

Geschäftsverzeichnisnr. 7023
Entscheid Nr. 27/2020 vom 20. Februar 2020

ENTSCHEID

In Sachen: Klage auf Nichtigkeitsklärung des Gesetzes vom 21. März 2018 « zur Abänderung des Gesetzes über das Polizeiamt im Hinblick auf die Regelung des Einsatzes von Kameras durch die Polizeidienste und zur Abänderung des Gesetzes vom 21. März 2007 zur Regelung der Installation und des Einsatzes von Überwachungskameras, des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste und des Gesetzes vom 2. Oktober 2017 zur Regelung der privaten und besonderen Sicherheit », erhoben von der VoG « Liga voor Mensenrechten ».

Der Verfassungsgerichtshof,

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

erlässt nach Beratung folgenden Entscheid:

*

* *

I. *Gegenstand der Klage und Verfahren*

Mit einer Klageschrift, die dem Gerichtshof mit am 15. Oktober 2018 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 16. Oktober 2018 in der Kanzlei eingegangen ist, erhob die VoG « Liga voor Mensenrechten », unterstützt und vertreten durch RA D. Pattyn, in Westflandern zugelassen, Klage auf Nichtigerklärung des Gesetzes vom 21. März 2018 « zur Abänderung des Gesetzes über das Polizeiamt im Hinblick auf die Regelung des Einsatzes von Kameras durch die Polizeidienste und zur Abänderung des Gesetzes vom 21. März 2007 zur Regelung der Installation und des Einsatzes von Überwachungskameras, des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste und des Gesetzes vom 2. Oktober 2017 zur Regelung der privaten und besonderen Sicherheit » (veröffentlicht im *Belgischen Staatsblatt* vom 16. April 2018).

Der Ministerrat, unterstützt und vertreten durch RA S. Sottiaux und RÄin E. Cloots, in Antwerpen zugelassen, und RA H. Graux und RÄin M. Van Der Sype, in Brüssel zugelassen, hat einen Schriftsatz eingereicht, die klagende Partei hat einen Erwiderungsschriftsatz eingereicht, und der Ministerrat hat auch einen Gegenerwiderungsschriftsatz eingereicht.

Durch Anordnung vom 18. Dezember 2019 hat der Gerichtshof nach Anhörung der referierenden Richter L. Lavrysen und J.-P. Moerman, in Vertretung des Ehrenrichters J.-P. Snappe, beschlossen, dass die Rechtssache verhandlungsreif ist, dass keine Sitzung abgehalten wird, außer wenn eine Partei innerhalb von sieben Tagen nach Erhalt der Notifizierung dieser Anordnung einen Antrag auf Anhörung eingereicht hat, und dass vorbehaltlich eines solchen Antrags die Verhandlung am 15. Januar 2020 geschlossen und die Rechtssache zur Beratung gestellt wird.

Da keine Sitzung beantragt wurde, wurde die Rechtssache am 15. Januar 2020 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 angefochtenen Bestimmungen

B.1. Die klagende Partei beantragt die Nichtigerklärung des Gesetzes vom 21. März 2018 « zur Abänderung des Gesetzes über das Polizeiamt im Hinblick auf die Regelung des Einsatzes von Kameras durch die Polizeidienste und zur Abänderung des Gesetzes vom 21. März 2007

zur Regelung der Installation und des Einsatzes von Überwachungskameras, des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste und des Gesetzes vom 2. Oktober 2017 zur Regelung der privaten und besonderen Sicherheit » (nachstehend: Gesetz vom 21. März 2018).

Dem Inhalt der Antragschrift lässt sich entnehmen, dass die Einwände nur gegen die Artikel 6, 9, 11, 12, 28, 35, 48, 49, 50, 60, 61, 69, 70, 71, 75, 80, 84, 85 und 86 des angefochtenen Gesetzes gerichtet sind. Der Gerichtshof beschränkt seine Prüfung auf diese Bestimmungen.

Sollte sich aus der näheren Prüfung der Klagegründe ergeben, dass nur einige der vorerwähnten Artikel oder einige Teile dieser Artikel beanstandet werden, wird die Prüfung gegebenenfalls darauf beschränkt.

B.2.1. Das Gesetz vom 21. März 2018 ändert die Regelungen in Bezug auf den Einsatz und die Installation von Überwachungskameras ab. Es versucht dabei, « die Privatsphäre der Bürger so weit wie möglich zu garantieren, wobei das Gleichgewicht zwischen der Realität und den praktischen Bedürfnissen bei Einsätzen aufrechterhalten wurde » (*Parl. Dok.*, Kammer, 2017-2018, DOC 54-2855/001, S. 5).

Wie sich aus dem Gesetzesnamen ergibt, ändert das angefochtene Gesetz vier andere Gesetze ab.

B.2.2. Das Gesetz vom 21. März 2018 ändert zunächst das Gesetz vom 5. August 1992 « über das Polizeiamt » (nachstehend: Gesetz über das Polizeiamt) ab. Es soll die Kameras der Polizeidienste aus dem Anwendungsbereich des Gesetzes vom 21. März 2007 « zur Regelung der Installation und des Einsatzes von Überwachungskameras » (nachstehend: Kameragesetz) herausnehmen, um deren Einsatz im Gesetz über das Polizeiamt zu regeln, und soll folglich « eine Sonderregelung bezüglich des Einsatzes von Kameras durch die Polizeidienste sowohl im Rahmen ihrer Aufgaben als Verwaltungspolizei als auch als Gerichtspolizei ausarbeiten » (ebenda, S. 3).

Das Gesetz vom 21. März 2018 regelt die Ermächtigung zur Installation und zum Einsatz von Kameras durch die Polizeidienste sowie die Regeln zur Verarbeitung gesammelter Daten.

Es erlaubt im bestimmten Fällen den nicht sichtbaren Einsatz von Kameras und enthält einen Rahmen für die Nutzung der durch Kameras für die automatische Nummernschilderkennung (ANPR) gesammelten Daten (ebenda, SS. 3 und 4).

Die Abänderungen hinsichtlich des Gesetzes über das Polizeiamt sind in Kapitel 2 des Gesetzes vom 21. März 2018 enthalten (Artikel 2 bis 62).

B.2.3. Das Gesetz vom 21. März 2018 ändert auch das vorerwähnte Kameragesetz ab, zum einen um Zweifel und Anwendungsschwierigkeiten in Bezug auf manche Bestimmungen des Kameragesetzes aus dem Weg zu räumen beziehungsweise zu beseitigen und zum anderen um das Gesetz an die Entwicklungen auf europäischer Ebene anzupassen (ebenda, S. 4).

Das Kameragesetz finden Anwendung auf die Installation und den Einsatz von Überwachungskameras, die darauf abzielen, Straftaten gegen Personen oder Güter vorzubeugen, festzustellen oder aufzuspüren (Artikel 3 Absatz 1 Nr. 1) oder ungesellschaftliches Verhalten im Sinne von Artikel 135 des Neuen Gemeindegesetzes vorzubeugen, festzustellen oder aufzuspüren, die Einhaltung der Gemeindeverordnungen zu kontrollieren oder die öffentliche Ordnung aufrechtzuerhalten (Artikel 3 Absatz 1 Nr. 2).

Das Gesetz vom 21. März 2018 fügt neue Regeln für den Einsatz intelligenter mobiler Überwachungskameras in das Kameragesetz ein sowie besondere Maßnahmen hinsichtlich Situationen, in denen diese aufgrund der Art des Ortes und des Sicherheitsrisikos gerechtfertigt sind, nämlich die Aufbewahrung der Bilder während eines Zeitraums von drei Monaten statt eines Monats, das Aufzeichnen des Perimeters eines Ortes und die Ermöglichung des Zugriffs auf die Bilder in Echtzeit zugunsten der Polizeidienste (ebenda, SS. 4 und 5).

Die Abänderungen hinsichtlich des Kameragesetzes sind in Kapitel 3 des Gesetzes vom 21. März 2018 enthalten (Artikel 63 bis 83).

B.2.4. Ferner ändert das Gesetz vom 21. März 2018 das Gesetz vom 30. November 1998 « über die Nachrichten- und Sicherheitsdienste » (nachstehend: Gesetz über die Nachrichten- und Sicherheitsdienste) ab. Die Nachrichten- und Sicherheitsdienste können im Interesse der Ausübung ihrer Aufgaben und unter bestimmten Bedingungen auf die Kameras

zugreifen, die die Polizeidienste benutzen dürfen, und auf die Datenbanken, in denen die personenbezogenen Daten und Informationen gesammelt werden (ebenda, S. 5).

Die Abänderungen bezüglich des Gesetzes über die Nachrichten- und Sicherheitsdienste sind in Kapitel 4 des Gesetzes vom 21. März 2018 enthalten (Artikel 84 bis 86).

B.2.5. Schließlich ändert das Gesetz vom 21. März 2018 das Gesetz vom 2. Oktober 2017 « zur Regelung der privaten und besonderen Sicherheit » ab, indem es die Befugnis der Wachleute regelt, sich die Bilder von auf öffentlichen Straßen installierten Kameras anzusehen (ebenda, S. 5).

Die Abänderungen sind in Kapitel 5 des Gesetzes vom 21. März 2018 enthalten (Artikel 87), auf das sich die Antragschrift nicht bezieht.

In Bezug auf die Zulässigkeit

B.3.1. Der Ministerrat stellt die Zulässigkeit der Nichtigkeitsklage in Abrede, sofern der Gerichtshof ersucht werde, sich zur Vereinbarkeit des angefochtenen Gesetzes mit den Artikeln der Europäischen Menschenrechtskonvention und der Charta der Grundrechte der Europäischen Union und des Gesetzes vom 30. Juli 2018 « über den Schutz natürlicher Personen hinsichtlich der Verarbeitung personenbezogener Daten » zu äußern.

B.3.2. Die internationalen Bestimmungen, anhand derer der Gerichtshof keine unmittelbare Prüfung vornehmen darf, werden zusammen mit Verfassungsbestimmungen angeführt, anhand derer der Gerichtshof eine unmittelbare Prüfung vornehmen darf, sodass alle diese Bestimmungen im Zusammenhang gelesen werden müssen.

B.3.3. Der Gerichtshof ist jedoch nicht befugt, gesetzliche Bestimmungen auf ihre Rechtmäßigkeit unter Zugrundelegung anderer gesetzlicher Bestimmungen, die nicht die Zuständigkeitsverteilung regeln, zu prüfen.

Der Einwand, der einen Verstoß gegen das Gesetz vom 30. Juli 2018 « über den Schutz natürlicher Personen hinsichtlich der Verarbeitung personenbezogener Daten » zum Gegenstand hat, ist unzulässig.

Zur Hauptsache

B.4.1. Der erste Klagegrund ist abgeleitet aus einem Verstoß gegen die Artikel 10, 11 und 22 der Verfassung in Verbindung mit Artikel 8 der Europäischen Menschenrechtskonvention, mit den Artikeln 7, 8 und 52 der Charta der Grundrechte der Europäischen Union und mit den Artikeln 4, 5, 6 und 7 der 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: Polizeirichtlinie).

B.4.2. Der zweite Klagegrund ist abgeleitet aus einem Verstoß gegen die Artikel 10, 11, 12, 14 und 22 der Verfassung, gegebenenfalls in Verbindung mit den Artikeln 6, 7 und 8 der Europäischen Menschenrechtskonvention, mit den Artikeln 7, 8, 47, 48 und 52 der Charta der Grundrechte der Europäischen Union, mit den Artikeln 4, 5, 6 und 7 der Polizeirichtlinie, mit dem allgemeinen Rechtsgrundsatz des Rechts auf ein faires Verfahren und des Rechts der Verteidigung und mit dem Legalitätsprinzip in Strafsachen.

B.4.3. Beide Klagegründe beziehen sich hauptsächlich auf das Recht auf Achtung des Privatlebens. Sie richten sich gegen die Aufbewahrungsfristen zu den registrierten Informationen und personenbezogenen Daten (erster Klagegrund) und die Verarbeitung dieser Informationen und Daten (erster und zweiter Teil des zweiten Klagegrundes).

Der zweite Klagegrund (dritter und vierter Teil) bezieht sich darüber hinaus auf das Legalitätsprinzip und den Grundsatz der Gleichheit und Nichtdiskriminierung.

In Bezug auf das Recht auf Achtung des Privatlebens

B.5. Nach Ansicht der klagenden Partei stellt die durch das Gesetz vom 21. März 2018 vorgesehene Möglichkeit, Informationen und personenbezogene Daten, die mittels polizeilicher Kameras gesammelt würden, während eines Zeitraums von zwölf Monaten aufzubewahren und Bilder, die mittels Einsatzes von Überwachungskameras aufgezeichnet worden seien, während eines Zeitraums von drei Monaten aufzubewahren, einen unverhältnismäßigen Eingriff in das Recht auf Achtung des Privatlebens dar (erster Klagegrund). Auch die Verarbeitung der gesammelten Informationen und personenbezogenen Daten, die das angefochtene Gesetz vorsehe, stelle einen unverhältnismäßigen Eingriff in das Recht auf Achtung des Privatlebens dar (erster und zweiter Teil des zweiten Klagegrundes).

B.6.1. 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.6.2. 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.6.3. 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.6.4. 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 weitreichende Tragweite und umfasst unter anderem den Schutz der personenbezogenen Daten und der persönlichen Information. Der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte lässt sich entnehmen, dass auch Kamerabilder von diesem Recht geschützt sind, sobald die Bilder gespeichert und verarbeitet werden, und zwar sogar dann, wenn sie an öffentlichen Orten aufgenommen worden sind (siehe insbesondere EuGHMR, 18. Oktober 2016, *Vukota-Bojić gegen Schweiz*, §§ 55-56; Große Kammer, 17. Oktober 2019, *López Ribalda u.a. gegen Spanien*, §§ 89-90). Das ist insbesondere der Fall, wenn die Bilder es erlauben, Personen zu identifizieren und in Erfahrung zu bringen, wer sich an welchem Ort zu einem bestimmten Zeitpunkt befindet.

Der Europäische Gerichtshof ist ebenfalls der Auffassung, dass sich die Achtung des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten auf jede Information erstreckt, die eine bestimmte oder bestimmbare natürliche Person betrifft (EuGH, Große Kammer, 9. November 2010, C-92/09 und C-93/09, *Volker und Markus Schecke und Eifert*, RandNr. 52; 16. Januar 2019, C-496/17, *Deutsche Post AG*, RandNr. 54).

B.7.1. Artikel 7 der Charta der Grundrechte der Europäischen Union bestimmt:

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

B.7.2. Artikel 8 der Charta der Grundrechte der Europäischen Union bestimmt:

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

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

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

B.7.3. Artikel 52 Absatz 1 der Charta der Grundrechte der Europäischen Union 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.7.4.1. Artikel 52 Absatz 3 der Charta der Grundrechte der Europäischen Union bestimmt:

« So weit diese Charta Rechte enthält, die den durch die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten garantierten Rechten entsprechen, haben sie die gleiche Bedeutung und Tragweite, wie sie ihnen in der genannten Konvention verliehen wird. Diese Bestimmung steht dem nicht entgegen, dass das Recht der Union einen weiter gehenden Schutz gewährt ».

B.7.5. Die Polizeirichtlinie legt in den Bereichen der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit spezifische Vorschriften 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, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit fest, wobei den Besonderheiten dieser Tätigkeiten Rechnung getragen wird.

Die klagende Partei erwähnt diese Richtlinie in beiden Klagegründen, jedoch knüpft sie daran keine konkreten Einwände.

B.7.6. Durch seinen Entscheid Nr. 96/2018 vom 19. Juli 2018 hat der Verfassungsgerichtshof im Rahmen von Klagen auf Nichtigerklärung des Gesetzes vom 29. Mai 2016 « über die Sammlung und Aufbewahrung der Daten im Bereich der

elektronischen Kommunikation » dem Gerichtshof der Europäischen Union drei Vorabentscheidungsfragen gestellt über die Auslegung von Artikel 15 Nr. 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 « über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation ».

Die Aufbewahrung und die Verarbeitung von Kamerabildern, die Straßen und den öffentlichen Raum betreffen, unterscheiden sich vor dem Hintergrund der Sensibilität privater Daten gleichwohl wesentlich von der Aufbewahrung und der Verarbeitung elektronischer Kommunikationsdaten, sodass der Gerichtshof die Antwort auf die Vorabentscheidungsfragen nicht abwarten muss, um vorliegende Klage beurteilen zu können.

Ihrer Natur nach stellen die Aufbewahrung und die Verarbeitung von Kamerabildern einen weniger einschneidenden Eingriff in das Privatleben dar als die Aufbewahrung und die Verarbeitung elektronischer Kommunikationsdaten. Das beruht einerseits darauf, dass die Erwartung in Bezug auf die Privatsphäre bei öffentlichen Orten nicht so hoch ist wie bei geschlossenen Kreisen, und andererseits darauf, dass Bilder die persönliche Lebenssphäre in der Regel weniger berühren als Kommunikationsdaten.

Letzteres gilt umso mehr, als das angefochtene Gesetz die Aufbewahrung und die Verarbeitung von Bildern ausschließt, die die Intimität einer Person verletzen oder die darauf abzielen, Informationen über die rassische oder ethnische Herkunft einer Person, ihre religiösen oder weltanschaulichen Überzeugungen, ihre politischen Meinungen, ihre Mitgliedschaft in einer Gewerkschaftsorganisation, ihren Gesundheitszustand, ihr Sexualleben oder ihre sexuelle Orientierung zu gewinnen (Artikel 25/3 § 3, eingefügt durch Artikel 8 des Gesetzes vom 21. März 2018).

B.7.7. Das Recht auf Achtung des Privatlebens ist nicht absolut. Die angeführten Verfassungs- und internationalen Bestimmungen schließen einen staatlichen Eingriff in das Recht auf Achtung des Privatlebens nicht aus, sondern schreiben vor, dass ein solcher Eingriff durch eine hinreichend genaue Gesetzesbestimmung erlaubt wird, dass dieser einem zwingenden gesellschaftlichen Bedürfnis in einer demokratischen Gesellschaft entspricht sowie im Verhältnis zum damit verfolgten gesetzlichen Ziel steht.

Der Gesetzgeber besitzt diesbezüglich einen Ermessensspielraum. Dieser Ermessensspielraum ist jedoch nicht unbegrenzt; damit eine gesetzliche Regelung mit dem Recht auf Achtung des Privatlebens vereinbar ist, ist es erforderlich, dass der Gesetzgeber ein faires Gleichgewicht zwischen allen betroffenen Rechten und Interessen gefunden hat. Bei der Beurteilung dieses Gleichgewichts berücksichtigt der Europäische Gerichtshof für Menschenrechte unter anderem die Bestimmungen des Übereinkommens des Europarates vom 28. Januar 1981 «zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten» (nachstehend: Übereinkommen Nr. 108) und die Empfehlung Nr. R (87) 15 des Ministerkomitees an die Vertragsstaaten über die Nutzung personenbezogener Daten im Polizeibereich (nachstehend: Empfehlung Nr. R (87) 15) (EuGHMR, 25. Februar 1997, *Z gegen Finnland*, § 95; Große Kammer, 4. Dezember 2008, 2010, *S. und Marper gegen Vereinigtes Königreich*, § 103).

Aus der unterschiedlichen Natur der in B.7.6 erwähnten Maßnahmen geht hervor, dass der Ermessensspielraum des Gesetzgebers bei Maßnahmen zur Aufbewahrung und Verarbeitung von Kamerabildern größer ist als bei Maßnahmen derselben Art, die sich auf Kommunikationsdaten beziehen.

B.8.1. Das angefochtene Gesetz sieht verschiedene Aufbewahrungsfristen vor, die auf eindeutige Weise in den nachfolgenden Bestimmungen erwähnt sind.

B.8.2. Die Aufbewahrung und die Registrierung von Informationen und personenbezogenen Daten, die die Polizei mittels Kameras sammelt, sollen dazu beitragen, die öffentliche Sicherheit zu gewährleisten, die öffentliche Ordnung zu schützen, Straftaten zu verhüten und die Rechte und Freiheiten anderer zu wahren. Die Maßnahme entspricht folglich einem zwingenden gesellschaftlichen Bedürfnis in einer demokratischen Gesellschaft.

B.8.3. Bei der Beurteilung der Verhältnismäßigkeit von Maßnahmen in Bezug auf die Verarbeitung personenbezogener Daten sind u.a. deren automatischer Charakter, die verwendeten Techniken, der Genauigkeitsgrad, die Relevanz, der gegebenenfalls außergewöhnliche Charakter der zu verarbeitenden Daten, das etwaige Vorhandensein von Maßnahmen zur Begrenzung der Datenspeicherfrist, das etwaige Vorhandensein eines unabhängigen Überwachungssystems, mit dem geprüft werden kann, ob eine Datenspeicherung weiterhin erforderlich ist, das etwaige Vorhandensein von ausreichenden Kontrollrechten und

Rechtsbehelfen für die betroffenen Personen, das etwaige Vorhandensein von Garantien zur Vermeidung einer Stigmatisierung der Personen, deren Daten verarbeitet werden, der unterscheidende Charakter der Regelung und das etwaige Vorhandensein von Garantien zur Vermeidung einer falschen Nutzung und von Missbrauch der verarbeiteten personenbezogenen Daten durch öffentliche Behörden zu berücksichtigen (Entscheid Nr. 108/2016 vom 14. Juli 2016, B.12.2; Entscheid Nr. 29/2018 vom 15. März 2018, B.14.4; 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. u.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.8.4. Aus der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte geht hervor, dass personenbezogene Daten nicht länger als notwendig für die Verwirklichung des Ziels, zu dem sie gespeichert werden, in einer Form aufbewahrt werden dürfen, die eine Identifizierung zulässt oder die zulässt, eine Verbindung zwischen einer Person und strafbaren Handlungen herzustellen. Bei der Beurteilung der Verhältnismäßigkeit der Dauer der Aufbewahrung in Bezug auf den Zweck, zu dem die Daten gespeichert wurden, berücksichtigt der Europäische Gerichtshof für Menschenrechte den Umstand, ob eine unabhängige Kontrolle über die Rechtfertigung für die Bewahrung der Daten in den Datenbanken anhand deutlicher Kriterien besteht oder nicht, sowie die Schwere der Taten, den Umstand, ob die betreffende Person früher bereits Gegenstand einer Festnahme war, die Schwere der auf einer Person ruhenden Verdächtigungen sowie jeden anderen besonderen Umstand (EuGHMR, Große Kammer, 4. Dezember 2008, *S. und Marper gegen Vereinigtes Königreich*, § 103; 18. April 2013, *M.K. gegen Frankreich*, § 35; 17. Dezember 2009, *B.B. gegen Frankreich*, § 61; 18. September 2014, *Brunet gegen Frankreich*, §§ 35-40).

In Artikel 5 Buchstabe e) des Übereinkommens Nr. 108 und in Artikel 7 der Empfehlung Nr. R (87) 15 sind ähnliche Garantien vorgesehen.

B.9.1. In Bezug auf den sichtbaren Einsatz von Kameras durch die Polizei bestimmt Artikel 25/6 des Gesetzes über das Polizeiamt, eingefügt durch Artikel 11 des Gesetzes vom 21. März 2018:

« Die Informationen und personenbezogenen Daten, die mittels Kameras gesammelt werden, können registriert und für eine Dauer von höchstens zwölf Monaten ab der Registrierung aufbewahrt werden, außer wenn in Abschnitt 12 des vorliegenden Kapitels eine andere Frist vorgesehen ist ».

In Bezug auf den nicht sichtbaren Einsatz von Kameras durch die Polizei bestimmt Artikel 46/12 Absatz 1 des Gesetzes über das Polizeiamt, eingefügt durch Artikel 60 des Gesetzes vom 21. März 2018:

« Die Informationen und personenbezogenen Daten, die mittels nicht sichtbarer Kameras gesammelt werden, können registriert und für eine Dauer von höchstens zwölf Monaten ab der Registrierung aufbewahrt werden, außer wenn eine andere Frist in Kapitel 4 Abschnitt 12 vorgesehen ist ».

Diese Bestimmungen finden auch Anwendung auf Polizeidienste, wenn sie in Anwendung des Kameragesetzes oder anderer Gesetze Zugang in Echtzeit zu Bildern von Überwachungskameras haben, die von anderen Verantwortlichen für die Verarbeitung installiert worden sind, und wenn dieser Zugang ein Aufzeichnen der Bilder innerhalb von Polizeidiensten ermöglicht (Artikel 25/1 § 2 des Gesetzes über das Polizeiamt, eingefügt durch Artikel 6 des Gesetzes vom 21. März 2018).

In Bezug auf die Kameras für die automatische Nummernschilderkennung bestimmt Artikel 44/11/3*decies* des Gesetzes über das Polizeiamt, eingefügt durch Artikel 35 des Gesetzes vom 21. März 2018:

« § 1. Die technischen Datenbanken, die infolge des Einsatzes von intelligenten Kameras für die automatische Nummernschilderkennung oder von intelligenten Systemen für die automatische Nummernschilderkennung eingerichtet worden sind, enthalten folgende Daten, wenn sie auf den Kamerabildern erscheinen:

1. Datum, Uhrzeit und genauer Ort der Durchfahrt des Nummernschilds,
2. Merkmale des mit diesem Nummernschild verbundenen Fahrzeugs,
3. Foto des Nummernschilds an der Vorderseite des Fahrzeugs und gegebenenfalls an der Hinterseite,

4. Foto des Fahrzeugs,
5. gegebenenfalls Foto des Fahrers und der Fahrzeuginsassen,
6. Daten der Protokollierung der Verarbeitungen.

§ 2. Die in § 1 vorgesehenen personenbezogenen Daten und Informationen können für eine Dauer von höchstens zwölf Monaten ab der Registrierung aufbewahrt werden.

Sobald diese Daten die Bedingungen erfüllen, um eine in Artikel 44/2 § 1 Nr. 1 und 2 erwähnte Datenbank zu speisen, werden sie nach manueller Validierung binnen einer Frist von einem Monat nach Erfüllung dieser Bedingungen darin kopiert und aufbewahrt

[...] ».

Die in Artikel 44/2 § 1 Nrn. 1 und 2 erwähnten Datenbanken sind die Allgemeine Nationale Datenbank und die Basisdatenbanken. Die Allgemeine Nationale Datenbank ist die polizeiliche Datenbank, die die Daten und die Informationen enthält, die alle Polizeidienste zur Erfüllung ihrer Aufträge benötigen. Es handelt sich dabei daher um eine nationale Datenbank, deren Daten und Informationen von verschiedenen Polizeidiensten stammen (vgl. Entscheid Nr. 108/2016 vom 14. Juli 2016). Die Basisdatenbanken sind die polizeilichen Datenbanken, die zugunsten der gesamten integrierten Polizei eingerichtet werden, « mit dem Zweck, die verwaltungs- und gerichtspolizeilichen Aufträge zu erfüllen, indem die darin enthaltenen personenbezogenen Daten und Informationen genutzt werden und die zuständigen Behörden über die Erfüllung dieser Aufträge informiert werden » (Artikel 44/11/2, § 1).

B.9.2. Bei der in den vorerwähnten Bestimmungen genannten Aufbewahrungsfrist von zwölf Monaten handelt es sich, wie sich aus der Formulierung « nicht länger als » ergibt und wie auch ausdrücklich im Rahmen der Vorarbeiten bestätigt wurde, um eine Höchstfrist:

« Le fait qu'il s'agit d'un délai maximum permet de rencontrer le principe de proportionnalité, comme le remarque le Conseil d'État, dans son avis n° 62.006/2 du 9 octobre 2017 [...]. En effet, de la même manière que les services de police doivent veiller au respect du principe de proportionnalité dans leur choix et leur manière d'utiliser des caméras, le délai de conservation des images est également un traitement qui doit respecter le principe de proportionnalité et correspondre aux finalités visées par les services de police » (*Parl. Dok.*, Kammer, 2017-2018, DOC 54-2855/001, S. 28).

Die Aufbewahrungsfrist von zwölf Monaten setzt der Anwendung des Verhältnismäßigkeitsgrundsatzes durch die Polizeidienste auf diese Weise eine klare Grenze.

B.9.3. In Bezug auf den nicht sichtbaren Einsatz von Kameras durch die Polizei hat der Gesetzgeber selbst in Artikel 46/12 des Gesetzes über das Polizeiamt einige Ausnahmen von der maximalen Aufbewahrungsfrist von zwölf Monaten geregelt, nämlich wenn die Informationen und Daten im Rahmen der Vorbereitung gerichtspolizeilicher Aktionen und der Aufrechterhaltung der öffentlichen Ordnung bei diesen Aktionen (Artikel 46/12 Absatz 2 des Gesetzes über das Polizeiamt), im Rahmen der spezialisierten Aufträge in Sachen Personenschutz (Artikel 46/12 Absatz 3) und im Rahmen der Überführung von Häftlingen (Artikel 46/12 Absatz 4) gesammelt wurden.

In diesen Fällen können die Informationen und Daten nur für die Dauer der Aktion oder des Auftrags aufbewahrt werden, und können sie nur länger aufbewahrt und verwendet werden, um zufällig festgestellte strafbare Handlungen zu beweisen oder um deren Täter zu identifizieren. Wie sich aus den Vorarbeiten ergibt, ist die Verlängerung nur möglich, wenn die Feststellung einer Straftat innerhalb der ursprünglichen Frist aufgrund dieser Daten stattgefunden hat (ebenda, S. 56).

B.9.4. In Bezug auf den sichtbaren Einsatz von Kameras durch die Polizei hat der Gesetzgeber die Installation und den Einsatz der betreffenden Kameras von einer vorherigen grundsätzlichen Erlaubnis des Gemeinderates, wenn es sich um eine Polizeizone handelt, oder des Ministers des Innern oder seines Beauftragten, für Dienste der föderalen Polizei, abhängig gemacht (Artikel 25/4 § 1 des Gesetzes über das Polizeiamt, eingefügt durch Artikel 9 des Gesetzes vom 21. März 2018).

Der Antrag auf Erlaubnis muss eine Analyse der Auswirkungen und Risiken auf Ebene des Schutzes des Privatlebens und auf operativer Ebene berücksichtigen, insbesondere in Bezug auf die Kategorien der verarbeiteten personenbezogenen Daten, die Verhältnismäßigkeit der angewandten Mittel, die zu erreichenden operativen Ziele und die Dauer der Aufbewahrung der Daten, die notwendig ist, um diese Ziele zu erreichen (Artikel 25/4 § 2 Absatz 2 des Gesetzes über das Polizeiamt, eingefügt durch Artikel 9 des Gesetzes vom 21. März 2018).

B.9.5. In Bezug auf die Kameras für die automatische Nummernschilderkennung können die Daten in der Allgemeinen Nationalen Datenbank und den Basisdatenbanken aufbewahrt

werden (Artikel 44/11/3*decies* § 2 Absatz 2 des Gesetzes über das Polizeiamt, eingefügt durch Artikel 35 des Gesetzes vom 21. März 2018).

Die Artikel 44/9 und 44/10 des Gesetzes über das Polizeiamt legen die Regeln bezüglich der Dauer der Aufbewahrung von personenbezogenen Daten und Informationen in der Allgemeinen Nationalen Datenbank und bezüglich der Archivierung dieser Daten und Informationen nach Ablauf dieses Zeitraums fest. Artikel 44/11/2 dieses Gesetzes legt die Regeln bezüglich der Aufbewahrung der in den Basisdatenbanken enthaltenen Daten fest. Durch seinen vorerwähnten Entscheid Nr. 108/2016 hat der Gerichtshof die Klage auf Nichtigerklärung dieser Bestimmungen abgewiesen (B.112-B.116).

B.9.6. Die Aufbewahrungsfrist muss ferner von der Zugriffsfrist unterschieden werden. Die Möglichkeit des Zugriffs auf die betreffenden Daten unterliegt unterschiedlichen Regelungen, je nachdem, ob es um Aufträge der Verwaltungspolizei oder der Gerichtspolizei geht. Die Aufträge der Verwaltungspolizei beziehen sich im Wesentlichen auf die Aufrechterhaltung der öffentlichen Ordnung. Die Aufträge der Gerichtspolizei beziehen sich im Wesentlichen auf die Ermittlung und Feststellung von Straftaten.

Der Zugriff auf die personenbezogenen Daten und Informationen, die sowohl durch den sichtbaren als auch nicht sichtbaren Einsatz von Kameras gesammelt wurden, ist während eines Zeitraums von einem Monat ab der Registrierung erlaubt, sofern er in operativer Hinsicht begründet ist und zur Erfüllung eines bestimmten Auftrags notwendig ist. Dieser Zugriff bezieht sich auf die Aufträge der Verwaltungspolizei. Nach dem ersten Monat der Aufbewahrung ist der Zugriff auf diese personenbezogenen Daten und Informationen nur für gerichtspolizeiliche Zwecke und vorbehaltlich einer schriftlichen und mit Gründen versehenen Entscheidung des Prokurators des Königs beziehungsweise im Falle der nicht sichtbaren Kameranutzung des Untersuchungsrichters möglich (Artikel 25/7 und 46/13 des Gesetzes über das Polizeiamt, jeweils eingefügt durch die Artikel 12 und 61 des Gesetzes vom 21. März 2018).

Im Rahmen der automatischen Nummernschilderkennung hat der Gesetzgeber eine noch genauere Unterscheidung vorgenommen. Artikel 44/11/3*decies* §§ 3 und 4 des Gesetzes über das Polizeiamt, eingefügt durch Artikel 35 des Gesetzes vom 21. März 2018, bestimmt:

« § 3. Die Verarbeitung der in § 1 vorgesehenen personenbezogenen Daten und Informationen für gezielte Ermittlungen im Rahmen der verwaltungspolizeilichen Aufträge unter Berücksichtigung der in Artikel 44/11/3^{septies} vorgesehenen Zwecke ist während eines Zeitraums von einem Monat ab der Registrierung erlaubt, sofern sie in operativer Hinsicht begründet ist und für die Erfüllung eines bestimmten Auftrags notwendig ist. Der Beschluss wird entweder von einem Direktor beziehungsweise von den von ihm bestimmten Verwaltungspolizeioffizieren gefasst, wenn es sich um einen Dienst handelt, der zur föderalen Polizei gehört, oder vom Korpschef beziehungsweise von den von ihm bestimmten Verwaltungspolizeioffizieren, wenn es sich um eine Polizeizone handelt.

Die Verarbeitung der in § 1 vorgesehenen personenbezogenen Daten und Informationen für gezielte Ermittlungen im Rahmen der gerichtspolizeilichen Aufträge unter Berücksichtigung der in Artikel 44/11/3^{septies} bestimmten Zwecke ist während des gesamten Zeitraums der Aufbewahrung der Daten erlaubt, sofern sie in operativer Hinsicht begründet ist und für die Erfüllung eines bestimmten Auftrags notwendig ist. Der Beschluss wird entweder von einem Direktor beziehungsweise von den von ihm bestimmten Gerichtspolizeioffizieren gefasst, wenn es sich um einen Dienst handelt, der zur föderalen Polizei gehört, oder vom Korpschef beziehungsweise von den von ihm bestimmten Gerichtspolizeioffizieren, wenn es sich um eine Polizeizone handelt, oder vom Prokurator des Königs. Nach dem ersten Monat der Aufbewahrung wird der Beschluss vom Prokurator des Königs gefasst und kann nur Verstöße betreffen, die eine Hauptkorrektionalgefängnisstrafe von einem Jahr oder eine schwerere Strafe zur Folge haben können.

§ 4. Unter Berücksichtigung der in Artikel 44/11/3^{septies} vorgesehenen Zwecke können die in § 1 vorgesehenen personenbezogenen Daten und Informationen in Korrelation gebracht werden mit:

1. Listen, auf die die Polizeidienste gesetzlich Zugriff haben, oder Auszügen aus nationalen oder internationalen polizeilichen Datenbanken, auf die die Polizeidienste durch oder aufgrund des Gesetzes oder Belgien bindender internationaler Verträge Zugriff haben,

2. im Voraus festgelegten Bewertungskriterien.

Der Inhalt der in Absatz 1 Nr. 1 erwähnten Listen beziehungsweise Auszüge aus Datenbanken, die im Hinblick auf eine Korrelation verwendet werden, unterliegt der Erlaubnis:

1. für verwaltungspolizeiliche Aufträge: entweder eines Direktors beziehungsweise der von ihm bestimmten Verwaltungspolizeioffiziere, wenn es sich um einen Dienst handelt, der zur föderalen Polizei gehört, oder des Korpschefs beziehungsweise der von ihm bestimmten Verwaltungspolizeioffiziere, wenn es sich um eine Polizeizone handelt,

2. für gerichtspolizeiliche Aufträge: entweder eines Direktors beziehungsweise der von ihm bestimmten Gerichtspolizeioffiziere, wenn es sich um einen Dienst handelt, der zur föderalen Polizei gehört, oder des Korpschefs beziehungsweise der von ihm bestimmten Gerichtspolizeioffiziere, wenn es sich um eine Polizeizone handelt, oder des Prokurators des Königs.

Die in Absatz 1 Nr. 2 erwähnten Bewertungskriterien werden nach Billigung durch den Datenschutzbeauftragten festgelegt, dürfen nicht darauf abzielen, eine Person zu identifizieren, und müssen zielgerichtet, verhältnismäßig und bestimmt sein. Die rassische oder ethnische

Herkunft, die religiösen oder weltanschaulichen Überzeugungen, die politischen Meinungen, die Mitgliedschaft in einer Gewerkschaftsorganisation, der Gesundheitszustand, das Sexualleben oder die sexuelle Orientierung einer Person dürfen nicht als Grundlage für diese Kriterien dienen.

Die Listen beziehungsweise Auszüge aus Datenbanken oder die im Voraus festgelegten Bewertungskriterien, die in Korrelation mit den in § 1 vorgesehenen personenbezogenen Daten und Informationen gebracht werden müssen, können vorbereitet werden mit dem Ziel, diese Korrelation in Echtzeit zum Zeitpunkt der Sammlung der Daten durch die intelligenten Kameras oder die intelligenten Systeme für die automatische Nummernschilderkennung oder nach der Registrierung der Daten herzustellen.

Wenn die in Absatz 1 Nr. 1 und 2 erwähnte Korrelation im Rahmen der Erfüllung der verwaltungspolizeilichen Aufträge hergestellt wird, kann sie nur stattfinden:

1. in Echtzeit oder während eines Zeitraums von einem Monat ab der Registrierung der Daten,
2. nach Notifizierung an das Kontrollorgan, wenn es sich um eine Korrelation mit in Absatz 1 Nr. 1 erwähnten Listen beziehungsweise Auszügen aus Datenbanken handelt.

Wenn die in Absatz 1 Nr. 1 und 2 erwähnte Korrelation im Rahmen der Erfüllung der gerichtspolizeilichen Aufträge hergestellt wird, kann sie in Echtzeit oder während der gesamten Dauer der Aufbewahrung der Daten stattfinden. Nach dem ersten Monat der Aufbewahrung kann sie nur mit der Erlaubnis des Prokurators des Königs stattfinden und kann sie nur Verstöße betreffen, die eine Hauptkorrektionalgefängnisstrafe von einem Jahr oder eine schwerere Strafe zur Folge haben können ».

B.9.7. Insbesondere hinsichtlich der Verpflichtung zur Begründung des Zugriffs wird in den Vorarbeiten präzisiert:

« Les règles prévues au niveau du délai de conservation et au niveau de l'accès aux données enregistrées se complètent pour rencontrer cette nécessité de proportionnalité. Il sera donc important de motiver opérationnellement l'accès aux données, même pendant le premier mois. Par ailleurs, l'accès aura lieu conformément aux règles générales en matière de protection de la vie privée qui, comme mentionné plus haut, est d'application. Il sera donc nécessaire de faire état de son ' besoin d'en connaître ' (' need to know '). Les fonctionnaires de police n'y auront donc accès que si elles sont nécessaires à l'exercice d'une mission donnée (intérêt opérationnel). Bien entendu, l'objectif n'est pas que, dans le cadre d'une même enquête, les fonctionnaires de police accèdent, de manière systématique et autonome, aux données à caractère personnel recueillies, dans le délai d'un mois à compter de leur enregistrement. Ceci consisterait en effet à contourner les règles plus strictes qui s'appliquent aux données après le premier mois de conservation. Les fonctionnaires de police veilleront en particulier au respect de ces règles, entre autres à l'aide du login qui est conservé pour chaque accès » (*Parl. Dok., Kammer, 2017-2018, DOC 54-2855/001, SS. 29-30*).

Jeder Zugriff auf die betreffenden Daten muss folglich ausdrücklich unter Beachtung des Verhältnismäßigkeitsgrundsatzes begründet werden. Nach dem ersten Monat der Aufbewahrung ist außerdem in der Regel eine besondere Erlaubnis eines Magistrats erforderlich, der die Einhaltung des vorerwähnten Grundsatzes überwacht.

B.9.8. Schließlich hat der Gesetzgeber Kontrollmechanismen vorgesehen, um die gesammelten Daten und Informationen zu schützen.

Jeder Zugriff wird protokolliert und die konkreten Gründe der Zugriffe werden registriert (Artikel 25/7 § 1 Absatz 3 des Gesetzes über das Polizeiamt, eingefügt durch Artikel 12 des Gesetzes vom 21. März 2018). Auf diese Weise wird « eine Spur in Bezug auf jeden Zugriff auf diese Informationen und den Grund des Zugriffs registriert » (ebenda, S. 30).

Außerdem führt jeder Polizeidienst ein digitales Register mit allen Einsätzen von Kameras und bewahrt die föderale Polizei ein nationales Register mit der Geolokalisierung aller von den Polizeidiensten eingesetzten ortsfesten Kameras auf. Diese Register werden auf Verlangen dem in B.21.4 erwähnten Organ für die Kontrolle der polizeilichen Informationen, den Behörden der Verwaltungspolizei und der Gerichtspolizei und dem Datenschutzbeauftragten im Sinne von Artikel 144 des Gesetzes vom 7. Dezember 1998 « zur Organisation eines auf zwei Ebenen strukturierten integrierten Polizeidienstes » zur Verfügung gestellt (Artikel 25/8 und 46/14 des Gesetzes über das Polizeiamt, jeweils eingefügt durch die Artikel 13 und 62 des Gesetzes vom 21. März 2018). Der nicht sichtbare Kameraeinsatz, der auf bestimmte Fälle beschränkt ist, steht in der Regel unter der besonderen Aufsicht des vorerwähnten Kontrollorgans oder unter der Autorität eines Magistrats (Artikel 46/5 bis 46/11 des Gesetzes über das Polizeiamt, eingefügt durch die Artikel 49, 50, 52, 53, 55, 56 und 58 des Gesetzes vom 21. März 2018).

Schließlich ist jede Datenverarbeitung, die in den technischen Datenbanken durchgeführt wird, in denen die von der automatischen Nummernschilderkennung stammenden Informationen gespeichert werden, « Gegenstand einer Protokollierung, die während zehn Jahren ab der in den technischen Datenbanken durchgeführten Verarbeitung aufbewahrt wird » (Artikel 44/11/3novies des Gesetzes über das Polizeiamt, eingefügt durch Artikel 34 des Gesetzes vom 21. März 2018). Diese Verarbeitung erfolgt gemäß dem Gesetz vom 30. Juli 2018 « über den Schutz natürlicher Personen hinsichtlich der Verarbeitung personenbezogener Daten » (Artikel 44/3 § 1 des Gesetzes über das Polizeiamt, abgeändert durch Artikel 6 des

Gesetzes vom 22. Mai 2019 « zur Abänderung verschiedener Bestimmungen in Bezug auf die Verwaltung der polizeilichen Informationen »). Vor der Einrichtung der technischen Datenbank legt der Verantwortliche dem Datenschutzbeauftragten den Plan für die Einrichtung zur Stellungnahme vor, der « von einer Analyse der Auswirkungen und Risiken auf Ebene des Schutzes des Privatlebens und auf operativer Ebene begleitet [wird], insbesondere in Bezug auf die Kategorien der verarbeiteten personenbezogenen Daten, die Verhältnismäßigkeit der angewandten Mittel, die zu erreichenden operativen Ziele und die Dauer der Aufbewahrung der Daten, die notwendig ist, um diese Ziele zu erreichen » (Artikel 44/11/3*octies* des Gesetzes über das Polizeiamt, eingefügt durch Artikel 33 des Gesetzes vom 21. März 2018).

B.9.9. Bei der Besprechung des Gesetzentwurfs in dem Ausschuss der Kammer hat der zuständige Minister Vorstehendes wie folgt zusammengefasst:

« Durant l'audition, la Commission de la protection de la vie privée a fait remarquer que la durée de conservation de 12 mois pourrait être trop longue. Le ministre souligne que cette question a d'ailleurs donné lieu à un débat animé au sein de la Commission de la protection de la vie privée. Il est vrai qu'un équilibre délicat a dû être trouvé entre les intérêts en présence. D'une part, les services de police ont un besoin opérationnel de pouvoir analyser des images plus d'un mois en arrière, en vue de faire certains constats. D'autre part, le citoyen est assuré du fait que les informations ne seront pas demandées à la légère. Ainsi, les données, issues des caméras, datant de plus d'un mois ne peuvent être consultées qu'à des fins judiciaires et en accord avec le procureur du Roi. Sur avis de la Commission de la protection de la vie privée, il a été décidé d'introduire un seuil (peine d'un an d'emprisonnement concernant les données ANPR). Tout accès nécessite de s'identifier et de compléter les raisons de la demande afin de permettre un contrôle ultérieur.

La proportionnalité est en outre garantie, du fait de l'obligation d'une analyse d'impact et de risque préalable à l'installation de chaque caméra. Dès lors, des caméras ne peuvent pas être placées n'importe où dans le but d'alimenter les banques de données.

Enfin, le ministre ajoute que la durée de conservation de 12 mois constitue une durée maximale : il n'est donc pas obligatoire de conserver les données autant de temps. Le Conseil d'État était également d'avis que ce constat permet de rencontrer le principe de proportionnalité. Il s'agit également de la même durée que celle appliquée pour les données de communication (articles 46*bis* et 88*bis* du Code d'instruction criminelle) » (*Parl. Dok.*, Kammer, 2017-2018, DOC 54-2855/003, SS. 74-75).

Aus den Vorarbeiten geht darüber hinaus hervor, dass der Zugriff auf die gesammelten Daten und Informationen den allgemeinen Regeln betreffend den Schutz natürlicher Personen hinsichtlich der Verarbeitung personenbezogener Daten unterliegt (*Parl. Dok.*, Kammer, 2017-2018, DOC 54-2855/001, S. 29).

B.9.10. Aus dem Vorstehenden ergibt sich, dass der Gesetzgeber in Bezug auf die Regelung des Einsatzes von Kameras im Gesetz über das Polizeiamt und der Aufbewahrung und des Schutzes der auf diese Weise gesammelten Daten durch die darin vorgesehenen Beschränkungen und Garantien bezüglich der Aufbewahrungsfrist ein gerechtes Gleichgewicht zwischen dem Recht auf Achtung des Privatlebens und den verfolgten Zielen der Aufrechterhaltung der öffentlichen Ordnung und der Kriminalitätsbekämpfung geschaffen hat.

B.10.1. Das Kameragesetz regelt in der Fassung seiner Abänderung durch das angefochtene Gesetz den Einsatz von Kameras durch andere Personen als die Polizeidienste. Es unterscheidet zwischen ortsfesten und mobilen Überwachungskameras und sieht jeweils unterschiedliche Regelungen vor, je nach der Art des Ortes, an dem die Kamera eingesetzt wird:

(i) an einem nicht geschlossenen Ort: jeden Ort, der nicht durch eine Umfriedung abgegrenzt ist und der Öffentlichkeit frei zugänglich ist, darunter die öffentlichen Straßen, die von den für das Straßen- und Wegenetz zuständigen öffentlichen Behörden verwaltet werden (Artikel 2 Nr. 1 des Gesetzes vom 21. März 2007),

(ii) an einem der Öffentlichkeit zugänglichen geschlossenen Ort: jedes Gebäude oder jeden Ort, der durch eine Umfriedung abgegrenzt ist, zur Benutzung durch die Öffentlichkeit bestimmt ist und in dem beziehungsweise an dem der Öffentlichkeit Dienste geleistet werden können (Artikel 2 Nr. 2),

(iii) an einem der Öffentlichkeit nicht zugänglichen geschlossenen Ort: jedes Gebäude oder jeden Ort, der durch eine Umfriedung abgegrenzt ist und ausschließlich zur Benutzung durch die gewöhnlichen Benutzer bestimmt ist (Artikel 2 Nr. 3).

B.10.2. In Bezug auf den Einsatz ortsfester und zeitweilig ortsfest angebrachter Überwachungskameras an einem nicht geschlossenen Ort legte Artikel 5 § 4 des Kameragesetzes bereits vor der Abänderung durch das Gesetz vom 21. März 2018 fest, dass das Aufzeichnen von Bildern nur erlaubt ist, um Beweise für ungesellschaftliches Verhalten oder für Handlungen, die eine Straftat darstellen oder einen Schaden begründen, zu sammeln und um Täter, Störer der öffentlichen Ordnung, Zeugen oder Opfer aufzuspüren und zu identifizieren (Absatz 3).

Ferner sah derselbe Paragraph bereits vor, dass diese Bilder, wenn sie nicht dazu beitragen können, den Beweis für eine Straftat, einen Schaden oder ein ungesellschaftliches Verhalten zu

erbringen oder einen Täter, Störer der öffentlichen Ordnung, Zeugen oder ein Opfer zu identifizieren, nicht länger als einen Monat aufbewahrt werden (Absatz 4).

Diesem letzten Absatz, der zum fünften Absatz wird, fügt Artikel 69 Nr. 14 des Gesetzes vom 21. März 2018 folgenden Satz hinzu:

« Diese Frist wird für Orte, die ein besonderes Sicherheitsrisiko darstellen und die der König durch einen im Ministerrat beratenen Königlichen Erlass, dessen Entwurf der Datenschutzbehörde zur Stellungnahme vorgelegt wird, bestimmt, bis auf drei Monate verlängert ».

B.10.3. In Bezug auf den Einsatz ortsfester und zeitweilig ortsfest angebrachter Überwachungskameras an einem für die Öffentlichkeit zugänglichen geschlossenen Ort bestimmte Artikel 6 § 3 des Kameragesetzes bereits vor der Abänderung durch das Gesetz vom 21. März 2018, dass das Aufzeichnen von Bildern nur erlaubt ist, um Beweise für ungesellschaftliches Verhalten oder für Handlungen, die eine Straftat darstellen oder einen Schaden begründen, zu sammeln, und um Täter, Störer der öffentlichen Ordnung, Zeugen oder Opfer aufzuspüren und zu identifizieren (Absatz 2).

Ferner sah derselbe Paragraph bereits vor, dass diese Bilder, wenn sie nicht dazu beitragen können, den Beweis für eine Straftat, einen Schaden oder ein ungesellschaftliches Verhalten zu erbringen oder einen Täter, Störer der öffentlichen Ordnung, Zeugen oder ein Opfer zu identifizieren, nicht länger als einen Monat aufbewahrt werden (Absatz 3).

Diesem letzten Absatz fügt Artikel 70 Nr. 10 des Gesetzes vom 21. März 2018 folgenden Satz hinzu:

« Diese Frist wird für Orte, die aufgrund ihrer Art ein besonderes Sicherheitsrisiko darstellen und die der König durch einen im Ministerrat beratenen Königlichen Erlass, dessen Entwurf der Datenschutzbehörde zur Stellungnahme vorgelegt wird, bestimmt, bis auf drei Monate verlängert ».

B.10.4. In Bezug auf den Einsatz ortsfester und zeitweilig ortsfest angebrachter Überwachungskameras an einem für die Öffentlichkeit nicht zugänglichen geschlossenen Ort bestimmt Artikel 7 § 3 des Kameragesetzes, dass das Aufzeichnen von Bildern nur erlaubt ist, um Beweise für ungesellschaftliches Verhalten oder für Handlungen, die eine Straftat darstellen

oder einen Schaden begründen, zu sammeln, und um Täter, Störer der öffentlichen Ordnung, Zeugen oder Opfer aufzuspüren und zu identifizieren (Absatz 2).

Ferner sah derselbe Paragraph bereits vor der Abänderung durch das Gesetz vom 21. März 2018 vor, dass diese Bilder, wenn sie nicht dazu beitragen können, den Beweis für eine Straftat, einen Schaden oder ein ungesellschaftliches Verhalten zu erbringen oder einen Täter, Störer der öffentlichen Ordnung, Zeugen oder ein Opfer zu identifizieren, nicht länger als einen Monat aufbewahrt werden (nunmehr Absatz 3).

Diesem letzten Absatz fügt Artikel 71 Nr. 16 des Gesetzes vom 21. März 2018 folgenden Satz hinzu:

« Diese Frist wird für Orte, die aufgrund ihrer Art ein besonderes Sicherheitsrisiko darstellen und die der König durch einen im Ministerrat beratenen Königlichen Erlass, dessen Entwurf der Datenschutzbehörde zur Stellungnahme vorgelegt wird, bestimmt, bis auf drei Monate verlängert ».

B.10.5. In Bezug auf den Einsatz mobiler Überwachungskameras an geschlossenen oder nicht geschlossenen Orten durch oder im Auftrag kommunaler Behörden führt das angefochtene Gesetz eine ähnliche Regelung ein.

Artikel 7/3 § 4 des Gesetzes vom 21. März 2007, eingefügt durch Artikel 75 des Gesetzes vom 21. März 2018, bestimmt:

« Das Aufzeichnen von Bildern ist nur erlaubt, um Beweise für ungesellschaftliches Verhalten oder für Handlungen, die eine Straftat darstellen oder einen Schaden begründen, zu sammeln und um Täter, Störer der öffentlichen Ordnung, Zeugen oder Opfer aufzuspüren und zu identifizieren.

Wenn diese Bilder nicht dazu beitragen können, den Beweis für einen Verstoß, einen Schaden oder ein ungesellschaftliches Verhalten zu erbringen oder einen Täter, Störer der öffentlichen Ordnung, Zeugen oder ein Opfer zu identifizieren, dürfen sie nicht länger als einen Monat aufbewahrt werden. Diese Frist wird für Orte, die aufgrund ihrer Art ein besonderes Sicherheitsrisiko darstellen und die der König durch einen im Ministerrat beratenen Königlichen Erlass, dessen Entwurf der Datenschutzbehörde zur Stellungnahme vorgelegt wird, bestimmt, bis auf drei Monate verlängert ».

B.10.6. Für die erwähnten Formen der Kameranutzung gilt folglich eine ähnliche Regelung. Die maximale Aufbewahrungsfrist von einem Monat kann hinsichtlich bestimmter Orte bis auf drei Monate verlängert werden.

Aus den angeführten Bestimmungen ergibt sich, dass diese Regelung Beschränkungen unterliegt.

Zunächst ist das Aufzeichnen von Bildern nur bei Vorliegen eines bestimmten Zwecks erlaubt, nämlich um Beweise für ungesellschaftliches Verhalten oder für Handlungen, die eine Straftat darstellen oder einen Schaden begründen, zu sammeln und um Täter, Störer der öffentlichen Ordnung, Zeugen oder Opfer aufzuspüren und zu identifizieren.

Ferner beträgt die gewöhnliche Aufbewahrungsfrist weiterhin höchstens einen Monat und ist die Möglichkeit zur Verlängerung dieser Frist auf Orte beschränkt, die aufgrund ihrer Art ein besonderes Sicherheitsrisiko darstellen. Es obliegt dem König, diese Orte zu bestimmen. Aus den Vorarbeiten geht hervor, dass sich die Maßnahme insbesondere auf Orte wie Bahnhöfe, Flughäfen und Hafeneinrichtungen bezieht « oder andere Orte, die ein Anschlagziel für Terroristen sein können, wie die Orte, an denen Wachleute ihre situationsbezogene Befugnisse ausüben können, wie in Bezug auf Standorte von Atomkraftwerken, internationale Einrichtungen, Militärgelände usw. » (*Parl. Dok.*, Kammer, 2017-2018, DOC 54-2855/001, SS. 18 und 77, und DOC 54-2855/003, S. 11).

Der Gesetzgeber hat die vorerwähnte Ermächtigung zugunsten des Königs nicht nur inhaltlich auf ausreichend klare Weise beschränkt, sondern auch im Rahmen des Zustandekommens der Königlichen Erlasse besondere Garantien vorgesehen: diese müssen im Ministerrat beraten werden und der Datenschutzbehörde zur Stellungnahme vorgelegt werden.

Schließlich geht es um eine Frist, die im Rahmen der Anwendung des Verhältnismäßigkeitsgrundsatzes durch den Verantwortlichen für die Verarbeitung der Bilder als oberste Grenze anzusehen ist.

B.10.7. In den Vorarbeiten wird Vorstehendes wie folgt zusammengefasst und werden die Gründe der Maßnahme erläutert:

« Enfin, en ce qui concerne la durée de conservation des images, il est proposé de l'allonger d'un à trois mois, dans certains cas spécifiques. Après dix années d'application de cette loi, l'on constate en effet que ce délai maximum d'un mois n'est parfois pas suffisamment long et empêche, dans des cas où les images auraient pu être décisives, d'obtenir une preuve ou d'identifier des auteurs de faits ou des témoins. L'objectif n'est bien évidemment pas d'obliger les responsables du traitement à conserver les images pendant une durée de trois mois, mais d'offrir la possibilité, quand cela se justifie du point de vue de la proportionnalité, de les conserver pendant trois mois. C'est pourquoi cette possibilité n'est prévue que pour les lieux présentant un risque particulier pour la sécurité, déterminés par le Roi, par un arrêté royal délibéré en Conseil des ministres et dont le projet sera soumis pour avis à l'Autorité de protection des données. En dehors de ces cas qui seront déterminés par le Roi, le délai de conservation reste inchangé » (*Parl. Dok.*, Kammer, 2017-2018, DOC 54-2855/001, S. 75).

B.10.8. Aus dem Vorgenannten geht hervor, dass der Gesetzgeber in Bezug auf die Regelung des Einsatzes von Kameras im Kameragesetz durch die darin vorgesehenen Beschränkungen und Garantien bezüglich der Aufbewahrungsfrist ein gerechtes Gleichgewicht zwischen dem Recht auf Achtung des Privatlebens und den verfolgten Zielen der Aufrechterhaltung der öffentlichen Ordnung und der Kriminalitätsbekämpfung geschaffen hat.

B.11. Der erste Klagegrund ist unbegründet.

B.12. Im ersten Teil des zweiten Klagegrundes macht die klagende Partei einen unverhältnismäßigen Eingriff in das Recht auf Achtung des Privatlebens geltend, weil die im angefochtenen Gesetz vorgesehenen Maßnahmen nicht auf Fälle schwerwiegender Kriminalität oder gewichtige Gründe der öffentlichen Ordnung oder Sicherheit beschränkt seien. Es habe insbesondere zum Ziel (i) die Gestattung des Einsatzes nicht sichtbarer polizeilicher Kameras, (ii) den Zugriff der Polizeidienste und der Nachrichten- und Sicherheitsdienste auf die aufgrund des angefochtenen Gesetzes aufbewahrten Daten, (iii) die Ermächtigung der Polizeidienste und der Nachrichten- und Sicherheitsdienste, diese Daten in Korrelation mit anderen im Gesetz angeführten Daten zu bringen, (iv) die Ermächtigung der Nachrichten- und Sicherheitsdienste, über diesen Zugriff und diese Korrelation eine Observation mittels technischer Mittel durchzuführen.

Im zweiten Teil des zweiten Klagegrundes macht die klagende Partei einen unverhältnismäßigen Eingriff in das Recht auf Achtung des Privatlebens geltend, weil die vorerwähnten Gestattungen und Ermächtigungen keiner vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde unterworfen seien.

B.13.1. Der Einsatz nicht sichtbarer polizeilicher Kameras ist nach Artikel 46/4 des Gesetzes über das Polizeiamt, eingefügt durch Artikel 48 des angefochtenen Gesetzes, bei Vorliegen besonderer Umstände erlaubt:

« In Abweichung von Artikel 25/3 können zeitweilig ortsfest angebrachte und mobile Kameras, gegebenenfalls intelligente Kameras, vorbehaltlich einer Erlaubnis an nicht geschlossenen Orten und der Öffentlichkeit zugänglichen geschlossenen Orten auf nicht sichtbare Weise eingesetzt werden, wenn die Umstände es nicht zulassen, dass die Polizeibeamten identifiziert werden können, und derart sind, dass ein sichtbarer Einsatz von Kameras ineffizient würde, und wenn es um eine der folgenden Situationen geht:

1. in Artikel 22 Absatz 2 vorgesehene Situationen,

2. Sammlung der in Artikel 44/5 § 1 Absatz 1 Nr. 2 und 3 vorgesehenen verwaltungspolizeilichen Informationen, sofern es dabei um Folgendes geht:

a) radikalisierte Personen im Sinne von Artikel 3 Nr. 15 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste,

b) Personen, für die begründete und schwerwiegende Indizien vorliegen, dass sie sich in ein Gebiet begeben wollen, wo terroristische Vereinigungen, wie in Artikel 139 des Strafgesetzbuches bestimmt, aktiv sind, unter Bedingungen, die darauf schließen lassen, dass sie bei ihrer Rückkehr nach Belgien eine ernsthafte Bedrohung im Zusammenhang mit terroristischen Straftaten, wie in Artikel 137 des Strafgesetzbuches bestimmt, darstellen können oder dass diese Personen vorhaben, außerhalb des nationalen Hoheitsgebiets terroristische Straftaten, wie in Artikel 137 des Strafgesetzbuches bestimmt, zu begehen,

3. Einsatz auf einem Transportmittel der Polizei, das nicht als solches erkennbar ist, für die automatische Nummernschilderkennung, um gemeldete Fahrzeuge aufzuspüren ».

Die in Artikel 22 Absatz 2 geregelten Situationen beziehen sich auf das Zerstreuen verschiedener Arten von Menschaufläufen: (1) bewaffneten Aufläufen, (2) Aufläufen, die mit Verbrechen und Vergehen gegen Personen oder Güter oder mit Verstößen gegen das Gesetz vom 29. Juli 1934 « über das Verbot von Privatmilizen » einhergehen, (3) Aufläufen, bei denen zu erkennen ist, dass sie im Hinblick auf Verwüstung, Mord oder Plünderung oder im Hinblick auf einen Anschlag auf die körperliche Unversehrtheit oder das Leben von Personen gebildet worden sind beziehungsweise sich zu diesem Zweck bilden, und (4) Aufläufen, die sich der Durchführung des Gesetzes, einer Polizeiverordnung, einer polizeilichen Maßnahme, einer gerichtlichen Entscheidung oder einer Zwangsmaßnahme widersetzen.

Die verwaltungspolizeilichen Informationen im Sinne von Artikel 44/5 § 1 Absatz 1 Nrn. 2 und 3 betreffen (1) Daten in Bezug auf Personen, die von verwaltungspolizeilichen

Phänomenen betroffen sind, das heißt von allen Problemen, die eine Störung der öffentlichen Ordnung darstellen und angepasste verwaltungspolizeiliche Maßnahmen notwendig machen, weil sie gleicher Art sind und wiederkehren, von denselben Personen begangen werden oder gegen dieselben Kategorien von Opfern oder Orten gerichtet sind, und (2) Daten in Bezug auf Mitglieder einer nationalen oder internationalen Gruppierung, die die in Artikel 14 erwähnte öffentliche Ordnung stören könnten. Die Gewinnung von Informationen zu diesen Daten ist außerdem auf die ausdrücklich in Artikel 46/4 Nr. 2 erwähnten Personen beschränkt, die auf unzweideutige Weise mit Terrorismus in Verbindung gebracht werden können.

Die angefochtene Bestimmung regelt die besonderen Umstände, unter denen der Einsatz nicht sichtbarer polizeilicher Kameras erlaubt ist, folglich genau.

In seinem Entscheid Nr. 108/2016 vom 14. Juli 2016 hat der Gerichtshof im Übrigen entschieden, dass die in Artikel 44/5 § 1 Absatz 1 Nrn. 2 und 3 des Gesetzes über das Polizeiamt genannten Kategorien hinreichend genau sind (B.20-B.32).

B.13.2. Der Zugriff der Polizeidienste auf die aufgrund des angefochtenen Gesetzes aufbewahren Daten ist ebenso in den in B.9.6 erwähnten Bestimmungen genau geregelt.

Die Nachrichten- und Sicherheitsdienste haben Zugriff auf die aufgrund des angefochtenen Gesetzes aufbewahrten Daten, sofern dies in operativer Hinsicht begründet ist, zur Erfüllung eines bestimmten Auftrags notwendig ist und von einem Nachrichtenoffizier beschlossen wird. Nach dem ersten Monat der Aufbewahrung ist die Erlaubnis vom Dienstleiter oder von seinem Beauftragten erforderlich (Artikel 16/4 § 2 Absätze 1 und 2 des Gesetzes über die Nachrichten- und Sicherheitsdienste, eingefügt durch Artikel 84 des Gesetzes vom 21. März 2018). Der Zugriff muss außerdem « zielgerichtet » erfolgen, was nicht der Fall ist, « wenn der Bereich und die Dauer nicht auf verhältnismäßige Weise beschränkt sind. Zielgerichtet ist etwa die Abfrage, die sich auf eine bestimmte Einzelgarage und einen diesbezüglichen Zeitraum von zwei Monaten bezieht, um dort die Passagen von Mitgliedern eines terroristischen Netzwerks zu überprüfen. Oder auch eine Datenbankabfrage, um in Erfahrung zu bringen, ob Nummernschild X am Ort Y zum Zeitpunkt Z registriert worden ist » (*Parl. Dok.*, Kammer, 2017-2018, DOC 54-2855/001, S. 104).

Der Beschluss des Dienstleiters beziehungsweise seines Beauftragten wird mit der Begründung dieses Beschlusses schnellstmöglich dem Ständigen Ausschuss für die Kontrolle über die Nachrichten- und Sicherheitsdienste N (Ständiger Ausschuss N) übermittelt. Der Beschluss kann eine Gesamtheit von Daten in Bezug auf eine spezifische nachrichtendienstliche Untersuchung betreffen. In diesem Fall wird dem Ständigen Ausschuss N einmal pro Monat eine Liste der zielgerichteten Abfragen übermittelt. Der Ständige Ausschuss N verbietet den Nachrichten- und Sicherheitsdiensten, die Daten zu benutzen, die unter Bedingungen gesammelt worden sind, die die gesetzlichen Bedingungen nicht einhalten (Artikel 16/4 § 2 Absatz 3 des Gesetzes über die Nachrichten- und Sicherheitsdienste, eingefügt durch Artikel 84 des Gesetzes vom 21. März 2018).

Daneben übt der Ständige Ausschuss N seine allgemeine Kontrollbefugnis aus:

« Le Comité permanent R assure d'ailleurs un contrôle effectif. Ce sera spécifiquement rendu possible par le fait que chaque décision du dirigeant du service lui est notifiée. Cet organe de contrôle possède de larges compétences si une irrégularité est constatée. Il peut notamment ordonner la cessation de la méthode ainsi que l'interdiction de l'exploitation des données collectées et en même leur destruction. Une destruction s'étend également à toutes les mentions de ces données, par exemple dans des notes internes, de sorte que ces données ne peuvent plus être utilisées comme base de la mise en œuvre d'une nouvelle méthode de collecte. Pour ces raisons, les auteurs du projet de loi ne sont pas d'accord avec la remarque du Comité R selon laquelle la destruction n'aurait qu'une valeur symbolique.

Il existe aussi des règles internes qui contrent les abus. Ainsi, chaque collaborateur des services de renseignement et de sécurité fait l'objet d'une enquête de sécurité tous les 5 ans. En outre, tous les traitements sur des banques de données des services-mêmes ou d'autres services sont loggés; ceux-ci font l'objet d'un contrôle exercé par le bureau de sécurité de la VSSE et du SGRS et par le Comité permanent R. En plus, un collaborateur n'a accès qu'aux données qui sont en lien avec sa propre fonction, donc sur une base du principe du ' *need to know* ' (besoin d'en connaître), et seulement aux données qui peuvent être en relation avec des menaces bien déterminées pour lesquelles les services de renseignement et de sécurité sont compétents. Par ailleurs, les données que les services de renseignement obtiennent des caméras sont enregistrées dans un système sécurisé, voire classifié dès qu'elles sont traitées. Ceci renforce les prescriptions de sécurité avec lesquelles les données doivent être traitées. Enfin, un citoyen peut introduire une plainte à tout moment auprès de la Commission de la protection de la vie privée ou auprès du Comité permanent R, après quoi ces institutions peuvent procéder à une enquête. Le Comité permanent R peut aussi d'office et d'initiative procéder à une enquête. La VSSE et le SGRS sont tenus de prêter leur entière collaboration » (ebenda, SS. 106-107).

Der Zugriff auf die Informationen und personenbezogenen Daten ist geschützt, jeder Zugriff wird protokolliert und die konkreten Gründe der Zugriffe werden gespeichert

(Artikel 16/4 § 2 Absatz 4 des Gesetzes über die Nachrichten- und Sicherheitsdienste, eingefügt durch Artikel 84 des Gesetzes vom 21. März 2018).

B.13.3. Die Ermächtigung zugunsten der Polizeidienste, die aufbewahrten Daten mit anderen im Gesetz genannten Daten in Korrelation zu bringen, ist in dem in B.9.6 erwähnten Artikel 44/11/3*decies* § 4 des Gesetzes über das Polizeiamt, eingefügt durch Artikel 35 des Gesetzes vom 21. März 2018, genau geregelt.

Der Gesetzgeber hat die Nachrichten- und Sicherheitsdienste auf ähnliche Weise ermächtigt, die Daten aus den technischen Datenbanken in Korrelation zu bringen mit anderen Datenbanken, die sie selbst verwalten oder die ihnen zur Verfügung stehen oder zugänglich sind, mit Personenlisten, die sie im Rahmen ihrer Aufträge erstellen, oder mit im Voraus festgelegten Bewertungskriterien (Artikel 16/4 § 3 des Gesetzes über die Nachrichten- und Sicherheitsdienste, eingefügt durch Artikel 84 des Gesetzes vom 21. März 2018).

B.13.4. Schließlich ermächtigt das angefochtene Gesetz die Nachrichten- und Sicherheitsdienste, über einen Zugriff auf die betreffenden Daten und gegebenenfalls über die diesbezügliche Korrelation mit anderen erwähnten Daten eine Observation mit Hilfe von technischen Mitteln durchzuführen (Artikel 18/4 und 1811 des Gesetzes über die Nachrichten- und Sicherheitsdienste, eingefügt durch die Artikel 85 und 86 des Gesetzes vom 21. März 2018).

B.14.1. Die angefochtenen Gestattungen und Ermächtigungen sind in den vorerwähnten Bestimmungen auf klare Weise festgelegt. Sie sollen dazu beitragen, die öffentliche Sicherheit zu gewährleisten, die öffentliche Ordnung zu schützen, Straftaten zu verhüten und die Rechte und Freiheiten anderer zu wahren. Die Maßnahmen entsprechen folglich einem zwingenden gesellschaftlichen Bedürfnis in einer demokratischen Gesellschaft.

B.14.2. Die angefochtenen Gestattungen und Ermächtigungen unterliegen außerdem Beschränkungen.

B.14.3. Der Einsatz nicht sichtbarer polizeilicher Kameras kann nur für spezifische Zwecke erlaubt werden und wenn die Umstände es nicht zulassen, dass die Polizeibeamten identifiziert werden können, oder derart sind, dass ein sichtbarer Einsatz von Kameras

ineffizient würde. Der Einsatz wird von Fall zu Fall und immer für eine begrenzte Dauer vom Generalkommissar der föderalen Polizei oder dem Korpschef der lokalen Polizeizone, in bestimmten Fällen nach einer vorherigen verbindlichen Stellungnahme des Prokurators des Königs und der Staatssicherheit, erlaubt (Artikel 46/5 des Gesetzes über das Polizeiamt, eingefügt durch Artikel 79 des Gesetzes vom 21. März 2018). Der nicht sichtbare Einsatz steht in der Regel unter der besonderen Aufsicht des Kontrollorgans oder unter der Autorität eines Magistrats.

B.14.4. Der Zugriff der Polizeidienste auf die aufgrund des angefochtenen Gesetzes aufbewahrten Daten ist zeitlich begrenzt, muss in bestimmten Fällen von einem Magistrat erlaubt werden und unterliegt einer strikten Registrierung und einer Analyse der Auswirkungen und Risiken auf Ebene des Schutzes des Privatlebens. Ähnliche Beschränkungen gelten für den Zugriff durch die Nachrichten- und Sicherheitsdienste. Jedenfalls muss der Grundsatz der Verhältnismäßigkeit immer beachtet werden.

B.14.5. Die Ermächtigung zugunsten der Polizeidienste, die aufbewahrten Daten mit anderen im Gesetz genannten Daten in Korrelation zu bringen, gilt nur für die Daten aus den technischen Datenbanken, die von der automatischen Nummernschilderkennung stammenden Informationen enthalten und die mit genau beschriebenen anderen Daten in Verbindung gebracht werden können, für eine begrenzte Dauer und bei Vorliegen der vorgeschriebenen Gestattungen und Kontrollen. Ähnliche Beschränkungen gelten für den Zugriff durch die Nachrichten- und Sicherheitsdienste. Auch in diesem Fall muss immer der Grundsatz der Verhältnismäßigkeit beachtet werden.

B.14.6. Die Ermächtigung zugunsten der Nachrichten- und Sicherheitsdienste, über einen Zugriff auf die betreffenden Daten und gegebenenfalls über die diesbezügliche Korrelation mit anderen erwähnten Daten eine Observation mit Hilfe von technischen Mitteln durchzuführen, unterliegt denselben Bedingungen wie andere Methoden für das Sammeln von Daten im Sinne des Gesetzes über die Nachrichten- und Sicherheitsdienste.

Der Ständige Ausschuss N befindet über die Rechtmäßigkeit der Entscheidungen über diese Methoden sowie über die Einhaltung des Subsidiaritätsgrundsatzes und des Verhältnismäßigkeitsgrundsatzes (Artikel 43/2 Absatz 2 des Gesetzes über die

Nachrichten- und Sicherheitsdienste) (Artikel 43/2 Absatz 2 des Gesetzes über die Nachrichten- und Sicherheitsdienste).

B.14.7. Aus diesen Beschränkungen, durch die der Zugriff auf die aufbewahrten Daten und ihre Nutzung kontrolliert werden sollen, geht hervor, dass der Gesetzgeber ein gerechtes Gleichgewicht zwischen dem Recht auf Achtung des Privatlebens und den verfolgten Zielen der Aufrechterhaltung der öffentlichen Ordnung und der Kriminalitätsbekämpfung geschaffen hat.

Die bloße Feststellung, dass die angefochtenen Gestattungen und Ermächtigungen nicht auf Fälle schwerwiegender Kriminalität oder gewichtige Gründe der öffentlichen Ordnung oder Sicherheit beschränkt seien und dass sie keiner vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde unterworfen seien, lässt dies unberührt.

B.15. Der erste und der zweite Teil des zweiten Klagegrunds sind unbegründet.

In Bezug auf das Legalitätsprinzip

B.16. Im dritten Teil des zweiten Klagegrundes macht die klagende Partei einen Verstoß gegen das Legalitätsprinzip im Sinne von Artikel 22 der Verfassung aufgrund der weitreichenden Ermächtigung zugunsten des Ministers des Innern und der Justiz, Maßnahmen in Bezug auf die Verknüpfungen und die Korrelationen mit den technischen Datenbanken festzulegen (Artikel 28 des Gesetzes vom 21. März 2018), und des Königs, den unmittelbaren Zugriff der Sicherheits- und Nachrichtendienste auf die durch die polizeiliche Kameranutzung gesammelten Daten zu regeln (Artikel 84 desselben Gesetzes), geltend.

B.17. Indem Artikel 22 der Verfassung dem zuständigen Gesetzgeber die Befugnis vorbehält, festzulegen, in welchen Fällen und unter welchen Bedingungen vom Recht auf Achtung des Privatlebens abgewichen werden kann, gewährleistet er einem jedem Bürger, dass keinerlei Einmischung in dieses Recht erfolgen darf, außer aufgrund von Regeln, 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.18.1. Artikel 44/4 § 4 des Gesetzes über das Polizeiamt, eingefügt durch Artikel 28 des Gesetzes vom 21. März 2018, bestimmt:

« Der Minister des Innern und der Minister der Justiz bestimmen anhand von gemeinsamen Richtlinien die angemessenen, sachdienlichen und nicht übertriebenen Maßnahmen in Bezug auf die Verknüpfung oder die Korrelation zwischen den in Artikel 44/2 § 3 erwähnten technischen Datenbanken und den in Artikel 44/2 §§ 1 und 2 erwähnten Datenbanken oder anderen Datenbanken, auf die die Polizeidienste durch oder aufgrund des Gesetzes oder Belgien bindender internationaler Verträge Zugriff haben.

Diese gemeinsamen Richtlinien berücksichtigen die Kriterien Zeit, Raum und Häufigkeit der Verknüpfungen oder Korrelationen. Sie bestimmen mindestens die Behörde, die solche Maßnahmen bewilligt, und die Datenbanken, die miteinander verknüpft werden können ».

B.18.2 Artikel 44/4 des Gesetzes über das Polizeiamt wurde mittlerweile mit Wirkung zum 29. Juni 2019 durch Artikel 7 des Gesetzes vom 22. Mai 2019 « zur Abänderung verschiedener Bestimmungen in Bezug auf die Verwaltung der polizeilichen Informationen » ersetzt.

B.18.3. Da nicht feststeht, dass Artikel 44/4 des Gesetzes über das Polizeiamt, abgeändert durch Artikel 28 des Gesetzes vom 21. März 2018, vor dem 29. Juni 2019 angewandt worden ist, ist der dritte Teil des zweiten Klagegrundes gegenstandslos, sofern er sich auf diese Bestimmung bezieht.

B.19.1. Artikel 16/4 § 1 Absatz 1 des Gesetzes über die Nachrichten- und Sicherheitsdienste, eingefügt durch Artikel 84 des Gesetzes vom 21. März 2018, bestimmt:

« Gemäß den Modalitäten, die vom König nach Stellungnahme der für die Aufsicht über die Verarbeitung personenbezogener Daten zuständigen Behörde festgelegt werden, ist für die Nachrichten- und Sicherheitsdienste ein direkter Zugriff auf die Informationen und personenbezogenen Daten erlaubt, die mittels Kameras gesammelt worden sind, deren Einsatz durch die Polizeidienste gemäß Kapitel 4 Abschnitt 1 und Kapitel 4/1 Abschnitt 2 des Gesetzes über das Polizeiamt erlaubt ist, und die insbesondere in den in Artikel 44/2 desselben Gesetzes erwähnten Datenbanken verarbeitet werden ».

B.19.2. In den Vorarbeiten wird näher erläutert, dass der König die Modalitäten des Zugriffs aufgrund dieser Bestimmung festlegen wird:

« Il faudra notamment déterminer des règles générales quant à l'enregistrement des accès effectués par les membres des services de renseignement et de sécurité » (*Parl. Dok.*, Kammer, 2017-2018, DOC 54-2855/001, S. 102).

B.19.3. Da die Zugriffsvoraussetzungen vom Gesetzgeber selbst genau geregelt sind, wie sich aus B.13.2 ergibt, ist der dritte Teil des zweiten Klagegrundes unbegründet.

In Bezug auf den Gleichheitsgrundsatz

B.20. Im vierten Teil des zweiten Klagegrundes macht die klagende Partei einen Verstoß gegen den Grundsatz der Gleichheit und Nichtdiskriminierung geltend, weil für das Inkorrelationbringen von Daten im Sinne von Artikel 44/11/3*decies* § 4 des Gesetzes über das Polizeiamt in der Fassung der Einfügung durch Artikel 35 des Gesetzes vom 21. März 2018 nicht dieselben Garantien wie im Rahmen des Artikels 47*sexies* des Strafprozessgesetzbuches gälten. Dadurch sei auch das strafrechtliche Legalitätsprinzip verletzt. Da das Gesetz vom 21. März 2018 auch keine wirksame gerichtliche Kontrolle in Bezug auf die Korrelation und den Zugriff auf die Daten vorsehe, verletze es darüber hinaus das Recht auf ein faires Verfahren und das Verteidigungsrecht.

B.21.1. Unter engen, in B.9.6 erwähnten Voraussetzungen erlaubt Artikel 44/11/3*decies* § 4 des Gesetzes über das Polizeiamt es den Polizeidiensten, die von der automatischen Nummernschilderkennung stammenden und in technischen Datenbanken enthaltenen Informationen in Korrelation zu bringen mit (1) Listen, auf die die Polizeidienste gesetzlich Zugriff haben, oder Auszügen aus nationalen oder internationalen polizeilichen Datenbanken, auf die die Polizeidienste durch oder aufgrund des Gesetzes oder Belgien bindender internationaler Verträge Zugriff haben, und (2) im Voraus festgelegten Bewertungskriterien.

Diese Korrelation hat zum Ziel « Alarmsignale (Hits) zu generieren und kann in Echtzeit oder *a posteriori* stattfinden, nachdem die ANPR-Kameras oder [das] ANPR-Erkennungssystem die Daten registriert haben » (ebenda, S. 43).

B.21.2. Artikel 47*sexies* § 1 des Strafprozessgesetzbuches sieht die Observation als besondere Ermittlungsmethode vor. Bei der Observation handelt es sich um die systematische Beobachtung einer oder mehrerer Personen, ihrer Anwesenheit oder ihres Verhaltens oder bestimmter Sachen, Orte oder Geschehnisse durch einen Polizeibeamten. Bei einer systematischen Observation handelt es sich um eine Observation an mehr als fünf aufeinander folgenden Tagen oder an mehr als fünf nicht aufeinander folgenden Tagen verteilt über einen Zeitraum von einem Monat, um eine Observation, bei der technische Mittel verwendet werden, um eine Observation mit internationalem Charakter oder um eine Observation, die von Spezialeinheiten der föderalen Polizei durchgeführt wird.

Der Prokurator des Königs kann im Rahmen der Ermittlung eine Observation genehmigen, wenn die Untersuchung dies erfordert und wenn die anderen Untersuchungsmittel nicht auszureichen scheinen, um die Wahrheit herauszufinden (Artikel 47*sexies* § 2 Absatz 1). Die Genehmigung zur Observation erfolgt schriftlich und ist mit Gründen versehen (Artikel 47*sexies* § 3).

B.21.3. Das Inkorrelationbringen in Bezug auf bestimmte Daten stellt anders als die Observation keine besondere Ermittlungsmethode dar. Die Observation hat in der Regel das Sammeln neuer Daten zum Ziel, während sich das Inkorrelationbringen auf bestehende Daten bezieht, die auf eine Weise gesammelt wurden, die, wie sich aus der Prüfung des ersten Klagegrundes ergibt, mit hinreichenden Garantien versehen ist.

Es ist deshalb sachlich gerechtfertigt, dass für beide Techniken nicht dieselben Garantien gelten.

Wie in B.9.7 erwähnt wurde, muss außerdem jeder Zugriff auf die betreffenden Daten unter Beachtung des Verhältnismäßigkeitsgrundsatzes ausdrücklich begründet werden.

B.21.4. Gemäß Artikel 71 des Gesetzes vom 30. Juli 2018 « über den Schutz natürlicher Personen hinsichtlich der Verarbeitung personenbezogener Daten » wird bei der Abgeordnetenversammlung ein unabhängiges Aufsichtsorgan für die polizeilichen Informationen geschaffen, Organ für die Kontrolle der polizeilichen Informationen genannt, das mit der Kontrolle der Verarbeitung der Informationen und der Daten im Sinne von Artikel 44/1 des

Gesetzes über das Polizeiamt einschließlich solcher, die in die Datenbanken im Sinne von 44/2 aufgenommen wurden, beauftragt ist.

Aus dieser Bestimmung geht hervor, dass die Kontrollbefugnis, die dem Organ für die Kontrolle der polizeilichen Informationen eingeräumt wird, allgemeiner Natur ist in dem Sinne, dass alle Informationen und personenbezogenen Daten, die durch die Polizeidienste verarbeitet werden, durch das Kontrollorgan überprüft werden können (Artikel 44/1) und dass dieses Organ befugt ist, alle polizeilichen Datenbanken zu kontrollieren (Artikel 44/2).

Das Kontrollorgan überprüft mittels einer Untersuchung der Arbeitsweise, ob der Inhalt der Allgemeinen Nationalen Datenbank, der Basisdatenbanken, der besonderen Datenbanken und der technischen Datenbanken sowie das Verfahren für die Verarbeitung der darin aufbewahrten Daten und Informationen den Regelungen in den Artikeln 44/1 bis 44/11/13 des Gesetzes über das Polizeiamt und den diesbezüglichen Ausführungsmaßnahmen entsprechen (Artikel 239 des vorerwähnten Gesetzes vom 30. Juli 2018). Das Kontrollorgan wird von Amts wegen oder auf Antrag bestimmter Behörden tätig (Artikel 237 desselben Gesetzes).

B.21.5. Da das Inkorrelationbringen von Daten keine besondere Ermittlungsmethode ist, ist die Anklagekammer bei einem Abschluss der Ermittlungen nicht dafür zuständig, diese Technik einer Kontrolle zu unterwerfen.

Wie jedes staatliche Handeln kann auch das Inkorrelationbringen bestimmter Daten durch die Polizeidienste einer gerichtlichen Kontrolle unterworfen werden. Der zuständige Richter muss bei der Überprüfung der Rechtmäßigkeit der Maßnahme die Einhaltung des Verhältnismäßigkeitsgrundsatzes prüfen.

B.21.6. Die klagende Partei legt schließlich nicht dar, auf welche Weise die angefochtene Bestimmung das strafrechtliche Legalitätsprinzip verletzt.

B.22. Der vierte Teil des zweiten Klagegrunds ist unbegründet.

Aus diesen Gründen:

Der Gerichtshof

weist die Klage zurück.

Erlassen in niederländischer, französischer und deutscher Sprache, gemäß Artikel 65 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof, am 20. Februar 2020.

Der Kanzler,

Der Präsident,

F. Meersschant

A. Alen