecke nach Maßgabe des Unionsrechts und des nationalen Rechts werden biometrische Identifikatoren, die für die Zwecke der Personalisierung von Personalausweisen oder Aufenthaltsdokumenten gespeichert werden, auf hochsichere Weise sowie ausschließlich bis zu dem Tag der Abholung des Dokuments und keinesfalls länger als 90 Tage ab dem Tag der Ausstellung des Dokuments gespeichert Nach diesem Zeitraum werden die biometrischen Identifikatoren umgehend gelöscht oder vernichtet ».

Artikel 11 derselben Verordnung bezieht sich auf den Schutz personenbezogener Daten und die Haftung:

« 1. Unbeschadet der Verordnung (EU) 2016/679 gewährleisten die Mitgliedstaaten die Sicherheit, Integrität, Echtheit und vertrauliche Behandlung der für die Zwecke dieser Verordnung erfassten und gespeicherten Daten.

2. Für die Zwecke dieser Verordnung gelten die für die Ausstellung von Personalausweisen und Aufenthaltsdokumenten zuständigen Behörden als der Verantwortliche gemäß Artikel 4 Absatz 7 der Verordnung (EU) 2016/679, und sind für die Verarbeitung personenbezogener Daten verantwortlich.

3. Die Mitgliedstaaten sorgen dafür, dass die Aufsichtsbehörden ihren Aufgaben gemäß der Verordnung (EU) 2016/679 umfassend nachkommen können, was den Zugang zu allen personenbezogenen Daten und allen erforderlichen Informationen sowie zu den Geschäftsräumen und Datenverarbeitungsgeräten der zuständigen Behörden einschließt.

4. Durch die Zusammenarbeit mit externen Dienstleistungsanbietern wird ein Mitgliedstaat nicht von der Haftung nach dem Unionsrecht oder dem nationalen Recht für Verstöße gegen Pflichten im Zusammenhang mit personenbezogenen Daten befreit.

5. Maschinenlesbare Informationen dürfen nur gemäß dieser Verordnung oder dem nationalen Recht des ausstellenden Mitgliedstaats in einen Personalausweis und ein Aufenthaltsdokument aufgenommen werden.

6. Auf dem Speichermedium von Personalausweisen und Aufenthaltsdokumenten gespeicherte biometrische Daten dürfen nur gemäß dem Unionsrecht und dem nationalen Recht von ordnungsgemäß befugten Mitarbeitern der zuständigen nationalen Behörden und Agenturen der Union verwendet werden, um

a) den Personalausweis oder das Aufenthaltsdokument auf seine Echtheit zu überprüfen,

b) die Identität des Inhabers anhand direkt verfügbarer abgleichbarer Merkmale zu überprüfen, wenn die Vorlage des Personalausweises oder Aufenthaltsdokuments gesetzlich vorgeschrieben ist.

7. Die Mitgliedstaaten halten eine Liste der zuständigen Behörden vor, die Zugang zu den biometrischen Daten haben, die auf dem in Artikel 3 Absatz 5 dieser Verordnung genannten Speichermedium gespeichert sind, und übermitteln diese Liste jährlich der Kommission. Die Kommission veröffentlicht im Internet eine Zusammenstellung dieser nationalen Listen ».

Artikel 14 derselben Verordnung bezieht sich auf die zusätzlichen technischen Spezifikationen:

« 1. Um gegebenenfalls die erforderliche Übereinstimmung der in Artikel 2 Buchstaben a und c genannten Personalausweise und Aufenthaltsdokumente mit künftigen Mindestsicherheitsstandards zu gewährleisten, legt die Kommission im Wege von Durchführungsrechtsakten zusätzliche technische Spezifikationen zu Folgendem fest:

a) zusätzliche Sicherheitsmerkmale und -anforderungen, einschließlich höherer Standards zum Schutz vor Fälschung, Verfälschung und Nachahmung;

b) technische Spezifikationen für das Speichermedium der biometrischen Daten gemäß Artikel 3 Absatz 5 und deren Sicherung, einschließlich der Verhinderung des unbefugten Zugriffs und einer Erleichterung der Validierung;

c) Qualitätsanforderungen an und gemeinsame technische Standards für das Gesichtsbild und Fingerabdrücke.

Diese Durchführungsrechtsakte werden gemäß dem in Artikel 15 Absatz 2 genannten Prüfverfahren erlassen.

2. Nach dem in Artikel 15 Absatz 2 genannten Verfahren kann beschlossen werden, dass die Spezifikationen gemäß diesem Artikel geheim und nicht zu veröffentlichen sind. In diesem Fall werden sie ausschließlich den von den Mitgliedstaaten für den Druck benannten Stellen sowie Personen zugänglich gemacht, die von einem Mitgliedstaat oder der Kommission hierzu ordnungsgemäß ermächtigt worden sind.

3. Jeder Mitgliedstaat benennt eine Stelle, die für den Druck der Personalausweise, und eine Stelle, die für den Druck der Aufenthaltskarten für Familienangehörige von Unionsbürgern zuständig ist, und teilt der Kommission und den anderen Mitgliedstaaten die Namen dieser Stellen mit. Die Mitgliedstaaten können in der Folge andere Stellen benennen als die zunächst benannte; die Kommission und die Mitgliedstaaten sind entsprechend zu informieren.

Die Mitgliedstaaten können auch beschließen, eine einzige zuständige Stelle für den Druck von Personalausweisen und von Aufenthaltskarten für Familienangehörige von Unionsbürgern zu benennen ist; sie teilen der Kommission und den anderen Mitgliedstaaten den Namen dieser Stelle mit.

Zwei oder mehr Mitgliedstaaten können auch eine einzige Stelle für diese Zwecke benennen; sie informieren die Kommission und die anderen Mitgliedstaaten entsprechend ».

B.2.3. Nach ihrem Artikel 16 ist die Verordnung (EU) 2019/1157 am 2. August 2019 in Kraft getreten. Sie ist ab dem 2. August 2021 anwendbar, was bedeutet, dass die Mitgliedstaaten ab diesem Datum nur Ausweis- und Aufenthaltsdokumente ausstellen sollen, die die darin vorgesehenen Anforderungen erfüllen (Erwägungsgrund 44).

In Bezug auf die Zulässigkeit

Was die Zulässigkeit des Schriftsatzes des Ministerrates in der Rechtssache Nr. 7150 betrifft

B.3.1. Die klagenden Parteien in der Rechtssache Nr. 7150 machen die Nichtigkeit des Schriftsatzes des Ministerrates mit der Begründung geltend, dass er eine oder mehrere Stellen auf Englisch enthält, die nicht übersetzt sind, womit gegen Artikel 40 des Gesetzes vom

15. Juni 1935 « über den Sprachengebrauch in Gerichtsangelegenheiten » verstoßen würde und was eine Verletzung der Verteidigungsrechte zur Folge hätte.

B.3.2. Das Gesetz vom 15. Juni 1935 « über den Sprachengebrauch in Gerichtsangelegenheiten » findet auf Verfahren vor dem Verfassungsgerichtshof keine Anwendung. Der Schriftsatz des Ministerrates war gemäß Artikel 62 Absatz 2 Nr. 1 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof auf Niederländisch abgefasst. Die Wiedergabe einer Grafik durch den Ministerrat, deren Legende auf Englisch ist, die aber in dem Schriftsatz auf Niederländisch eindeutig erläutert ist, zur Untermauerung seiner Argumente, stellt keinen Verstoß gegen den vorerwähnten Artikel 62 Absatz 2 Nr. 1 dar.

B.3.3. Die Einrede wird abgewiesen.

Was die Folgen des Inkrafttretens der Verordnung (EU) 2019/1157 für die Zulässigkeit der Klagen betrifft

B.4.1. Der Ministerrat führt an, dass selbst wenn man annehme, dass das Interesse, das die klagenden Parteien nachweisen müssten, zum Zeitpunkt der Einreichung der Klageschriften bestanden hätte, dieses Interesse in jedem Fall aufgrund des Inkrafttretens der Verordnung (EU) 2019/1157 nach der Annahme der angefochtenen Bestimmung nicht mehr vorhanden sei.

B.4.2. Wie in B.1.4 erwähnt, hat der Gesetzgeber die angefochtene Bestimmung angenommen, als sich die Verordnung (EU) 2019/1157 noch im Entwurf befand.

Aus dem Umstand, dass bestimmte Bestimmungen des angefochtenen Artikels 27 des Gesetzes vom 25. November 2018 eine ähnliche Tragweite wie bestimmte Bestimmungen der Verordnung (EU) 2019/1157 haben, folgt weder, dass die klagenden Parteien gegebenenfalls kein aktuelles Interesse mehr an ihren Klagen haben, noch dass der Gerichtshof nicht mehr befugt wäre, über die Verfassungsmäßigkeit der angefochtenen Bestimmung zu befinden. Dieser Umstand hat jedoch zur Folge, dass der Gerichtshof die vorerwähnte Verordnung berücksichtigen muss.

B.4.3. Entgegen der Auffassung des Ministerrates müssen die klagenden Parteien keine Klage auf Nichtigerklärung der Verordnung (EU) 2019/1157 beim Gerichtshof der Europäischen Union einreichen, um ihr Interesse zu wahren.

B.4.4. Die Einrede wird abgewiesen.

Was die Zulässigkeit der Klagen betrifft

B.5.1. Der Ministerrat bestreitet das Interesse der klagenden Parteien in den Rechtssachen Nrn. 7125, 7150 und 7211. Seiner Auffassung nach weisen diese Parteien nicht konkret einen ausreichend individualisierten Zusammenhang zwischen der angefochtenen Bestimmung und ihrer Situation nach, zumal die klagende Partei in der Rechtssache Nr. 7211, die zum Zeitpunkt der Einreichung der Klageschrift ein Jahr alt war, nicht vor dem Alter von fünfzehn Jahren der Verpflichtung, einen Personalausweis zu besitzen, unterliege. Außerdem weise die « Parti Libertarien », erste klagende Partei in der Rechtssache Nr. 7125, weder nach, dass sie die Rechtspersönlichkeit besitze, noch dass sie die Ausnahme geltend machen könne, in deren Rahmen es politischen Parteien erlaubt ist, beim Gerichtshof Klage zu erheben.

B.5.2. Laut Artikel 2 Nr. 2 des Sondergesetzes vom 6. Januar 1989 muss die vor dem Gerichtshof klagende Partei eine natürliche oder juristische Person sein, die ein Interesse nachweist. Politische Parteien, die faktische Vereinigungen sind, haben grundsätzlich nicht die erforderliche Fähigkeit, vor dem Gerichtshof zu klagen.

Anders verhält es sich nur dann, wenn sie in Angelegenheiten auftreten, für die sie gesetzlich als separate Entitäten anerkannt werden, und wenn, während ihr Auftreten durch Gesetz anerkannt ist, gewisse Aspekte davon zur Debatte stehen.

B.5.3. Dies trifft in diesem Fall nicht zu. Die Klage ist unzulässig, insofern sie durch die « Parti Libertarien » eingereicht wurde.

B.5.4. Die Verfassung und das Sondergesetz vom 6. Januar 1989 über den Verfassungsgerichtshof erfordern, dass jede natürliche oder juristische Person, die eine Nichtigkeitsklage erhebt, ein Interesse nachweist. Das erforderliche Interesse liegt nur bei

jenen Personen vor, deren Situation durch die angefochtene Rechtsnorm unmittelbar und ungünstig beeinflusst werden könnte.

B.5.5. Mit der angefochtenen Bestimmung wird allen Belgiern, die der Verpflichtung unterliegen, einen Personalausweis zu besitzen, das heißt allen Belgiern ab dem Alter von zwölf Jahren (Artikel 1 und 2 des königlichen Erlasses vom 25. März 2003 « über die Personalausweise ») die Abnahme von zwei digitalen Fingerabdrücken und die Speicherung ihres digitalen Bildes auf dem Personalausweis auferlegt.

Sie beeinflusst also unmittelbar und ungünstig die Situation der zweiten klagenden Partei in der Rechtssache Nr. 7125, der vier klagenden Parteien in der Rechtssache Nr. 7150 sowie der klagenden Partei in der Rechtssache Nr. 7211. Der Umstand, dass die Umsetzung der angefochtenen Bestimmung, was jede einzelne dieser Parteien betrifft, nicht sofort, sondern bei der Ausstellung eines neuen Personalausweises oder gegebenenfalls, wenn die betroffene Person das Alter von zwölf Jahren erreicht, erfolgt, ändert nichts an dieser Feststellung.

Die zweite klagende Partei in der Rechtssache Nr. 7125, die vier klagenden Parteien in der Rechtssache Nr. 7150 und die klagende Partei in der Rechtssache Nr. 7211 weisen ein Interesse an ihren Klagen nach.

B.5.6. Außer in Bezug auf die Klageberechtigung der «Parti Libertarien » werden die Einreden abgewiesen.

B.5.7. Das Interesse der klagenden Parteien in den Rechtssachen Nrn. 7202 und 7203 an der Klageerhebung wird vom Ministerrat nicht bestritten.

Was das Interesse der intervenierenden Parteien in der Rechtssache Nr. 7150 betrifft

B.6.1. Der Ministerrat bestreitet das Interesse der « Parti Libertarien » und von Baudoin Collard, klagende Parteien in der Rechtssache Nr. 7125, und der VoG « Ligue des droits humains », klagende Partei in der Rechtssache Nr. 7203, an der Intervention in der Rechtssache Nr. 7150, da diese Parteien ihre Klagegründe bereits in ihrer eigenen Klageschrift geltend machen konnten und hilfsweise aus den gleichen wie den in B.5.1 erwähnten Gründen.

B.6.2. Aus dem gleichen Grund wie dem in B.5.2 und in B.5.3 aufgeführten ist die Intervention der « Parti Libertarien » unzulässig.

B.6.3. Wenn der Gerichtshof mit einer Nichtigkeitsklage befasst wird, kann « jede Person, die ein Interesse nachweist » in einem Schriftsatz ihre Bemerkungen an den Gerichtshof richten (Artikel 87 § 2 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof).

Ein Interesse im Sinne dieser Bestimmung weist eine Person nach, die beweist, dass ihre Situation direkt von dem Entscheid betroffen sein kann, den der Gerichtshof im Zusammenhang mit der Nichtigkeitsklage erlassen muss.

B.6.4. Unter Berücksichtigung des in B.5.5 Erwähnten weisen Baudoin Collard und die VoG « Ligue des droits humains » das erforderliche Interesse an ihrer Intervention nach.

B.6.5. Die Einrede wird abgewiesen.

Was die Zulässigkeit verschiedener Klagegründe betrifft

B.7.1. Der Ministerrat führt an, dass der zweite Teil des einzigen Klagegrunds in der Rechtssache Nr. 7125, der erste Teil des zweiten Klagegrunds in der Rechtssache Nr. 7150, der erste Klagegrund in der Rechtssache Nr. 7202 und der zweite Teil des vierten Klagegrunds in den Rechtssachen Nrn. 7203 und 7211 unzulässig seien, insoweit darin die fehlende Durchführung einer Datenschutz-Folgenabschätzung im Sinne von Artikel 35 der 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) » (nachstehend: Datenschutz-Grundverordnung) vor der Annahme der angefochtenen Bestimmung bemängelt werde. Laut dem Ministerrat ist der Gerichtshof nicht befugt, über einen Beschwerdegrund zu befinden, der sich auf das Verfahren oder die Modalitäten zur Ausarbeitung eines Gesetzes bezieht.

B.7.2. Hat die Verarbeitung personenbezogener Daten voraussichtlich « ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen » zur Folge, muss der Verantwortliche gemäß Artikel 35 der Datenschutz-Grundverordnung vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchführen. Aufgrund von Artikel 36 derselben Verordnung muss der Verantwortliche, wenn aus der Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft, vor der Verarbeitung die Aufsichtsbehörde konsultieren.

B.7.3. Ohne dass es notwendig ist, sich zur Befugnis des Gerichtshofs zu äußern, über Beschwerdegründe in Bezug auf das Verfahren oder die Modalitäten zur Ausarbeitung der angefochtenen Bestimmung zu befinden, ist festzustellen, dass Artikel 35 der Datenschutz-Grundverordnung die Durchführung einer Datenschutz-Folgenabschätzung vor einer Verarbeitung, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, vorschreibt, aber nicht bei der Ausarbeitung einer Gesetzesbestimmung über eine solche Verarbeitung.

Wenn die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, und wenn sie « auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte », ist nach Artikel 35 Absatz 10 der Datenschutz-Grundverordnung vor den Verarbeitungstätigkeiten keine neue Folgenabschätzung durchzuführen, es sei denn, es ist nach dem Ermessen der Mitgliedstaaten erforderlich.

Daraus folgt, dass die Durchführung einer allgemeinen Folgenschätzung im Rahmen der Annahme einer Gesetzesbestimmung über eine Verarbeitung, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, fakultativ ist, dass aber, wenn eine solche Folgenabschätzung durchgeführt wird, es grundsätzlich nicht notwendig ist, eine neue Folgenabschätzung vor der Verarbeitung durchzuführen.

Artikel 35 der Datenschutz-Grundverordnung steht somit der Durchführung einer Folgenabschätzung bei der Ausarbeitung der Ausführungserlasse der angefochtenen Bestimmung nicht entgegen.

Diese Feststellung berührt nicht die Verpflichtung der Mitgliedstaaten gemäß Artikel 36 Absatz 4 der Datenschutz-Grundverordnung; « die Aufsichtsbehörde bei der Ausarbeitung eines Vorschlags für von einem nationalen Parlament zu erlassende Gesetzgebungsmaßnahmen oder von auf solchen Gesetzgebungsmaßnahmen basierenden Regelungsmaßnahmen, die die Verarbeitung betreffen » zu konsultieren, auf die der Gesetzgeber im vorliegenden Fall verwiesen hat.

B.7.4. Der zweite Teil des einzigen Klagegrunds in der Rechtssache Nr. 7125, der erste Teil des zweiten Klagegrunds in der Rechtssache Nr. 7150, der erste Klagegrund in der Rechtssache Nr. 7202, insoweit dieser Klagegrund aus einem Verstoß gegen Artikel 35 der Datenschutz-Grundverordnung abgeleitet ist, und der zweite Teil des vierten Klagegrunds in den Rechtssachen Nrn. 7203 und 7211 sind somit unbegründet.

Da die Tragweite von Artikel 35 der Datenschutz-Grundverordnung im Sinne des Urteils *CILFIT* des Gerichtshofes der Europäischen Union vom 6. Oktober 1982 (C-283/81) für einen vernünftigen Zweifel keinerlei Raum lässt, ist die Vorabentscheidungsfrage zur Auslegung dieser Bestimmung dem Gerichtshof nicht zu stellen.

B.8.1. Der Ministerrat macht geltend, dass der erste Teil des einzigen Klagegrunds in der Rechtssache Nr. 7125 nicht zulässig sei, insoweit er aus einem Verstoß gegen die Artikel 10 und 11 der Verfassung abgeleitet sei, da die klagenden Parteien keine zwei Personenkategorien angeben, die in der angefochtenen Bestimmung in diskriminierender Weise behandelt würden.

B.8.2. Wenn ein Verstoß gegen den Grundsatz der Gleichheit und Nichtdiskriminierung in Verbindung mit einem anderen Grundrecht geltend gemacht wird, das in der Verfassung oder in einer Bestimmung internationalen Rechts gewährleistet ist oder sich aus einem allgemeinen Rechtsgrundsatz herleitet, muss die Personenkategorie, deren Grundrecht verletzt wird, mit der Personenkategorie verglichen werden, für die dieses Grundrecht gewährleistet wird.

B.8.3. Da die Artikel 10 und 11 der Verfassung in Verbindung mit mehreren Bestimmungen geltend gemacht werden, die das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten gewährleisten, wird die Einrede abgewiesen.

B.9.1. Der Ministerrat führt an, dass der zweite Klagegrund in der Rechtssache Nr. 7150 sowie die drei Klagegründe in der Rechtssache Nr. 7202 nicht zulässig seien, insoweit sie aus einem Verstoß gegen die Datenschutz-Grundverordnung, die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 « zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates » (nachstehend: « Polizei »-Richtlinie) und das Gesetz vom 30. Juli 2018 « zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten » (nachstehend: Gesetz vom 30. Juli 2018) abgeleitet seien.

Seiner Ansicht nach ist der Gerichtshof nicht befugt, unmittelbar über einen Verstoß gegen eine Verordnung, eine Richtlinie oder ein Gesetz zu befinden. Schließlich versäumten es die klagenden Parteien in der Rechtssache Nr. 7202 in den drei Klagegründe, die sie geltend machten, die Kategorien von Bürgern anzugeben, die im Rahmen einer mittelbaren Kontrolle anhand der Artikel 10 und 11 der Verfassung zu vergleichen seien. Schließlich gewährleisteten die Datenschutz-Grundverordnung und die « Polizei »-Richtlinie kein analoges Recht auf Achtung des Privatlebens wie Artikel 22 der Verfassung.

B.9.2. Der Gerichtshof ist nicht befugt, Gesetzesnormen unmittelbar anhand von Vertragsbestimmungen oder Bestimmungen des Unionsrechts zu prüfen.

Wenn jedoch eine für Belgien verbindliche Vertragsbestimmung oder Bestimmung des Rechts der Union eine Tragweite hat, die analog zu derjenigen einer der Verfassungsbestimmungen ist, deren Prüfung zum Zuständigkeitsbereich des Gerichtshofes gehört und gegen die ein Verstoß angeführt wird, bilden die in dieser Vertragsbestimmung oder Bestimmung des Rechts der Union enthaltenen Garantien ein untrennbares Ganzes mit den Garantien, die in die betreffenden Verfassungsbestimmungen aufgenommen wurden.

Daraus folgt, dass der Gerichtshof bei der Kontrolle, die er anhand der in B.9.1 erwähnten Verfassungsbestimmungen ausübt, Bestimmungen des internationalen Rechts oder des Rechts der Union, die analoge Rechte oder Freiheiten gewährleisten, berücksichtigt.

B.9.3. Artikel 22 der Verfassung gewährleistet das Recht auf Achtung vor dem Privat- und Familienleben. Dieses Recht schließt das Recht auf den Schutz personenbezogener Daten ein.

Nach Artikel 1 Absatz 2 schützt die Datenschutz-Grundverordnung « die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten ». Die Bestimmungen der Datenschutz-Grundverordnung, die von den klagenden Parteien geltend gemacht werden, konkretisieren dieses Recht.

B.9.4. Ohne dass es notwendig ist, einerseits zu bestimmen, ob und gegebenenfalls in welchem Maße die « Polizei »-Richtlinie im vorliegenden Fall anwendbar ist, und andererseits sich zu der Frage zu äußern, ob der Gerichtshof befugt ist, über einen Verstoß gegen das Gesetz vom 30. Juli 2018 in Verbindung mit den Artikeln 10 und 11 der Verfassung zu befinden, ist festzustellen, dass die klagenden Parteien in der Rechtssache Nr. 7202 weder eine besondere Kritik im Zusammenhang mit dieser Richtlinie oder diesem Gesetz darlegen, noch angeben, inwiefern diese andere Garantien als diejenigen enthalten würden, die in der Datenschutz-Grundverordnung vorgesehen sind und die im Hinblick auf die strittige Problematik relevant wären.

B.9.5. Insoweit sie aus einem Verstoß gegen die « Polizei »-Richtlinie und das Gesetz vom 30. Juli 2018 abgeleitet sind, sind der erste und dritte Klagegrund in der Rechtssache Nr. 7202 unzulässig. Die Einreden werden im Übrigen abgewiesen.

B.10.1. Der Ministerrat macht geltend, dass der erste bis dritte Klagegrund in den Rechtssachen Nrn. 7203 und 7211 unzulässig seien, denn die klagenden Parteien beschränkten sich darauf, auf die in der Rechtssache Nr. 7202 eingereichte Klageschrift zu verweisen, ohne diese Klagegründe überhaupt darzulegen.

B.10.2. Artikel 6 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof bestimmt:

« Die Klageschrift gibt den Gegenstand der Klage an und enthält eine Darlegung des Sachverhalts und der Klagegründe ».

Um den Erfordernissen dieser Bestimmung zu entsprechen, müssen die in der Klageschrift vorgebrachten Klagegründe angeben, welche Vorschriften, deren Einhaltung der Gerichtshof gewährleistet, verletzt wären und welche Bestimmungen gegen diese Vorschriften verstoßen würden, und darlegen, in welcher Hinsicht diese Vorschriften durch diese Bestimmungen verletzt würden. Diese Erfordernisse beruhen einerseits auf der Notwendigkeit, den Gerichtshof in die Lage zu versetzen, ab dem Zeitpunkt des Einreichens des Antrags die richtige Tragweite der Nichtigkeitsklage bestimmen zu können, und andererseits darauf, den anderen Verfahrensparteien die Möglichkeit zu geben, die Argumente der klagenden Parteien zu erwidern, wofür eine klare und unzweideutige Darlegung der Klagegründe unentbehrlich ist.

B.10.3. Der Verweis auf die in einer anderen Klage dargelegten Klagegründe, selbst wenn sie als vollständig wiedergegeben gelten, erfüllt nicht die vorerwähnten Erfordernisse von Artikel 6 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof. Der erste und dritte Klagegrund in den Rechtssachen Nrn. 7203 und 7211 sind daher unzulässig.

In Bezug auf die Anträge der klagenden Parteien auf gerichtliche Untersuchungsmaßnahmen

B.11.1. Die klagenden Parteien in den Rechtssachen Nrn. 7150 und 7202 beantragen beim Gerichtshof, gerichtliche Untersuchungsmaßnahmen anzuordnen, um ein technisches Gutachten bezüglich der unzureichenden Beschreibung und fehlenden Bestimmung der wesentlichen Elemente der strittigen Maßnahme, vorhandener Alternativen zu ihr sowie der Risiken, die sie im Bereich Sicherheit zur Folge hat, einzuholen.

B.11.2. Laut Artikel 91 Absatz 1 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof hat der Gerichtshof « weitestgehende Untersuchungs- und

Ermittlungsbefugnisse »; einige davon werden in Absatz 2 dieser Bestimmung aufgezählt. Der Gerichtshof kann diese Untersuchungs- und Ermittlungsbefugnis nur dann anwenden, wenn dies zur Lösung der Rechtsfragen, über die er entscheiden muss, notwendig ist. Eine Untersuchungsmaßnahme ist nur sachdienlich, insofern Fakten festgestellt werden können, die für die Beurteilung einer Nichtigkeitsklage, einer Vorabentscheidungsfrage oder eines Zwischenstreits relevant sind.

B.11.3. Unter Berücksichtigung der Elemente, über die der Gerichtshof verfügt, und der Erläuterungen, die diesbezüglich in den Klageschriften und Schriftsätzen gegeben wurden, sind zusätzliche gerichtliche Untersuchungsmaßnahmen nicht anzuordnen.

Der Antrag auf Untersuchungsmaßnahmen wird abgewiesen.

Zur Hauptsache

B.12. Die klagenden Parteien leiten mehrere Klagegründe aus einem Verstoß der angefochtenen Bestimmung gegen das Recht auf Achtung des Privatlebens und des Rechts auf Schutz personenbezogener Daten ab (erster Teil des einzigen Klagegrunds in der Rechtssache Nr. 7125 und des vierten Klagegrunds in den Rechtssachen Nrn. 7203 und 7211; erster Klagegrund und zweiter Teil des zweiten Klagegrunds in der Rechtssache Nr. 7150; erster bis dritter Klagegrund in der Rechtssache Nr. 7202).

In Bezug auf das Recht auf Achtung des Privatlebens und des Rechts auf Schutz personenbezogener Daten

B.13.1. 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.13.2. Artikel 8 der Europäischen Menschenrechtskonvention bestimmt:

« (1) Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.

(2) Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist ».

B.13.3. Der Verfassungsgeber hat eine möglichst weitgehende Übereinstimmung zwischen Artikel 22 der Verfassung und Artikel 8 der Europäischen Menschenrechtskonvention angestrebt (*Parl. Dok.*, Kammer, 1992-1993, Nr. 997/5, S. 2).

Die Tragweite dieses Artikels 8 entspricht derjenigen der vorerwähnten Verfassungsbestimmung, sodass die durch die beiden Bestimmungen gebotenen Garantien ein untrennbares Ganzes bilden.

B.14.1. Das Recht auf Achtung des Privat- und Familienlebens, so wie es durch die vorerwähnten Verfassungs- und Vertragsbestimmungen gewährleistet wird, bezweckt im Wesentlichen, die Personen gegen Einmischungen in ihr Privatleben und Familienleben zu schützen.

Dieses Recht hat eine große Tragweite und beinhaltet unter anderem den Schutz von personenbezogenen Daten und persönlichen 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 (siehe insbesondere EuGHMR, 26. März 1987, *Leander gegen Schweden*, §§ 47-48; Große Kammer, 4. Dezember 2008, *S. und Marper gegen Vereinigtes Königreich*, §§ 66-68; 17. Dezember 2009, *B.B. gegen Frankreich*, § 57; 10. Februar 2011, *Dimitrov-Kazakov gegen Bulgarien*, §§ 29-31; 18. Oktober 2011, *Khelili gegen Schweiz*, §§ 55-57; 9. Oktober 2012, *Alkaya gegen Türkei*,

§ 29; 18. April 2013, *M.K. gegen Frankreich*, § 26; 18. September 2014, *Brunet gegen Frankreich*, § 31).

B.14.2. Das Recht auf Achtung des Privatlebens ist jedoch kein absolutes Recht. Artikel 22 der Verfassung und Artikel 8 der Europäischen Menschenrechtskonvention schließen eine Einmischung der Behörden in das Recht auf Achtung des Privat- und Familienlebens nicht aus, sofern eine solche durch eine ausreichend präzise gesetzliche Bestimmung vorgesehen ist, sie einem zwingenden gesellschaftlichen Bedürfnis in einer demokratischen Gesellschaft entspricht und sie im Verhältnis zu dem damit angestrebten rechtmäßigen Ziel steht.

Der Gesetzgeber besitzt diesbezüglich einen Ermessensspielraum. Dieser Ermessensspielraum ist jedoch nicht unbegrenzt: Damit eine Norm mit dem Recht auf Achtung des Privatlebens vereinbar ist, ist es erforderlich, dass der Gesetzgeber ein faires Gleichgewicht zwischen allen betroffenen Rechten und Interessen hergestellt hat.

B.15.1. Die Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union (nachstehend: Charta) haben hinsichtlich der Verarbeitung von personenbezogenen Daten eine analoge Tragweite wie Artikel 8 der Europäischen Menschenrechtskonvention (EuGH, Große Kammer, 9. November 2010, C-92/09 und C-93/09, *Volker und Markus Schecke GbR u.a.*) und wie Artikel 22 der Verfassung. Das Gleiche gilt für Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union sowie für Artikel 17 des Internationalen Paktes über bürgerliche und politische Rechte.

B.15.2. Der Gerichtshof der Europäischen Union ist der Auffassung, dass sich die Achtung des Rechts auf Privatleben hinsichtlich der Verarbeitung personenbezogener Daten auf jede Information erstreckt, die eine bestimmte oder bestimmbare natürliche Person betrifft (EuGH, Große Kammer, 9. November 2010, vorerwähnt, Randnr. 52; 16. Januar 2019, C-496/17, *Deutsche Post AG*, Randnr. 54). Daher urteilt der Gerichtshof ebenso wie der Europäische Gerichtshof für Menschenrechte, dass die digitalen Fingerabdrücke personenbezogene Daten darstellen, « da sie objektiv unverwechselbare Informationen über natürliche Personen enthalten und deren genaue Identifizierung ermöglichen » (EuGH, 17. Oktober 2013, C-291/12, *Schwarz gegen Stadt Bochum*, Randnr. 27; 3. Oktober 2019, C-70/18, *Staatssecretaris van Justitie en Veiligheid gegen A, B und C*, Randnr. 55).

B.15.3. Artikel 52 Absatz 1 der Charta bestimmt:

« 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.15.4. Mit dem vorerwähnten Urteil *Schwarz gegen Stadt Bochum* vom 17. Oktober 2013 hat der Gerichtshof entschieden, dass die Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 « über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten » (nachstehend: Verordnung (EG) Nr. 2252/2004) Nr. 2252/2004), die die Abnahme von digitalen Fingerabdrücken und ihre Speicherung in den Reisepässen auferlegt, mit dem Recht auf Achtung des Privatlebens und mit dem Recht auf Schutz personenbezogener Daten vereinbar ist.

B.16.1. Artikel 5 der Datenschutz-Grundverordnung bezieht sich auf die Grundsätze für die Verarbeitung personenbezogener Daten:

« 1. Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (‘ Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz ’);

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken (‘ Zweckbindung ’);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (‘ Datenminimierung ’);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden (‘ Richtigkeit ’);

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist;

personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden (‘ Speicherbegrenzung ’);

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (‘ ntegrität und Vertraulichkeit ’);

2. Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können (‘ Rechenschaftspflicht ’) ».

B.16.2. Artikel 6 der Datenschutz-Grundverordnung bezieht sich auf die Rechtmäßigkeit der Verarbeitung:

« 1. Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

2. Die Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 Buchstaben c und e beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX.

3. Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e wird festgelegt durch

a) Unionsrecht oder

b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.

Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX. Das Unionsrecht oder das Recht der Mitgliedstaaten müssen ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.

4. Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt, so berücksichtigt der Verantwortliche — um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist — unter anderem

a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,

b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,

c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden,

d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,

e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann ».

B.16.3. Artikel 9 der Datenschutz-Grundverordnung bezieht sich auf die Verarbeitung besonderer Kategorien personenbezogener Daten:

« 1. Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

2. Absatz 1 gilt nicht in folgenden Fällen:

[…]

g) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich,

[…]

3. […]

4. Die Mitgliedstaaten können zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist ».

B.16.4. Artikel 25 der Datenschutz-Grundverordnung bezieht sich auf den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen:

« 1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen - wie z. B. Pseudonymisierung - trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung

aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

2. Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

3. Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Anforderungen nachzuweisen ».

B.16.5. Artikel 32 der Datenschutz-Grundverordnung bezieht sich auf die Sicherheit der Verarbeitung:

1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

2. Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch - ob unbeabsichtigt oder unrechtmäßig - Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

3. Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

4. Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet ».

Was die Prüfung der Beschwerdegründe betrifft

B.17. Aus der Prüfung der Klagegründe geht hervor, dass die klagenden Parteien mehrere Aspekte der angefochtenen Bestimmung bemängeln, die der Gerichtshof in der folgenden Reihenfolge prüft:

1. Die Abnahme von zwei digitalen Fingerabdrücken und die Speicherung ihres digitalen Bildes auf dem Personalausweis, einschließlich der technischen Aspekte;

2. Die zentralisierte Speicherung des digitalen Bildes der Fingerabdrücke für die Zwecke der Herstellung und Ausstellung des Personalausweises;

3. Das Lesen des digitalen Bildes der Fingerabdrücke.

1. Die Abnahme von zwei digitalen Fingerabdrücken und die Speicherung ihres digitalen Bildes auf dem Personalausweis, einschließlich der technischen Aspekte

B.18. Die klagenden Parteien machen geltend, dass die angefochtene Bestimmung dadurch, dass sie die Abnahme von zwei digitalen Fingerabdrücken und die Speicherung ihres digitalen Bildes auf dem Personalausweis vorschreibt, eine Einmischung in das Recht auf Achtung des Privatlebens und in das Recht auf Schutz personenbezogener Daten zur Folge habe, die kein legitimes Ziel verfolge. Die verfolgten Ziele stellten in jedem Fall keinen Grund eines erheblichen öffentlichen Interesses im Sinne von Artikel 9 Absatz 2 Buchstabe g der Datenschutz-Grundverordnung dar.

Die klagenden Parteien führen an, dass die angefochtene Bestimmung gegen das durch die in den Klagegründen erwähnten Bestimmungen gewährleistete Legalitätsprinzip verstoße, da

die Ermächtigung des Königs in Bezug auf die Ausführung der angefochtenen Bestimmung nicht ausreichend präzise beschrieben sei und deren erforderliche wesentliche Elemente nicht alle festlege.

Sie machen insbesondere geltend, dass der Prozess der Herstellung und Ausstellung der Personalausweise nicht ausreichend von der angefochtenen Bestimmung beschrieben werde. So bestimme diese weder die verwendete Technologie noch die technischen Maßnahmen zum Schutz der digitalen Fingerabdrücke auf dem Mikrochip, was es daher ermögliche, die digitalen Fingerabdrücke kontaktlos und aus der Ferne ohne Wissen des Inhabers des Ausweises zu lesen sowie sie mit bloßem Auge zu lesen. Sie bestimme auch nicht die Technik oder Methode, mit der der digitale Fingerabdruck erfasst und gelesen werde. In der angefochtenen Bestimmung sei auch kein Grundsatz einer Sanktion im Fall der Nichteinhaltung der Vorschriften zur Herstellung vorgesehen, insbesondere, was die obligatorische Löschung der Daten nach Abschluss dieses Prozesses betreffe. Schließlich erlaube die angefochtene Bestimmung die Speicherung der Daten nach der Herstellung des Personalausweises.

Die klagenden Parteien machen ebenfalls geltend, dass die Einmischung weder notwendig sei, noch im Verhältnis zu den verfolgten Zielen stehe. Sie führen an, dass die Personalausweise heutzutage ausreichend sicher und schwer zu fälschen seien. Außerdem seien die Zahlen zum Betrug, die in den Vorarbeiten vorgebracht wurden, geringfügig und könnten die Abnahme von digitalen Fingerabdrücken und deren Speicherung auf dem Personalausweis von allen Belgiern ab zwölf Jahren, was zu einer « Vorkriminalisierung » aller betroffenen Personen führe und ein erhebliches Missbrauchsrisiko nach sich ziehe, nicht rechtfertigen. Schließlich machen die klagenden Parteien geltend, dass neben dem Umstand, dass die digitalen Fingerabdrücke nicht unfehlbar seien, alternative Maßnahmen bestünden, die weniger stark in das Recht auf Achtung des Privatlebens eingreifen.

B.19.1. Wie in B.14.1 erwähnt, schließt das Recht auf Achtung des Privatlebens den Schutz personenbezogener Daten und persönlicher Informationen ein, zu denen insbesondere digitale Fingerabdrücke gehören.

Dadurch, dass sie die Abnahme von zwei digitalen Fingerabdrücken und die Speicherung ihres digitalen Bildes auf dem Personalausweis vorsieht, hat die angefochtene Bestimmung also eine Einmischung in das Recht auf Achtung des Privatlebens und in das Recht auf Schutz

personenbezogener Daten zur Folge, wie sie durch die in B.13 bis B.16 zitierten Bestimmungen gewährleistet werden.

B.19.2. Wie in B.14.2 darüber erwähnt, ist eine solche Einmischung nur zulässig, wenn sie durch eine ausreichend präzise gesetzliche Bestimmung vorgesehen ist, wenn sie einem zwingenden gesellschaftlichen Bedürfnis in einer demokratischen Gesellschaft entspricht und wenn sie im Verhältnis zu dem damit angestrebten rechtmäßigen Ziel steht. Aus Artikel 52 Absatz 1 der Charta geht außerdem hervor, dass die Einmischung den Wesensgehalt der betroffenen Rechte achten muss und dass unter Wahrung des Grundsatzes der Verhältnismäßigkeit Einschränkungen nur vorgenommen werden dürfen, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

Da die digitalen Fingerabdrücke biometrische Daten im Sinne von Artikel 4 Nummer 14 der Datenschutz-Grundverordnung darstellen und die angefochtene Bestimmung die Durchführung von mehreren Verarbeitungen dieser Daten im Sinne von Artikel 4 Nummer 2 derselben Datenschutz-Grundverordnung voraussetzt, muss die Einmischung ebenfalls den von Artikel 9 der Datenschutz-Grundverordnung festgelegten Bedingungen genügen. Nach Artikel 11 Absatz 1 der Verordnung (EU) 2019/1157 unterliegen die personenbezogenen Daten, die in Anwendung der Verordnung verarbeitet werden, der Datenschutz-Grundverordnung.

Artikel 9 Absatz 2 Buchstabe g der Datenschutz-Grundverordnung gestattet die Verarbeitung von sensiblen personenbezogenen Daten wie zum Beispiel biometrischen Daten, wenn sie auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist.

B.20.1. Laut der Begründung zielt die angefochtene Bestimmung darauf ab, die möglichst effiziente Identifizierung von Personen zu ermöglichen, um die Bekämpfung des Identitätsbetrugs zu verstärken:

« À l'heure actuelle, il s'impose de prendre les mesures nécessaires en vue d'identifier le plus efficacement possible les individus.

Sur le même principe que le passeport et pour renforcer la lutte contre la fraude à l'identité, le présent article prévoit que la puce des cartes d'identité intégrera les empreintes digitales, plus précisément l'image numérisée des empreintes digitales de l'index de la main gauche et celui de la main droite.

Cet enregistrement sur la carte d'identité permettra par exemple aux services de police de vérifier l'exactitude du lien entre une carte d'identité et le porteur de celle-ci » (*Parl. Dok.*, Kammer, 2017-2018, DOC 54-3256, S. 34).

Der Bericht des Ausschusses für Inneres, Allgemeine Angelegenheiten und öffentlichen Dienst der Kammer legt dar:

« Il sera ainsi possible de contrôler les cartes d'identité, comme les passeports, lors du franchissement des frontières intérieures de l'Europe » (*Parl. Dok.*, Kammer, 2018-2019, DOC 54-3256/003, S. 16).

Mit der angefochtenen Bestimmung soll konkret der Betrug, der auf einer Ähnlichkeit beruht (auch als « *Look-alike* »-Betrug bezeichnet), und die betrügerische Erlangung von echten Papieren bekämpft werden. Diese zwei Betrugsarten würden zunehmen, während der klassische Betrug, der in der Totalfälschung von Ausweisdokumenten bestehe, abnimmt (ebenda, S. 31).

Die angefochtene Bestimmung trägt so dazu bei, Straftaten im Zusammenhang mit dem Identitätsbetrug vorzubeugen, wobei dieser « in den meisten Fällen mit einer anderen Straftat verbunden ist (Menschenhandel, Betrug, Kriminelle, die unter dem Radar bleiben wollen, Personen, die zum Kämpfen nach Syrien gereist sind und die versuchen, illegal nach Europa einzureisen, potenzielle Terroristen usw.) » (ebenda, S. 33).

Wie in B.1.4 erwähnt, wird mit der angefochtenen Bestimmung das gleiche Ziel verfolgt wie mit dem Vorschlag für eine Verordnung, aus der die Verordnung (EU) 2019/1157 geworden ist, wie es der Minister der Sicherheit und des Innern im Ausschuss der Kammer bestätigt hat:

« De manière générale, [l'Autorité de protection des données] se demande quel est l'objectif de cette mesure. Ce dernier est pourtant indiqué dans l'exposé des motifs ainsi que dans la justification par la Commission européenne de la proposition de

règlement COM (2018) 212 relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des titres de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation.

Le ministre renvoie également à la communication de la Commission au Parlement européen et au Conseil de 2016 (COM 2016/790) relative au Plan d'action visant à renforcer la réponse de l'UE aux fraudes liées aux documents de voyage. Le dépôt de l'actuelle proposition de règlement de la Commission européenne découle directement de ce document. On peut y lire ce qui suit:

‘ Les documents de voyage de l'UE sont très prisés des fraudeurs. Au moins trois quarts des documents frauduleux détectés aux frontières extérieures, mais également dans l'espace sans contrôle aux frontières intérieures, imitent certains documents délivrés par des États membres de l'UE et des pays associés à l'espace Schengen. Selon des rapports récents du corps européen de garde-frontières et de garde-côtes, les cartes nationales d'identité d'un moindre degré de sécurité délivrées par des États membres sont les faux documents les plus fréquemment détectés en ce qui concerne les déplacements à l'intérieur de l'espace Schengen. La fraude basée sur la ressemblance (où la personne en possession du document n'est qu'un sosie du véritable titulaire) continue d'augmenter et demeurait, au deuxième trimestre 2016, le type de fraude le plus fréquemment signalé. L'obtention de documents authentiques à partir de faux documents ‟ sources ” (certificats de naissance, de mariage ou de décès) reste l'une des plus grandes menaces car elle est extrêmement difficile à détecter. ’

Selon le rapport 2016 du corps européen de garde-frontières et de garde-côtes, les faits d'imposture et d'obtention frauduleuse de documents authentiques ont respectivement augmenté de 4 % et 76 % entre le premier trimestre 2015 et le premier trimestre 2016, tandis que la fraude consistant en la falsification de documents a diminué (-8 %).

Nous apprenons ainsi que trois quarts des documents frauduleux détectés aux frontières extérieures sont d'origine européenne. Il s'avère de même que la fraude basée sur la ressemblance et l'obtention frauduleuse de documents authentiques (par le biais des communes) ne cessent de s'accroître, l'augmentation atteignant respectivement 4 % et 76 % en 2015 et 2016.

Comment cela se traduit-il en Belgique, l'un des 15 États membres à rendre la carte d'identité obligatoire ? Depuis l'introduction des nouvelles cartes d'identité électroniques en 2005 et l'utilisation d'éléments de sécurité de pointe, le nombre de cartes falsifiées a considérablement baissé. La falsification d'une carte d'identité électronique a été rendue si difficile qu'un glissement s'est opéré vers la fraude basée sur la ressemblance et l'obtention frauduleuse de documents authentiques par le biais de la commune, sur la base d'un faux nom ou d'une fausse photo. Au cours de la période 2006-2010, les falsifications ont reculé de 62 % à 29 %, la fraude intellectuelle (basée sur la ressemblance et l'obtention frauduleuse de documents authentiques) passant de 38 % à 71 %.

Les chiffres du SPOC fraude à l'identité nationale (mis en place au sein de la task force fraude à l'identité) concernant le nombre de dossiers de fraude potentielle à l'identité ouverts en 2016, 2017 et jusqu'en septembre 2018 sont éloquents. Il est passé de 402 dossiers en 2016 à 796 en 2017 et à 955 dossiers déjà en 2018.

À cet égard, il est frappant de constater la différence entre les cartes d'identité électroniques et les passeports et les cartes pour étrangers sur lesquels les empreintes digitales figurent déjà. En 2016, on a dénombré 230 dossiers de fraude à l'identité à l'aide d'une carte d'identité électronique, en 2017, 467 et en 2018, déjà 566. Pour ce qui est des passeports et des cartes pour étrangers, le nombre de dossiers s'élevait respectivement à 76 et 13 en 2016, 60 et 19 en 2017 et 97 et 7 en 2018. Il ressort donc des chiffres que la fraude aux titres pourvus d'empreintes digitales recule par rapport à la carte d'identité électronique qui devient un maillon faible et est davantage utilisée pour la fraude à l'identité.

Les dossiers du SPOC national ' fraude à l'identité ' se basent sur les cas signalés par les communes. Les services de police observent toutefois également une augmentation du nombre de tentatives de fraude fondées sur la ressemblance et de tentatives d'obtention frauduleuse d'un document authentique établi au nom d'une autre personne. En 2013, le service de police ' faux documents ' a été amené à enquêter sur 96 cas. Ce chiffre est passé à 340 en 2017 et on enregistrait déjà 159 cas au premier semestre 2018. Il convient de souligner à nouveau que ces statistiques reprennent uniquement les cas qui ont été découverts. Entre 2013 et le premier semestre 2018, 2 027 cas ont été enregistrés lors de contrôles de police effectués à la frontière.

Si l'on y ajoute les 1 374 dossiers instruits par le service ' faux documents ', on obtient au total 3 401 cas pour cette période. On constate également qu'au cours de la même période, la fraude fondée sur la ressemblance et l'acquisition frauduleuse de documents authentiques sont passées de 20 à 30 % du nombre total de cas de fraude à l'identité perpétrés par le biais de documents.

Or, la fraude fondée sur la ressemblance et l'acquisition frauduleuse de documents authentiques sont précisément des formes de fraude qui exploitent les points faibles de la photographie. Dans le premier cas, le fraudeur utilise la carte d'une personne qui lui ressemble ou à laquelle il fait en sorte de ressembler (il peut s'agir d'une carte volée ou trouvée ou encore d'une carte qui a été donnée). Dans le second, le fraudeur fournit sa propre photo pour faire établir un document au nom d'une autre personne. Il affirme par exemple avoir égaré sa carte d'identité électronique et introduit une demande pour en obtenir une nouvelle. En l'absence d'éléments biométriques supplémentaires comme l'empreinte digitale, ce type de fraude est impossible à déceler. La photo ne suffit pas à elle seule à garantir rapidement et de façon efficace qu'il s'agit bien de la véritable identité de l'intéressé » (ebenda, SS. 30-32).

Mit der angefochtenen Bestimmung wird daher, wenn auch vorzeitig die Verordnung (EU) 2019/1157 umgesetzt, die - wie in B.2.1 erwähnt - « die Erhöhung der Sicherheit und die Erleichterung der Ausübung des Rechts auf Freizügigkeit von Unionsbürgern und ihren Familienangehörigen » (Erwägungsgrund 46) und die Verringerung des Risikos des Identitätsbetrugs (Erwägungsgrund 18) bezweckt.

B.20.2. Diese Ziele sind legitim, da sie darauf abzielen, die Rechte und Freiheiten anderer zu schützen. Sie stellen überdies dem Gemeinwohl dienende Ziele, die von der Union anerkannt sind, dar.

Der Gerichtshof der Europäischen Union hat nämlich entschieden, dass die Verordnung (EG) Nr. 2252/2004, die die Aufnahme von zwei digitalen Fingerabdrücken in die Reisepässe vorsieht und deren Ziele sind, einerseits der Fälschung von Reisepässen vorzubeugen, und andererseits ihre betrügerische Verwendung zu verhindern, und zwar insbesondere um die illegale Einreise von Personen in das Unionsgebiet zu verhindern, eine von der Union anerkannte dem Gemeinwohl dienende Zielsetzung verfolgt (EuGH, 17. Oktober 2013, C-291/12, *Schwarz gegen Stadt Bochum*, Randnrn. 36-38; siehe auch EuGH, 7. November 2013, C-225/12, *Demir*, Randnr. 41; 3. Oktober 2019, C-70/18, *Staatssecretaris van Justitie en Veiligheid c. A, B und C*, Randnrn. 46-49).

Die vorerwähnten Ziele stellen ebenfalls Gründe eines erheblichen öffentlichen Interesses im Sinne von Artikel 9 Absatz 2 Buchstabe g der Datenschutz-Grundverordnung dar, was sich zudem aus der Annahme der Verordnung (EU) 2019/1157 durch den europäischen Gesetzgeber ergibt.

B.21.1. Die angefochtene Bestimmung ist im Hinblick auf die Verwirklichung der angestrebten Ziele sachdienlich, da die Speicherung des digitalen Bildes der Fingerabdrücke auf dem Personalausweis einerseits geeignet ist, die Gefahr der Fälschung von Personalausweisen zu verringern und die Aufgabe der mit der Überprüfung von deren Authentizität insbesondere an den Grenzen betrauten Stellen zu erleichtern, und andererseits vor der betrügerischen Verwendung von Personalausweisen zu schützen, wie der Gerichtshof bezüglich Reisepässen zur Verordnung (EG) Nr. 2252/2004 geurteilt hat (EuGH, 17. Oktober 2013, C-291/12, *Schwarz gegen Stadt Bochum*, Randnrn. 41-45).

Das Fehlen einer völligen Zuverlässigkeit des Verfahrens und die damit einhergehende Unmöglichkeit, es völlig auszuschließen, dass bestimmte Fälle von Ähnlichkeitsbetrug nicht erkannt werden, führen nicht zu einer anderen Schlussfolgerung. So hat der Gerichtshof der Europäischen Union in seinem vorerwähnten Urteil *Schwarz gegen Stadt Bochum* entschieden, dass « es nicht entscheidend darauf ankommt, dass die […] Methode nicht völlig zuverlässig ist. Zum einen reicht es nämlich aus, dass diese Methode, auch wenn sie die Akzeptanz unbefugter Personen nicht völlig ausschließt, die Gefahr solcher Akzeptanzen, die bestehen würde, wenn sie nicht angewandt würde, doch erheblich vermindert » (Randnr. 43).

B.21.2. Der Umstand, dass bestimmte Formen des Identitätsbetrugs die Verwendung eines Personalausweises nicht voraussetzen, ändert nichts an der Realität des Phänomens des Ähnlichkeitsbetrugs mittels eines Personalausweises, der mit der angefochtenen Bestimmung bekämpft werden soll, indem es den Stellen, die dazu ermächtigt sind, erlaubt wird, das digitale Bild von zwei Fingerabdrücken zu lesen.

B.21.3. Entgegen der Auffassung der klagenden Parteien kann der Umstand, dass der Mikrochip, der das digitale Bild der Fingerabdrücke enthält, beschädigt werden kann, ohne dass dadurch die Verwendung des Personalausweises durch seinen Inhaber verhindert wird – unterstellt dies wäre technisch erwiesen –, die Wirksamkeit der angefochtenen Bestimmung nicht in Frage stellen. Die Neutralisierung des Mikrochips hätte zur Folge, dass die zum Lesen des digitalen Bildes der Fingerabdrücke befugten Stellen Verdacht schöpfen würden, was sie dazu veranlassen würde, eine genauere Prüfung der Identität der betroffenen Person vorzunehmen, was wahrscheinlich nicht das Ziel ist, das von den Personen verfolgt wird, die sich die Identität eines Dritten aneignen.

B.22.1. Artikel 22 der Verfassung behält dem zuständigen Gesetzgeber die Befugnis vor, festzulegen, in welchen Fällen und unter welchen Bedingungen das Recht auf Achtung des Privatlebens beeinträchtigt werden kann. Somit garantiert er jedem Bürger, dass eine Einmischung in die Ausübung dieses Rechts nur aufgrund von Regeln erfolgen darf, die durch eine demokratisch gewählte beratende Versammlung angenommen wurden.

Eine Ermächtigung einer anderen Gewalt steht jedoch nicht im Widerspruch zum Legalitätsprinzip, sofern die Ermächtigung ausreichend präzise beschrieben ist und sich auf die Ausführung von Maßnahmen bezieht, deren wesentliche Elemente vorher durch den Gesetzgeber festgelegt wurden.

B.22.2. Neben dem formalen Erfordernis der Legalität wird durch Artikel 22 der Verfassung in Verbindung mit Artikel 8 der Europäischen Menschenrechtskonvention und mit den Artikeln 7, 8 und 52 der Charta ebenfalls die Verpflichtung auferlegt, dass die Einmischung in das Recht auf Achtung des Privatlebens und das Recht auf den Schutz personenbezogener Daten deutlich und ausreichend präzise formuliert wird, damit es möglich ist, die Fälle vorherzusehen, in denen der Gesetzgeber eine solche Einmischung erlaubt.

Auf dem Gebiet des Datenschutzes bedeutet dieses Erfordernis der Vorhersehbarkeit, dass ausreichend präzise vorgesehen werden muss, unter welchen Umständen Verarbeitungen von personenbezogenen Daten erlaubt sind (EuGHMR, Große Kammer, 4. Mai 2000, *Rotaru gegen Rumänien*, § 57; Große Kammer, 4. Dezember 2008, *S. und Marper gegen Vereinigtes Königreich*, § 99).

Jeder muss somit eine ausreichend klare Vorstellung von den verarbeiteten Daten, den von einer bestimmten Datenverarbeitung betroffenen Personen und den Bedingungen und Zwecken dieser Verarbeitung haben.

B.22.3. Es ist also zu prüfen, ob einerseits die Ermächtigungen des Königs dem Legalitätsprinzip entsprechen und ob andererseits unter Berücksichtigung der verschiedenen in der angefochtenen Bestimmung enthaltenen Elemente jeder, der der Pflicht unterliegt, im Besitz eines Personalausweises zu sein, ausreichend präzise wissen kann, unter welchen Bedingungen die Abnahme seiner digitalen Fingerabdrücke und die Speicherung ihres digitalen Bildes auf dem Personalausweis, gegebenenfalls nach den vom König bestimmten Modalitäten, stattfinden. Da diese beiden Fragen untrennbar miteinander verbunden sind, prüft der Gerichtshof sie zusammen.

B.23.1. Wie in B.1.3 erwähnt, bestimmt die angefochtene Bestimmung die Daten, die Gegenstand der strittigen Maßnahme sind, nämlich das digitale Bild von zwei Fingerabdrücken, die Höchstdauer der Speicherung dieser Information zum Zweck der Herstellung und Ausstellung des Personalausweises, den Umstand, dass die Daten nur auf dem Personalausweis gespeichert werden und dass sie ausschließlich elektronisch lesbar sind, sowie die Stellen, die befugt sind, sie zu lesen.

Im Gegensatz zu dem, was die klagenden Parteien anführen, geht aus dem Wortlaut der angefochtenen Bestimmung eindeutig hervor, dass das digitale Bild der Fingerabdrücke auf dem Personalausweis nur elektronisch lesbar und nicht mit bloßem Auge erkennbar ist und dass diese Information nach dem Zeitraum, der für die Herstellung und Ausstellung des Personalausweises notwendig ist und der höchstens drei Monate betragen darf, endgültig vernichtet werden muss, ohne Möglichkeit der späteren Wiederherstellung der Daten.

Der Gesetzgeber hat die dem König erteilte Ermächtigung ebenfalls darauf beschränkt, einerseits die Bedingungen und Modalitäten für die Erfassung des digitalen Bildes der Fingerabdrücke und andererseits die Form und Modalitäten der Herstellung, Ausstellung und Verwendung des Personalausweises zu bestimmen. Die Umsetzung dieser Ermächtigungen muss nach Stellungnahme der Datenschutzbehörde und im ersten Fall durch einen im Ministerrat beratenen Erlass erfolgen.

B.23.2. Aus dem Vorstehenden ergibt sich, dass der Gesetzgeber die wesentlichen Elemente der Maßnahmen, deren Ausführung er dem König überträgt, bestimmt hat und dass diese Ermächtigungen somit nicht zu dem in Artikel 22 der Verfassung enthaltenen Legalitätsprinzip im Widerspruch stehen.

Wie der Ministerrat anführt, betreffen die Elemente, die nach Auffassung der klagenden Parteien hätten vom Gesetzgeber selbst geregelt werden müssen, nämlich die Art des verwendeten Mikrochips, die technischen Maßnahmen zur Sicherung und zum Lesen und die konkreten Modalitäten zur Löschung der Daten zum Zeitpunkt der Ausstellung des Personalausweises, Aspekte der Ausführung oder rein technische Aspekte, die aus diesem Grund unter Einhaltung übergeordneter Normen und insbesondere der Verordnung (EU) 2019/1157 und der zu deren Ausführung getroffenen Entscheidungen sowie der Datenschutz-Grundverordnung vom König geregelt werden können.

Es obliegt gegebenenfalls dem zuständigen Richter zu prüfen, ob die Nutzung der vorerwähnten Ermächtigungen durch den König den in den Klagegründen angeführten Verfassungsbestimmungen und Bestimmungen des Unionsrechts entsprechen, wie sie in B.13 bis B.16 präzisiert wurden.

Schließlich ist in Anbetracht der Sanktionen, die bereits insbesondere durch Artikel 7 des Gesetzes vom 19. Juli 1991 in Verbindung mit Artikel 6*quater* desselben Gesetzes vorgesehen sind, nicht erkennbar, dass der Gesetzgeber zur Beachtung des Legalitätsprinzips eine spezifische Sanktion für den Fall eines Verstoßes gegen die von der angefochtenen Bestimmung festgelegten Regeln hätte einführen müssen.

B.24. Die Personen, die der Pflicht unterliegen, im Besitz eines Personalausweises zu sein, können außerdem ausreichend präzise die Bedingungen kennen, unter denen die

Abnahme der digitalen Fingerabdrücke und die Speicherung ihres digitalen Bildes auf dem Personalausweis, gegebenenfalls nach den vom König bestimmten Modalitäten, stattfinden.

B.25.1. Der Gerichtshof prüft nun die Notwendigkeit und die Verhältnismäßigkeit der Einmischung.

B.25.2. Im Rahmen dieser Prüfung ist zu prüfen, ob der Eingriff nicht über das hinausgeht, was zur Erreichung der verfolgten Ziele erforderlich ist und insbesondere ob es Maßnahmen gibt, die weniger stark in die betreffenden Rechte eingreifen und trotzdem den Zielen der in Rede stehenden Regelung wirksam dienen (EuGH, 17. Oktober 2013, C-291/12, *Schwarz gegen Stadt Bochum*, Randnrn. 46 und 47).

B.25.3. Bei der Beurteilung der Verhältnismäßigkeit von Maßnahmen in Bezug auf die Verarbeitung personenbezogener Daten sind u. a. deren automatisierter Charakter, die verwendeten Techniken, der Genauigkeitsgrad, die Relevanz, der gegebenenfalls übermäßige 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, und das etwaige Vorhandensein von Garantien zur Vermeidung einer falschen Nutzung und von Missbrauch der verarbeiteten personenbezogenen Daten durch öffentliche Behörden zu berücksichtigen (Entscheid Nr. 108/2016 vom 14. Juli 2016, B.12.2; Entscheid Nr. 29/2018 vom 15. März 2018, B.14.4; Entscheid Nr. 27/2020 vom 20. Februar 2020, B.8.3; EuGHMR, Große Kammer, 4. Mai 2000, *Rotaru gegen Rumänien*, § 59; Entscheidung, 29. Juni 2006, *Weber und Saravia gegen Deutschland*, § 135; 28. April 2009, *K.H. e.a. gegen Slowakei*, §§ 60-69; Große Kammer, 4. Dezember 2008, *S. und Marper gegen Vereinigtes Königreich*, §§ 101-103, 119, 122 und 124; 18. April 2013, *M.K. gegen Frankreich*, §§ 37 und 42-44; 18. September 2014, *Brunet gegen Frankreich*, §§ 35-37; 12. Januar 2016, *Szabó und Vissy gegen Ungarn*, § 68; EuGH, Große Kammer, 8. April 2014, C-293/12, *Digital Rights Ireland Ltd*, und C-594/12, *Kärntner Landesregierung u.a.*, Randnrn. 56-66).

B.26.1. Die klagenden Parteien machen geltend, dass Personalausweise nicht mit Reisepässen vergleichbar seien, sodass das vorerwähnte Urteil *Schwarz gegen Stadt Bochum* vom 17. Oktober 2013 des Gerichtshofs der Europäischen Union nicht entsprechend anwendbar sei. Ihrer Auffassung nach sind Personalausweise und Reisepässe grundverschiedene Dokumente. Die Beurteilung der Notwendigkeit und der Verhältnismäßigkeit der Einmischung müsse daher nach unterschiedlichen Kriterien erfolgen.

B.26.2. In seiner Stellungnahme zum Vorschlag für eine Verordnung, der der Verordnung (EU) 2019/1157 zugrunde lag, hat der Europäische Datenschutzbeauftragte (EDSB) folgende Anmerkungen gemacht:

« 22. In diesem Zusammenhang unterstützt der EDSB das Ziel der Kommission, die Freizügigkeit zu erleichtern. Dessen ungeachtet weist der EDSB darauf hin, dass die beiden Arten von Dokumenten – Personalausweise und Reisepässe – sowohl aus rechtlicher Sicht als auch im Hinblick auf ihre Verwendung in der Praxis höchst unterschiedlich sind. Auch wenn sie als Reisedokumente im Kontext der Freizügigkeit verwendet werden, können nationale Personalausweise, anders als Pässe, nur für Reisen in EU-Mitgliedstaaten und diejenigen Drittländer verwendet werden, die EU-Bürgern die Einreise mit ihrem nationalen Personalausweis gestatten. Vor diesem Hintergrund fragt sich der EDSB, welchen Mehrwert die Aufnahme biometrischer Daten in die Personalausweise bringt, da diese bei Reisen zwischen den EU-Mitgliedstaaten nicht routinemäßig kontrolliert werden.

23. Noch viel wichtiger ist, dass Personalausweise für eine Vielfalt von Zwecken genutzt werden, die über die Ausübung des Rechts auf Freizügigkeit in Verbindung mit der Unionsbürgerschaft weit hinausgehen, nämlich für die Interaktion mit Verwaltungen im Heimatland eines Bürgers und für die Interaktion mit einer Vielzahl von Akteuren aus dem gesamten privaten Sektor (Banken, Fluggesellschaften usw.). Des Weiteren, so die Folgenabschätzung zum Vorschlag, leben rund 15 Millionen EU-Bürger in einem anderen EU-Mitgliedstaat und arbeiten 11 Millionen in einem anderen Mitgliedstaat.28 Hieraus schließt der EDSB, dass für die überwiegende Mehrheit der EU-Bürger die Hauptfunktionen von Personalausweisen nicht unmittelbar mit der Freizügigkeit zu tun haben. Man kann auch bei Weitem nicht davon ausgehen, dass alle potenziell von den Anforderungen des Vorschlags, ihre Fingerabdrücke in nationale Personalausweise aufnehmen zu lassen, betroffenen EU-Bürger ihr Recht auf Freizügigkeit tatsächlich wahrnehmen. Ganz im Gegenteil: Mobile EU-Bürger machen eine kleine Minderheit dieser potenziell von dem Vorschlag Betroffenen aus. Und selbst diejenigen, die ihr Recht auf Freizügigkeit tatsächlich ausüben, können dies häufig mit einem Pass und nicht mit einem Personalausweis tun und tun es auch. Die von der Kommission vorgetragene Rechtfertigung des Vorschlags ist daher nicht gänzlich überzeugend » (Stellungnahme 7/2018 des EDSB zu dem Vorschlag für eine Verordnung zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern und anderer Dokumente, 10. August 2018, S. 11).

Die Datenschutzbehörde hat ähnliche Bemerkungen geäußert:

« 25. L'assimilation des cartes d'identité avec les passeports qui est avancée par le gouvernement pour justifier cette mesure n'est pas acceptable : même si les cartes d'identité peuvent aussi être utilisées comme titre de voyage dans l'Union européenne, elles ne font actuellement pas l'objet de contrôle systématique pour ces voyages vu le principe de liberté de circulation au sein de l'Union européenne. De plus, contrairement aux passeports, les cartes d'identité nationale offrent beaucoup d'autres utilisations (applications du secteur privé, …). Ce point a également été relevé par le CEPD dans son avis. Compte tenu des différences entre les cartes d'identité et les passeports, l'introduction dans les cartes d'identité d'éléments de sécurité pouvant être considérés comme appropriés dans le cas des passeports ne peut être automatique, mais exige une réflexion et une analyse approfondie qui ne semble pas avoir été réalisée » (Stellungnahme Nr. 106/2018 vom 17. Oktober 2018, *Parl. Dok.*, Kammer, 2018-2019, DOC 54-3256/003, S. 120).

B.26.3. In den Vorarbeiten zu der angefochtenen Bestimmung heißt es, dass Personalausweise heutzutage als Reisedokumente verwendet werden:

« En effet, en ce qui concerne les passeports, ainsi que le rappelle la Commission, une réglementation européenne spécifique impose aux États membres de collecter les empreintes digitales.

Or, les cartes d'identité électroniques constituent elles aussi un document de voyage » (*Parl. Dok.*, Kammer, 2017-2018, DOC 54-3256/001, S. 34).

Auch weil « die Freizügigkeit […] das Recht ein[schließt], mit einem gültigen Personalausweis oder Reisepass Mitgliedstaaten zu verlassen und in Mitgliedstaaten einzureisen », hat der europäische Gesetzgeber die Verordnung (EU) 2019/1157 angenommen, mit der Mindeststandards für die Sicherheit und die Gestaltung von Personalausweisen im Hinblick auf « die Erhöhung der Sicherheit und die Erleichterung der Ausübung des Rechts auf Freizügigkeit von Unionsbürgern und ihren Familienangehörigen » eingeführt werden (siehe die Erwägungsgründe 2 und 46 dieser Verordnung).

Als Antwort auf die Bemerkungen der Datenschutzbehörde hat der Minister der Sicherheit und des Innern im Ausschuss der Kammer Folgendes erläutert:

« Dans le point 25 de son avis, l'APD conteste l'assimilation opérée entre le passeport et la carte d'identité électronique en tant que document de voyage. Le ministre observe à ce sujet que les premières e-gates équipées de lecteur d'empreintes digitales sont déjà en cours d'utilisation en Europe. Vu la législation européenne, elles seront de plus en plus utilisées. Si l'on souhaite encore utiliser la carte eID comme document de voyage, il faudra également s'y

adapter. Pour rappel, la carte eID est reconnue dans une cinquantaine de pays, même hors Europe. Le fait que la carte eID comporte encore d'autres fonctions est pertinent. Comme titre de voyage, la carte eID doit satisfaire aux mêmes normes. En effet, ce n'est pas parce que la libre circulation est en vigueur au sein de l'Union européenne que les autorités des autres États membres ou des citoyens ne peuvent pas demander la carte eID. Dans d'autres États membres, il peut également être demandé à une personne de prouver son identité au moyen de sa carte eID.

Lors d'un contrôle d'identité, il est essentiel de pouvoir en apporter la preuve rapidement et efficacement. Comme [le ministre] l'a expliqué plus haut, la photo seule ne suffit pas alors que la vérification des empreintes digitales enregistrées sur la carte offre bien ces garanties » (*Parl. Dok.*, Kammer, 2018-2019, DOC 54-3256/003, S. 34).

B.26.4. Auch wenn Personalausweise und Reisepässe Dokumente unterschiedlicher Art sind, die in der Regel zu unterschiedlichen Zwecken verwendet werden, ist festzustellen, dass Personalausweise heutzutage häufig als Reisedokumente innerhalb der Europäischen Union sowie im Rahmen von Reisen in eine begrenzte Zahl von Drittstaaten verwendet werden und dass sie in diesem Zusammenhang kontrolliert werden können. Personalausweise können ebenfalls als Ausgangsdokumente zur Erlangung eines Reisepasses dienen.

B.26.5. Eine Analogie zwischen Reisepässen und Personalausweisen herzustellen, ist somit zulässig. Es kann jedoch in Übereinstimmung mit dem EDSB und der Datenschutzbehörde angenommen werden, dass die Notwendigkeits- und Verhältnismäßigkeitsprüfung für Personalausweise strenger als für Reisepässe sein muss, insbesondere unter Berücksichtigung der Bedeutung von Ersteren bei alltäglichen Handlungen und ihres obligatorischen Besitzes, wie er in B.5.5 erwähnt wurde. Es obliegt also dem Gerichtshof zu prüfen, ob der Gesetzgeber im vorliegenden Fall eine Maßnahme ergriffen hat, die notwendig ist und im Verhältnis zum angestrebten Ziel steht. Im Rahmen dieser Prüfung berücksichtigt der Gerichtshof das vorerwähnte Urteil *Schwarz gegen Stadt Bochum* des Gerichtshofs der Europäischen Union.

B.27.1. In der Stellungnahme Nr. 19/2018 der Datenschutzbehörde (ehemaliger Ausschuss für den Schutz des Privatlebens) vom 28. Februar 2018 heißt es:

« 69. En l'absence de justification étayée et chiffrée sur des cas avérés de fraudes liés à l'insuffisance des moyens de non falsification dont est dotée notre actuelle carte d'identité susceptible d'attester du caractère éventuellement insuffisant de la photo comme moyen d'authentification du porteur de la carte et en l'absence de justification conforme aux exigences de l'article 9.2.g, la mesure apparait disproportionnée aux yeux de la Commission et non

conforme au RGPD » (Stellungnahme Nr. 19/2018 vom 28. Februar 2018, *Parl. Dok.*, Kammer, 2017-2018, DOC 54-3256/001, S. 220).

In ihrer Stellungnahme Nr. 106/2018 vom 17. Oktober 2018 heißt es außerdem:

« 23. Il n'y a toujours pas de réelle justification de la mesure envisagée dans l'exposé des motifs alors que cela a été demandé par l'Autorité de protection des données. Notre carte d'identité est déjà dotée de dispositifs de lutte contre la falsification (hologramme, …) ainsi que d'un élément biométrique (l'image faciale). En quoi concrètement est-ce insuffisant ? Quelles sont les statistiques dont disposent le gouvernement qui étayent la mesure envisagée ?

24. Dans son avis précité, le contrôleur européen à la protection des données (CEPD) a relevé que les statistiques ne plaident pas en faveur de la proposition de la Commission européenne qui va dans le même sens de celle du gouvernement. Des statistiques de l'agence européenne des gardes-frontières (frontex) ne révèlent qu'un constat de 38.870 cas d'utilisation frauduleuse de cartes d'identité nationale pour la période 2013-2017. De plus, on constate une baisse d'utilisation de titre de séjour frauduleux de personnes en provenance des pays tiers depuis 2015 de l'ordre d'au moins 11 %.

25. L'assimilation des cartes d'identité avec les passeports qui est avancée par le gouvernement pour justifier cette mesure n'est pas acceptable : même si les cartes d'identité peuvent aussi être utilisées comme titre de voyage dans l'Union européenne, elles ne font actuellement pas l'objet de contrôle systématique pour ces voyages vu le principe de liberté de circulation au sein de l'Union européenne. De plus, contrairement aux passeports, les cartes d'identité nationale offrent beaucoup d'autres utilisations (applications du secteur privé, …). Ce point a également été relevé par le CEPD dans son avis. Compte tenu des différences entre les cartes d'identité et les passeports, l'introduction dans les cartes d'identité d'éléments de sécurité pouvant être considérés comme appropriés dans le cas des passeports ne peut être automatique, mais exige une réflexion et une analyse approfondie qui ne semble pas avoir été réalisée.

[…]

27. L'interdiction de traitement des données biométriques ne peut être levée que sur base de l'article 9.2.g du RGPD qui exige non seulement le motif d'intérêt public important mais également notamment le caractère proportionné de la mesure face à l'objectif poursuivi et l'adoption de mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts des personnes concernées. Elles sont actuellement insuffisantes :

a. Le choix du gouvernement de collecter et stocker dans la puce de la carte l'image numérisée des empreintes digitales ne constitue selon le CEPD pas un choix des plus opportun au vu du risque d'usurpation d'identité en cas de hacking des données figurant sur la puce électronique de la carte. Il convient de revoir ce choix et de limiter les données dactyloscopiques stockées dans la puce des cartes d'identité à un sous-ensemble de caractéristiques extrait de l'image de l'empreinte digitale ou encore à des techniques biométriques sans trace (contour de la main, réseau veineux d'un doigt…).

b. Au lieu de déléguer au Roi la tâche de déterminer les autorités qui seront habilitées à lire les empreintes digitales, c'est au législateur au sens formel du terme qu'il appartient de le faire.

c. Il convient également que la loi précise que la lecture de ces données ne pourra se faire que pour vérifier l'authenticité de la carte d'identité. Il convient de prévoir déjà dans la loi des mesures de limitation pour les lecteurs de cartes qui permettront de lire les empreintes digitales.

d. Quelles seront les mesures de protection spécifiques qui seront prises pour limiter au maximum le risque de hacking du certificat de la carte d'identité qui contiendra l'image des empreintes digitales que ce soit tant en terme de sécurisation de la puce dans laquelle ces données seront insérées que de sécurisation des lecteurs de ces données ?

e. Quelles sont les mesures de protection pour la base de données temporaire qui reprendra de manière centralisée les empreintes digitales pendant 3 mois et quel en sera le responsable de traitement ?

f. Enfin, comme relevé par le CEPD, des enfants de moins de 14 ans ne devraient pas être soumis à cette mesure » (Stellungnahme Nr. 106/2019 vom 17. Oktober 2018, *Parl. Dok.*, Kammer, 2018-2019, DOC 54-3256/003, SS. 119-121).

B.27.2. Als Antwort auf diese ablehnenden Stellungnahmen hat der Minister der Sicherheit und des Innern im Ausschuss der Kammer die folgenden Erläuterungen abgegeben:

« Dans le point 24 de l'avis, l'APD [Autorité de protection des données] déclare ceci : ' on constate une baisse d'utilisation de titre de séjour frauduleux de personnes en provenance des pays tiers depuis 2015 de l'ordre d'au moins 11 % '. Le ministre rappelle à ce sujet que les empreintes digitales sur les cartes d'étranger n'ont commencé à être enregistrées qu'à partir de 2013, la généralisation s'est essentiellement déroulée début 2014. Dès lors, l'APD ne fait que confirmer que la mesure relative à l'intégration des empreintes digitales sur les cartes est efficace. Lors d'un contrôle des empreintes digitales sur la carte, les fraudeurs qui ont pour mode opératoire le ' lookalike ' tombent inéluctablement dans les mailles du filet.

Selon l'APD, ' des statistiques de l'agence européenne des gardes-frontières (frontex) ne révèlent qu'un constat de 38 870 cas d'utilisation frauduleuse de cartes d'identité nationale pour la période 2013-2017 '. Le ministre estime que ce nombre ne doit pas être sous-estimé. Ce sont en effet 38 870 personnes qui ont essayé d'entrer en Europe sous une fausse identité. Or, la fraude à l'identité est la plupart du temps associée à un autre délit (trafic d'êtres humains, fraude, criminels souhaitant rester sous le radar, personnes parties combattre en Syrie qui essaient d'entrer clandestinement en Europe, terroristes potentiels, etc.). Il ne s'agit par ailleurs que des cas qui ont été découverts. Si, tout comme pour les passeports et les cartes d'étranger, il est possible de faire une vérification au moyen des empreintes digitales, ces chiffres augmenteront sans nul doute.

[…]

Le ministre réagit ensuite aux observations formulées par l'APD dans le point 27 de son avis.

a) La procédure pour les empreintes digitales est exactement la même que pour les passeports et les titres de séjour pour les ressortissants de pays tiers. Dès lors, la remarque de l'APD ne manque pas d'étonner puisqu'elle impliquerait qu'un problème existe depuis fin 2012, moment où les premiers passeports biométriques ont commencé à être délivrés dans les communes. Pourtant, le ministre n'a eu connaissance d'aucun piratage de la puce. La puce répond aux normes de sécurité les plus élevées et n'est accessible que de manière limitée (inspection des frontières, police). Il se demande dès lors sur quelles informations concrètes se fonde cette remarque.

b) L'APD estime qu'il appartient au législateur de désigner les autorités habilitées à lire les empreintes digitales. Cette proposition peut être suivie. Actuellement, [le] projet de loi prévoit qu'il appartiendra au Roi, par un arrêté délibéré en Conseil des ministres et après avis de l'APD, de procéder à cette désignation.

[…]

c) Seuls les lecteurs de cartes habilités pourront lire les empreintes digitales. Dans la pratique, il s'agira des communes, des consulats et de la police. Cela sera confirmé lorsque le projet de loi sera adapté comme annoncé au point b).

d) L'APD se demande à quelles normes de sécurité devra répondre la puce se trouvant sur la carte eID afin d'éviter le piratage de la puce et le vol des empreintes digitales. On utilise la même norme internationale que pour les passeports et les titres de séjour pour les ressortissants de pays tiers. Les mêmes normes sont également d'application en ce qui concerne la base de données dans laquelle les empreintes digitales sont provisoirement enregistrées. Cette base de données a un accès limité avec habilitations personnelles pour les personnes autorisées. Cet accès se fait via des connexions sécurisées et il y a une journalisation de l'utilisation de celle-ci ainsi que des personnes qui l'utilisent.

e) Enfin, l'APD propose que les empreintes digitales ne soient collectées qu'à partir de l'âge de 14 ans. Cela serait toutefois discriminatoire par rapport aux ressortissants de pays tiers pour lesquels on doit enregistrer les empreintes digitales sur les cartes d'étranger dès l'âge de 12 ans » (*Parl. Dok.*, Kammer, 2018-2019, DOC 54-3256/003, SS. 33-36).

Es wurde ebenfalls präzisiert:

« Les empreintes digitales seront protégées par un certificat permettant une lecture uniquement par des lecteurs autorisés » (*Parl. Dok.*, Kammer, 2017-2018, DOC 54-3256/001, S. 35).

B.28. Zunächst kann aus den Zahlen, die bei den Vorarbeiten zu der angefochtenen Bestimmung vorgelegt wurden und die in B.20.1 zitiert wurden, nicht abgeleitet werden, dass das Phänomen des Ähnlichkeitsbetrugs und der betrügerischen Erlangung von echten Dokumenten, das mit der angefochtenen Bestimmung bekämpft werden soll, ob auf belgischer Ebene oder der Ebene der Europäischen Union, nur marginal wäre. So geht aus den Vorarbeiten

hervor, dass zwar die Zahlen über die Totalfälschung von Dokumenten in letzter Zeit abgenommen haben, dies aber nicht für die Zahlen zum Ähnlichkeitsbetrug gilt, wobei sich diese Zahlen nur auf die entdeckten Betrugsfälle beziehen (siehe insbesondere im gleichen Sinne: *Parl. Dok.*, Kammer, 2018-2019, DOC 54-3256/003, S. 33).

B.29. Was die Verhältnismäßigkeit der angefochtenen Bestimmung betrifft, ist nicht erkennbar – und die klagenden Parteien behaupten es auch nicht –, dass mit der angefochtenen Bestimmung der Wesensgehalt des Rechts auf Achtung des Privatlebens und des Rechts auf den Schutz personenbezogener Daten beeinträchtigt würde.

B.30. Wie der Gerichtshof der Europäischen Union im Hinblick auf Reisepässe in dem vorerwähnten Urteil *Schwarz gegen Stadt Bochum* zur Verordnung (EG) Nr. 2252/2004 festgestellt hat, besteht « die Erfassung nur in der Abnahme der Abdrücke zweier Finger […]. Diese Finger sind auch normalerweise den Blicken anderer Personen ausgesetzt, so dass die Erfassung kein Vorgang intimer Natur ist. Ebenso wie die Aufnahme des Gesichtsbilds führt auch sie nicht zu einer besonderen körperlichen oder psychischen Unannehmlichkeit für den Betroffenen » (Randnr. 48; siehe auch EuGH, 3. Oktober 2019, C-70/18, *Staatssecretaris van Justitie en Veiligheid gegen A, B und C*, Randnr. 58).

B.31.1. Mit der angefochtenen Bestimmung wird kein zentrales Register der digitalen Fingerabdrücke von allen Besitzern eines Personalausweises eingerichtet. Vorbehaltlich der Speicherung des digitalen Bildes der Fingerabdrücke für die Zwecke der Herstellung und Ausstellung des Personalausweises während einer Dauer von höchstens drei Monaten beschränkt sich die angefochtene Bestimmung darauf, das digitale Bild von zwei Fingerabdrücken in den Personalausweis und nur in diesen aufzunehmen, wie es in den Vorarbeiten bestätigt wurde (*Parl. Dok.*, Kammer, 2018-2019, DOC 54-3256/003, S. 16).

Entgegen der Auffassung der klagenden Parteien hat die angefochtene Bestimmung, indem sie auf die Bekämpfung des Ähnlichkeitsbetrugs abzielt, also weder eine « Vorkriminalisierung » von sämtlichen Inhabern eines Personalausweises zum Gegenstand noch zur Folge.

B.31.2. Die Bewertung der Notwendigkeit der angefochtenen Bestimmung durch den Gesetzgeber ist somit nicht unvernünftig.

B.32.1. Wie in B.23.2 erwähnt, obliegt es dem König, bei der Ausführung der ihm erteilten Ermächtigungen die geeigneten technischen und organisatorischen Maßnahmen zur Sicherung der Daten unter Einhaltung insbesondere der einschlägigen Bestimmungen der Datenschutz-Grundverordnung und der Verordnung (EU) 2019/1157 zu ergreifen.

Es obliegt dem zuständigen Richter, gegebenenfalls zu prüfen, ob diese Maßnahmen angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person im Sinne von Artikel 9 Absatz 2 Buchstabe g der Datenschutz-Grundverordnung darstellen.

B.32.2. Vorbehaltlich der Umsetzung dieser Befugnisse durch den König ist das von den klagenden Parteien angeführte Risiko des Missbrauchs nicht ausreichend stichhaltig.

Es trifft zwar zu, dass der Diebstahl der Daten zu den digitalen Fingerabdrücken schwerwiegende Nachteile für die betroffene Person, deren Identität missbräuchlich verwendet werden könnte, nach sich ziehen könnte, aber dieses Risiko kann erheblich durch die begrenzte Speicherdauer der Daten für die Zwecke der Herstellung und Ausstellung des Personalausweises sowie durch die technischen Sicherungsmaßnahmen eingegrenzt werden, die der König ergreifen muss. Wie der Minister der Sicherheit und des Innern im Ausschuss der Kammer bemerkt hat, ist es im Übrigen « für denjenigen, der die Fingerabdrücke einer Person ‘ stehlen ’ möchte, einfacher, einen Gegenstand zu nehmen, auf dem diese Person ihre Fingerabdrücke hinterlassen hat, als zu versuchen, sich derer zu bemächtigen, die sich auf dem Personalausweis befinden » (*Parl. Dok.*, Kammer, 2018-2019, DOC 54-3256/003, S. 61).

B.33. Schließlich sind gemäß Artikel 6*quater* des Gesetzes vom 19. Juli 1991 « Personen, die bei der Ausübung ihres Amtes an der Sammlung, Verarbeitung oder Übermittlung der Informationen beteiligt sind, […] an das Berufsgeheimnis gebunden » (Absatz 1). Diese Personen « müssen alle notwendigen Vorsichtsmaßnahmen zur Sicherung der registrierten Informationen treffen und insbesondere deren Entstellung, Beschädigung oder Mitteilung an Personen, die nicht zu deren Kenntnisnahme ermächtigt worden sind, verhindern » (Absatz 2). Die Nichteinhaltung dieser Pflichten wird gemäß Artikel 7 des Gesetzes vom 19. Juli 1991 strafrechtlich geahndet. Außerdem stellen die Artikel 461, 550*bis* und 550*ter* des

Strafgesetzbuches jeweils den Diebstahl, den unbefugten Zugriff zu einem Datenverarbeitungssystem und die unbefugte Änderung eines solchen Systems unter Strafe.

B.34. Die angefochtene Bestimmung hat daher in Anbetracht der verfolgten Ziele keine unverhältnismäßigen Folgen für die betroffenen Personen.

B.35. Dadurch, dass sie die Abnahme von zwei digitalen Fingerabdrücken und die Speicherung ihres digitalen Bildes auf dem Personalausweis vorsieht, verstößt die angefochtene Bestimmung nicht gegen das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten, wie sie durch die in den Klagegründen genannten Bestimmungen gewährleistet werden.

Im Übrigen weisen die klagenden Parteien nicht konkret nach, inwiefern die angefochtene Bestimmung gegen die Artikel 1 bis 4, 25 und 32 der Datenschutz-Grundverordnung verstoßen würde.

B.36. Insoweit sich die Beschwerdegründe auf die Abnahme von zwei digitalen Fingerabdrücken und die Speicherung ihres digitalen Bildes auf dem Personalausweis beziehen, sind sie unbegründet.

2. Die zentralisierte Speicherung des digitalen Bildes der Fingerabdrücke für die Zwecke der Herstellung und Ausstellung des Personalausweises

B.37. Die klagenden Parteien beanstanden die zentralisierte Speicherung des digitalen Bildes der Fingerabdrücke für die Zwecke der Herstellung und Ausstellung des Personalausweises während einer Dauer von höchstens drei Monaten. Sie führen an, dass eine solche Maßnahme nicht notwendig sei, weil es technisch möglich sei, die Information zum Zeitpunkt der Abholung des Personalausweises durch seinen Inhaber direkt in den Mikrochip zu integrieren. Sie bemängeln außerdem das Fehlen von geeigneten technischen Maßnahmen, um die Integrität und Vertraulichkeit der so gespeicherten Daten zu gewährleisten.

B.38.1. Aus den Vorarbeiten geht hervor, dass das digitale Bild der Fingerabdrücke für die Zwecke der Herstellung und Ausstellung des Personalausweises vorübergehend in einer zentralisierten Datenbank gespeichert wird:

« Les empreintes digitales ne seront en aucune façon stockées ni centralisées, si ce n'est durant la période nécessaire à la fabrication et à la délivrance de la carte d'identité, à l'instar de toutes autres données figurant sur la carte, et en tout état de cause durant maximum 3 mois. Aussi longtemps que la carte n'est pas délivrée au citoyen, il se peut qu'elle soit détruite, défectueuse,…, et dans ce cas, une nouvelle carte serait fabriquée, sans que le citoyen ne doive se présenter à nouveau auprès de son administration communale. Après ce délai, la loi en projet spécifie que ces données doivent impérativement être détruites et effacées de la banque de données » (*Parl. Dok.*, Kammer, 2017-2018, DOC 54-3256/001, S. 34).

Im Ausschuss der Kammer hat der Minister der Sicherheit und des Innern erläutert, dass die maximale Speicherdauer der Daten von drei Monaten durch technische Pflichten gerechtfertigt sei und dass die digitalen Fingerabdrücke gelöscht werden, sobald der Personalausweis ausgestellt sei:

« En ce qui concerne les empreintes digitales, [le membre] estime que le délai maximal de trois mois pour la fabrication de la carte d'identité est trop long.

Il s'agit en l'occurrence d'obligations techniques. Le délai est d'ailleurs identique à celui des passeports et des cartes d'étranger. Il n'y a donc rien de nouveau sous le soleil. En outre, il est explicitement indiqué que les empreintes digitales ne peuvent être conservées qu'aussi longtemps que nécessaire pour la fabrication, avec un maximum de trois mois. Cela signifie que dès que la carte a été délivrée au citoyen, généralement dans un délai de 1 à 2 semaines, les empreintes digitales sont effacées immédiatement » (*Parl. Dok.*, Kammer, 2018-2019, DOC 54-3256/003, S. 48).

B.38.2. In Übereinstimmung mit dem Ministerrat kann angenommen werden, dass die Zentralisierung der digitalen Fingerabdrücke für die Zwecke der Herstellung und Ausstellung des Personalausweises aus Gründen der Datensicherheit und -integrität gerechtfertigt ist. Die Zentralisierung der Daten anstelle ihrer Integration in den Mikrochip des Personalausweises bei dessen Ausstellung bietet mehr Garantien hinsichtlich ihrer Sicherheit und Integrität. Das Missbrauchsrisiko wäre nämlich höher, wenn es in jeder Gemeindeverwaltung des Landes möglich wäre, die digitalen Fingerabdrücke in einen Personalausweis zu integrieren.

In diesem Zusammenhang ist die Speicherung des digitalen Bildes der Fingerabdrücke « während der Zeit, die für die Herstellung und Ausstellung des Personalausweises erforderlich ist, und in jedem Fall während eines Zeitraums von höchstens drei Monaten » angesichts der

Zielsetzung, das heißt der Herstellung und Ausstellung des Personalausweises, nicht offensichtlich übermäßig. In der angefochtenen Bestimmung ist ausdrücklich die Pflicht vorgesehen, die Daten nach Ablauf dieses Zeitraums zu vernichten und zu löschen, was, wie in B.23.1 erwähnt, deren endgültige Löschung voraussetzt.

Zudem obliegt es, wie in B.23.2 erwähnt, in Ausführung der ihm erteilten Ermächtigungen dem König, die geeigneten technischen und organisatorischen Maßnahmen zu ergreifen, um die Integrität und Vertraulichkeit der so gespeicherten Daten zu gewährleisten.

B.38.3. Die Kritik, die die klagende Partei in der Rechtssache Nr. 7202 in ihrem Erwiderungsschriftsatz an Artikel 10 Absatz 3 der Verordnung (EU) 2019/1157 äußert, insofern er die Datenspeicherung einerseits bis zu 90 Tage nach Ausstellung des Ausweisdokuments und andererseits für andere Zwecke als die in der Verordnung vorgesehenen Zwecke länger als 90 Tage erlaube, sind im vorliegenden Fall nicht relevant, da in der angefochtenen Bestimmung die Datenspeicherung « nur während der Zeit, die für die Herstellung und Ausstellung des Personalausweises erforderlich ist » und in jedem Fall nur für eine Dauer von höchstens drei Monaten ab der Abnahme des digitalen Bildes der Fingerabdrücke und nicht ab der Ausstellung des Personalausweis vorgesehen ist.

Die Behauptung derselben klagenden Partei, dass die Verordnung (EU) 2019/1157 in Verbindung mit dem Durchführungsbeschluss K(2018) 7767 der Europäischen Kommission vom 30. November 2018 « zur Festlegung der technischen Spezifikationen für die einheitliche Gestaltung des Aufenthaltstitels für Drittstaatsangehörige und zur Aufhebung der Entscheidung K(2002) 3069 » keine geeigneten technischen und organisatorischen Maßnahmen enthalte, um die Sicherheit der gespeicherten digitalen Fingerabdrücke zu gewährleisten, wird nicht begründet. Unter Berücksichtigung des in B.38.2 Erwähnten, ist im vorliegenden Fall diese Kritik in jedem Fall nicht relevant.

B.39. Die in B.37 aufgeführten Beschwerdegründe sind also unbegründet. Unter Berücksichtigung des in B.38.3 Erwähnten, ist dem Gerichtshof der Europäischen Union die von der klagenden Partei in der Rechtssache Nr. 7202 vorgeschlagene Vorabentscheidungsfrage zur Gültigkeit von Artikel 10 Absatz 3 der Verordnung (EU) 2019/1157 nicht zu stellen.

3. Das Lesen des digitalen Bildes der Fingerabdrücke durch die dazu ermächtigten Stellen

B.40. Die klagenden Parteien führen mehrere Beschwerdegründe gegen die angefochtene Bestimmung an, was das Lesen des digitalen Bildes der Fingerabdrücke durch die dazu ermächtigten Stellen betrifft.

B.41.1. Die klagenden Parteien bemängeln, dass in der angefochtenen Bestimmung nicht die Technik oder die Methode bestimmt werde, mit der der digitale Fingerabdruck erfasst und gelesen wird, und dass darin nicht die Aufzeichnung der Daten bei dieser Gelegenheit verboten werde. Sie beanstanden ebenfalls, dass darin nicht präzisiert sei, ob die Ermächtigungen mit technischen Maßnahmen einhergehen müssten.

B.41.2. Die Bestimmung der konkreten Modalitäten zum Lesen des digitalen Bildes der Fingerabdrücke gehört zur Ausführung des Gesetzes. Aus den gleichen wie den in B.23.2 erwähnten Gründen, obliegt es dem König, unter der Kontrolle des zuständigen Richters die für diesen Zweck geeigneten technischen Maßnahmen unter Einhaltung der relevanten Bestimmungen der Datenschutz-Grundverordnung und der Verordnung (EU) 2019/1157 zu ergreifen.

Diesbezüglich wurde in den Vorarbeiten präzisiert:

« Les empreintes digitales seront protégées par un certificat permettant une lecture uniquement par des lecteurs autorisés » (*Parl. Dok.*, Kammer, 2017-2018, DOC 54-3256/001, S. 35; siehe auch *Parl. Dok.*, Kammer, 2018-2019, DOC 54-3256/003, S. 36).

Artikel 6*quater* Absatz 2 des Gesetzes vom 19. Juli 1991 sieht außerdem ausdrücklich die Pflicht für « Personen, die bei der Ausübung ihres Amtes an der Sammlung, Verarbeitung oder Übermittlung der Informationen beteiligt sind, » vor, « alle notwendigen Vorsichtsmaßnahmen zur Sicherung der registrierten Informationen [zu] treffen und insbesondere deren Entstellung, Beschädigung oder Mitteilung an Personen, die nicht zu deren Kenntnisnahme ermächtigt worden sind, [zu] verhindern ».

B.41.3. Mit der angefochtenen Bestimmung werden mehrere Stellen ermächtigt, das digitale Bild der Fingerabdrücke zu lesen. Diese Ermächtigung gilt nur für das Lesen. Außerdem ist die angefochtene Bestimmung so auszulegen, dass sie die Aufzeichnung der Daten, wenn sie gelesen werden, nicht erlaubt. So heißt es in den Vorarbeiten, dass « die digitalen Fingerabdrücke in keiner Weise gespeichert oder zentralisiert werden, abgesehen von dem Zeitraum, der für die Herstellung und Ausstellung des Personalausweises erforderlich ist » (*Parl. Dok.*, Kammer, 2017-2018, DOC 54-3256/001, S. 34, und *Parl. Dok.*, Kammer, 2018-2019, DOC 54-3256/003, S. 16).

B.41.4. Vorbehaltlich der in B.41.3 erwähnten Auslegung ist der in B.41.1 genannte Beschwerdegrund unbegründet.

B.42.1. Die klagenden Parteien bemängeln, dass in der angefochtenen Bestimmung nicht präzisiert sei, worin das Lesen des digitalen Bildes der Fingerabdrücke bestehe. Sie machen geltend, dass die angefochtene Bestimmung den betroffenen Behörden eine zu weit gefasste Ermächtigung erteile, was den Zugriff auf die Daten und ihre spätere Nutzung betreffe. So gehe aus der angefochtenen Bestimmung nicht der Zweck des Lesens der digitalen Fingerabdrücke durch die mit der Grenzkontrolle beauftragten Bediensteten hervor – wobei die Ermächtigung ebenfalls für ausländisches Personal gelte, das gegebenenfalls eine Privatfirma sein könne – und die Verarbeitung von digitalen Fingerabdrücken durch die Polizei im Rahmen von Behinderungen der verwaltungspolizeilichen Aufträge sei nicht auf Gründe eines erheblichen öffentlichen Interesses begrenzt.

B.42.2.1. Der Zweck des Lesens des digitalen Bildes der Fingerabdrücke durch die befugten Stellen ergibt sich logischerweise aus dem Gegenstand der Maßnahme sowie aus den Aufträgen, die diese Stellen übernehmen, so wie diese Aufträge in der angefochtenen Bestimmung erwähnt sind.

B.42.2.2. In Bezug auf das Personal, das mit der Grenzkontrolle sowohl in Belgien als auch im Ausland beauftragt ist, muss die angefochtene Bestimmung vernünftigerweise so ausgelegt werden, dass sie das Lesen nur im Rahmen der Grenzkontrolle und allein zu diesem Zweck erlaubt.

Der Umstand, dass das Personal im Ausland ermächtigt wird, das digitale Bild der Fingerabdrücke zu lesen, ergibt sich aus der Notwendigkeit, die Identität von Personen nicht nur an den belgischen Grenzen, sondern auch an den Binnengrenzen zwischen Mitgliedstaaten und an den Außengrenzen der Europäischen Union zu überprüfen. Aufgrund von Artikel 11 Absatz 6 der Verordnung (EU) 2019/1157 dürfen die digitalen Fingerabdrücke nur « von ordnungsgemäß befugten Mitarbeitern der zuständigen nationalen Behörden und Agenturen der Union verwendet werden […] ».

B.42.2.3. Was die Polizeidienste betrifft, so dürfen diese das digital Bild der Fingerabdrücke nur lesen, « sofern dies für die Erfüllung ihrer verwaltungs- und gerichtspolizeilichen gesetzlichen Aufträge im Rahmen der Betrugsbekämpfung erforderlich ist, insbesondere der Bekämpfung des Menschenhandels und -schmuggels, des Betrugs und der Untreue, der Geldwäsche, des Terrorismus, der Fälschung und des Gebrauchs gefälschter Urkunden, der Namensanmaßung und des Gebrauchs eines falschen Namens, der Verstöße gegen das Gesetz vom 15. Dezember 1980 über die Einreise ins Staatsgebiet, den Aufenthalt, die Niederlassung und das Entfernen von Ausländern ».

Diese Ermächtigung der Polizeidienste ist ausreichend eingegrenzt und beruht auf Gründen eines erheblichen öffentlichen Interesses im Sinne von Artikel 9 Absatz 2 Buchstabe g der Datenschutz-Grundverordnung.

B.42.2.4. Die Betreffenden können also die Zwecke des Lesens des digitalen Bildes ihrer Fingerabdrücke auf dem Personalausweis ausreichend präzise kennen.

B.42.2.5. Wie in B.41.3 erwähnt, gilt die Ermächtigung schließlich nur für das Lesen des digitalen Bildes der Fingerabdrücke und erlaubt somit keine Aufzeichnung von Daten, was ihre spätere Nutzung ausschließt.

B.42.3. Vorbehaltlich der in B.42.2.2 erwähnten Auslegung ist der in B.42.1 genannte Beschwerdegrund unbegründet.

B.43.1. Die klagenden Parteien bemängeln den Umstand, dass es die angefochtene Bestimmung den in Artikel 6 § 2 Absatz 6 des Gesetzes vom 19. Juli 1991 aufgezählten Stellen erlaube, das digitale Bild der Fingerabdrücke nicht nur auf dem Personalausweis, sobald dieser

seinem Inhaber ausgestellt ist, sondern auch während der Phase der Herstellung zu lesen, indem sie auf die zentralisierte Datenbank zugreifen können, in der die Informationen vorübergehend gespeichert sind.

B.43.2. In Bezug auf die Ermächtigung zum Lesen des digitalen Bildes der Fingerabdrücke wird zwar in der angefochtenen Bestimmung keine Unterscheidung der Phase der Herstellung und Ausstellung des Personalausweises einerseits und der Phase nach der Ausstellung des Personalausweises für seinen Inhaber andererseits vorgenommen.

Wie der Ministerrat anführt, werden die verschiedenen Stellen, die dazu ermächtigt sind, das digitale Bild der Fingerabdrücke zu lesen, jedoch im Rahmen der Ausübung ihres Amtes, wie diese gesetzlich beschrieben sind, dazu ermächtigt.

Daraus folgt, dass die angefochtene Bestimmung während der Phase der Herstellung und Ausstellung des Personalausweises vernünftigerweise so ausgelegt werden muss, dass sie den Abruf des digitalen Bildes der Fingerabdrücke allein zum Zweck der Herstellung und Ausstellung des Personalausweises erlaubt.

Diesbezüglich geht aus den Vorarbeiten hervor, dass der Zugriff auf die Datenbank, in der die digitalen Fingerabdrücke vorübergehend gespeichert werden, eingeschränkt ist:

« Cette base de données a un accès limité avec habilitations personnelles pour les personnes autorisées. Cet accès se fait via des connexions sécurisées et il y a une journalisation de l'utilisation de celle-ci ainsi que des personnes qui l'utilisent » (*Parl. Dok.*, Kammer, 2018-2019, DOC 54-3256/003, S. 36).

In dieser Auslegung erlaubt es die angefochtene Bestimmung den Polizeidiensten und dem mit der Grenzkontrolle beauftragten Personal also nicht, in der Phase der Herstellung und Ausstellung des Personalausweises die digitalen Fingerabdrücke abzurufen.

B.43.3. Vorbehaltlich der in B.43.2 erwähnten Auslegung ist der in B.43.1 genannte Beschwerdegrund unbegründet.

B.44.1. Die klagenden Parteien bemängeln, dass die angefochtene Bestimmung das Lesen der digitalen Fingerabdrücke auf dem Personalausweis in großem Maßstab, kontaktlos und im

Geheimen insbesondere durch die Polizeidienste erlaube und den Abgleich dieser Daten mit anderen Informationen zur Identifizierung einer Person gestatte. In der angefochtenen Bestimmung sei auch nicht vorgesehen, dass das Lesen nur subsidiär erfolgen darf und auf den Zweck der Prüfung der Echtheit des Personalausweises und der Identität des Inhabers beschränkt sei.

B.44.2. Die Stellen, die befugt sind, die digitalen Fingerabdrücke zu lesen, sind nur im Rahmen der Ausübung ihres Amtes, wie dieses gesetzlich beschrieben ist, dazu befugt.

Es obliegt ihnen, diese Ermächtigung unter Einhaltung der Grundsätze umzusetzen, die zum Schutz personenbezogener Daten anwendbar sind. Nach Artikel 9 Absatz 2 Buchstabe g der Datenschutz-Grundverordnung darf eine Verarbeitung von sensiblen personenbezogenen Daten nur vorgenommen werden, wenn sie erforderlich ist und in angemessenem Verhältnis zu den verfolgten Gründen eines erheblichen öffentlichen Interesses steht, was bedeutet, dass die Prüfung der digitalen Fingerabdrücke erst nach vorrangiger Überprüfung des Gesichtsbilds und falls sie « zur zweifelsfreien Bestätigung der Echtheit des Dokuments und der Identität des Inhabers notwendig » ist, erfolgen darf, wie es im Erwägungsgrund 19 der Verordnung (EU) 2019/1157 empfohlen ist.

Die Umsetzung dieser Pflichten fällt unter die Anwendung des Gesetzes, für die der Gerichtshof nicht zuständig ist.

Im Übrigen erläutern die klagenden Parteien nicht, warum die Polizeidienste im Rahmen der Ausübung ihres Amtes das digitale Bild der Fingerabdrücke zu anderen Zwecken als der Überprüfung der Echtheit des Personalausweises oder der Identität des Inhabers lesen könnten.

B.44.3. Der Datenabgleich, um eine Person zu identifizieren, ist nicht möglich, da die digitalen Fingerabdrücke, wie in B.41.3 erwähnt, beim Lesen nicht gespeichert werden dürfen.

Wie der Ministerrat anführt, können die digitalen Fingerabdrücke außerdem nicht ohne Wissen des Betroffenen gelesen werden, da das Abrufen der digitalen Fingerabdrücke im Rahmen einer von den Polizeidiensten durchgeführten Kontrolle einen direkten Kontakt mit dem Bürger voraussetzt, in Bezug auf den überprüft werden soll, dass die digitalen

Fingerabdrücke mit denen übereinstimmen, deren digitales Bild auf dem Personalausweis gespeichert ist.

B.44.4. Der in B.44.1 genannte Beschwerdegrund ist unbegründet.

Zu den Anträgen, Vorabentscheidungsfragen beim Gerichtshof der Europäischen Union zu stellen

B.45.1. Die klagenden Parteien in den Rechtssachen Nrn. 7150, 7202, 7203 und 7211 schlagen vor, dem Gerichtshof der Europäischen Union mehrere Vorabentscheidungsfragen zur Gültigkeit der Verordnung (EU) 2019/1157 zu stellen.

Die klagenden Parteien schlagen ebenfalls vor, dem Gerichtshof mehrere Vorabentscheidungsfragen zur Auslegung des Unionsrechts zu stellen.

B.45.2. Die Prüfung der geltend gemachten Beschwerdegründe hat keine Zweifel bezüglich der Gültigkeit von einer oder mehreren Maßnahmen der angefochtenen Bestimmung, die ihre Entsprechung in der Verordnung (EU) 2019/1157 haben, oder bezüglich der Auslegung der im vorliegenden Fall anwendbaren Bestimmungen des Unionsrechts aufkommen lassen, sodass den vorerwähnten Anträgen nicht nachzukommen ist.

Aus diesen Gründen:

Der Gerichtshof

weist die Klagen vorbehaltlich der in B.41.3, B.42.2.2 und B.43.2 erwähnten Auslegungen zurück.

Erlassen in französischer, niederländischer und deutscher Sprache, gemäß Artikel 65 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof, am 14. Januar 2021.

Der Kanzler, Der Präsident,

P.-Y. Dutilleux F. Daoût