Geschäftsverzeichnisnr. 6711
Entscheid Nr. 174/2018 vom 6. Dezember 2018

E N T S C H E I D

In Sachen: Klage auf Nichtigerklärung der Artikel 2 und 7 des Gesetzes vom 25. Dezember 2016 « zur Festlegung verschiedener Abänderungen des Strafprozessgesetzbuches und des Strafgesetzbuches im Hinblick auf die Verbesserung der besonderen Ermittlungsmethoden und bestimmter Ermittlungsmaßnahmen in Sachen Internet, elektronische Nachrichten und Telekommunikation und zur Schaffung einer Datenbank der Stimmabdrücke », erhoben von der VoG « Ligue des Droits de l'Homme » und der VoG « Liga voor Mensenrechten ».

Der Verfassungsgerichtshof,

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

erlässt nach Beratung folgenden Entscheid:

*

* *

I. *Gegenstand der Klage und Verfahren*

Mit einer Klageschrift, die dem Gerichtshof mit am 17. Juli 2017 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 19. Juli 2017 in der Kanzlei eingegangen ist, erhoben Klage auf Nichtigerklärung der Artikel 2 und 7 des Gesetzes vom 25. Dezember 2016 « zur Festlegung verschiedener Abänderungen des Strafprozessgesetzbuches und des Strafgesetzbuches im Hinblick auf die Verbesserung der besonderen Ermittlungsmethoden und bestimmter Ermittlungsmaßnahmen in Sachen Internet, elektronische Nachrichten und Telekommunikation und zur Schaffung einer Datenbank der Stimmabdrücke » » (veröffentlicht im *Belgischen Staatsblatt* vom 17. Januar 2017): die VoG « Ligue des Droits de l'Homme » und die VoG « Liga voor Mensenrechten », unterstützt und vertreten durch RA D. Ribant und RÄin C. Forget, in Brüssel zugelassen, und durch RA J. Heymans, in Gent zugelassen, und RA J. Vander Velpen, in Antwerpen zugelassen.

Der Ministerrat, unterstützt und vertreten durch RA S. Depré, RA E. de Lophem und RA M. Chomé, in Brüssel zugelassen, hat einen Schriftsatz eingereicht, die klagenden Parteien haben einen Erwiderungsschriftsatz eingereicht und der Ministerrat hat auch einen Gegenerwiderungsschriftsatz eingereicht.

Durch Anordnung vom 18. Juli 2018 hat der Gerichtshof nach Anhörung der referierenden Richter P. Nihoul und E. Derycke 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 19. September 2018 geschlossen und die Rechtssache zur Beratung gestellt wird.

Infolge des Antrags der klagenden Parteien auf Anhörung hat der Gerichtshof durch Anordnung vom 25. September 2018 den Sitzungstermin auf den 17. Oktober 2018 anberaumt.

Auf der öffentlichen Sitzung vom 17. Oktober 2018

- erschienen

. RÄin A. Gruwez, in Brüssel zugelassen, *loco* RA D. Ribant, für die VoG « Ligue des Droits de l'Homme »,

. RA M. Chomé, ebenfalls *loco* RA S. Depré und RA E. de Lophem, für den Ministerrat,

- haben die referierenden Richter P. Nihoul und E. Derycke Bericht erstattet,

- wurden die vorgenannten Rechtsanwälte angehört,

- wurde die Rechtssache 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 den Gegenstand der Klage

B.1.1. Die Klage bezieht sich auf die Artikel 2 und 7 des Gesetzes vom 25. Dezember 2016 « zur Festlegung verschiedener Abänderungen des Strafprozessgesetzbuches und des Strafgesetzbuches im Hinblick auf die Verbesserung der besonderen Ermittlungsmethoden und bestimmter Ermittlungsmaßnahmen in Sachen Internet, elektronische Nachrichten und Telekommunikation und zur Schaffung einer Datenbank der Stimmabdrücke » (nachstehend: Gesetz vom 25. Dezember 2016).

B.1.2. Mit diesem Gesetz soll eine Reihe von Änderungen des Strafprozessgesetzbuches bezüglich der strafrechtlichen Ermittlung und Untersuchung vorgenommen werden, insbesondere bei der Anwendung von besonderen Ermittlungsmethoden und bestimmten anderen Untersuchungsmethoden für die Suche im Internet und in elektronischen Nachrichten. Die durch das angefochtene Gesetz abgeänderten Bestimmungen wurden durch verschiedene Gesetze in das Strafprozessgesetzbuch eingeführt und « seit dem Jahr 2000 nicht mehr abgeändert oder angepasst », was « in der Welt der sich rasch entwickelnden Informationstechnologie eine Ewigkeit » darstellt (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-1966/001, S. 5). Mit dem angefochtenen Gesetz wollte der Gesetzgeber daher « einen für die Suche in einem Datenverarbeitungssystem und die Überwachung sowie die Kenntnisnahme von elektronischen Nachrichten geeigneteren Rechtsrahmen » schaffen (ebd., S. 7).

B.1.3. Der erste Klagegrund, der fünf Teile umfasst, richtet sich gegen Artikel 2 dieses Gesetzes, der die Suche in einem Datenverarbeitungssystem betrifft. Der zweite Klagegrund, der drei Teile enthält, richtet sich gegen Artikel 7 dieses Gesetzes, der die Infiltrierung im Internet betrifft.

In Bezug auf den ersten Klagegrund

Was die angefochtene Bestimmung betrifft

B.2. Durch Artikel 2 des Gesetzes vom 25. Dezember 2016 wird Artikel 39*bis* des Strafprozessgesetzbuches wie folgt abgeändert:

1. In Paragraph 1 – der bestimmte: « Unbeschadet der spezifischen Bestimmungen des vorliegenden Artikels sind die Regeln des vorliegenden Gesetzbuches mit Bezug auf die Beschlagnahme einschließlich des Artikels 28*sexies* auf Maßnahmen anwendbar, die darin bestehen, in einem Datenverarbeitungssystem gespeicherte Daten zu kopieren, unzugänglich zu machen und zu entfernen » - werden zwischen den Wörtern « in einem Datenverarbeitungssystem » und den Wörtern « gespeicherte Daten » die Wörter « oder einem Teil davon » eingefügt.

2. Die Paragraphen 2 bis 6 werden durch folgende Bestimmungen ersetzt:

« § 2. Die Suche in einem Datenverarbeitungssystem oder einem Teil davon, das beschlagnahmt worden ist, kann von einem Gerichtspolizeioffizier beschlossen werden.

Unbeschadet des Absatzes 1 kann der Prokurator des Königs eine Suche in einem Datenverarbeitungssystem oder einem Teil davon, das von ihm beschlagnahmt werden kann, anordnen.

Die in den Absätzen 1 und 2 erwähnten Suchen können sich nur auf Daten erstrecken, die im Datenverarbeitungssystem gespeichert sind, das entweder beschlagnahmt worden ist oder beschlagnahmt werden kann. Zu diesem Zweck wird vor Beginn der Suche jede externe Verbindung dieses Datenverarbeitungssystems verhindert.

§ 3. Der Prokurator des Königs kann die auf der Grundlage von § 2 begonnene Suche in einem Datenverarbeitungssystem oder einem Teil davon auf ein Datenverarbeitungssystem oder einen Teil davon ausweiten, das sich an einem anderen Ort als dem, wo die Suche durchgeführt wird, befindet:

- wenn diese Ausweitung für die Wahrheitsfindung mit Bezug auf die Straftat, die Gegenstand der Suche ist, notwendig ist und

- wenn andere Maßnahmen unverhältnismäßig wären oder wenn das Risiko besteht, dass ohne diese Ausweitung Beweismaterial verloren geht.

Die Ausweitung der Suche in einem Datenverarbeitungssystem darf nicht über die Datenverarbeitungssysteme oder Teile von solchen Systemen hinausgehen, zu denen die

Personen, die berechtigt sind, das untersuchte Datenverarbeitungssystem zu benutzen, insbesondere Zugang haben.

Was die durch die Ausweitung der Suche in einem Datenverarbeitungssystem gesammelten Daten betrifft, die denselben Zwecken dienen wie die der Beschlagnahme, sind die in § 6 vorgesehenen Regeln anwendbar.

Wenn sich herausstellt, dass diese Daten sich nicht auf dem Staatsgebiet des Königreichs befinden, dürfen sie nur kopiert werden. In diesem Fall teilt der Prokurator des Königs dies unverzüglich dem Föderalen Öffentlichen Dienst Justiz mit, der die zuständigen Behörden des betreffenden Staates darüber informiert, wenn dieser richtigerweise bestimmt werden kann.

In Fällen äußerster Dringlichkeit kann der Prokurator des Königs die Ausweitung der in Absatz 1 erwähnten Suche mündlich anordnen. Diese Anordnung wird schnellstmöglich unter Angabe der Gründe für die äußerste Dringlichkeit schriftlich bestätigt.

§ 4. Nur der Untersuchungsrichter kann eine andere Suche in einem Datenverarbeitungssystem oder einem Teil davon als die in den Paragraphen 2 und 3 erwähnten Suchen anordnen:

- wenn diese Suche für die Wahrheitsfindung mit Bezug auf die Straftat, die Gegenstand der Suche ist, notwendig ist und

- wenn andere Maßnahmen unverhältnismäßig wären oder wenn das Risiko besteht, dass ohne diese Suche Beweismaterial verloren geht.

In Fällen äußerster Dringlichkeit kann der Untersuchungsrichter die Ausweitung der in Absatz 1 erwähnten Suche mündlich anordnen. Diese Anordnung wird schnellstmöglich unter Angabe der Gründe für die äußerste Dringlichkeit schriftlich bestätigt.

§ 5. Um die in vorliegendem Artikel erwähnten Maßnahmen zu ermöglichen, kann der Prokurator des Königs oder der Untersuchungsrichter anordnen, jederzeit auch ohne die Zustimmung des Eigentümers oder des Inhabers seiner Rechte oder des Nutzers:

- jegliche Sicherung der betreffenden Datenverarbeitungssysteme gegebenenfalls mit Hilfe von technischen Mitteln, falschen Signalen, falschen Schlüsseln oder falschen Eigenschaften zeitweilig aufzuheben,

- technische Vorrichtungen in die betreffenden Datenverarbeitungssysteme zu installieren im Hinblick auf die Entschlüsselung und die Dekodierung der durch dieses Datenverarbeitungssystem gespeicherten, verarbeiteten oder übermittelten Daten.

Jedoch kann nur der Untersuchungsrichter diese zeitweilige Aufhebung der Sicherung oder diese Installierung technischer Vorrichtungen anordnen, wenn dies insbesondere für die Anwendung von § 3 notwendig ist.

§ 6. Wenn in den betreffenden Datenverarbeitungssystemen gespeicherte Daten entdeckt werden, die für dieselben Zwecke nützlich sind wie die der Beschlagnahme, jedoch die Beschlagnahme des Datenträgers nicht wünschenswert ist, werden diese Daten sowie diejenigen, die notwendig sind, um sie zu verstehen, auf Datenträger kopiert, die der Behörde

gehören. Im Dringlichkeitsfall oder aus technischen Gründen können Datenträger verwendet werden, die Personen, die berechtigt sind, das Datenverarbeitungssystem zu benutzen, zur Verfügung stehen.

Außerdem werden geeignete technische Mittel verwendet, um den Zugang zu diesen Daten im Datenverarbeitungssystem sowie zu den Kopien dieser Daten, die Personen, die berechtigt sind, das Datenverarbeitungssystem zu benutzen, zur Verfügung stehen, zu verhindern und ihre Unversehrtheit zu gewährleisten.

Wenn die in Absatz 1 vorgesehene Maßnahme aus technischen Gründen oder wegen des Umfangs der Daten nicht möglich ist, verwendet der Prokurator des Königs die geeigneten technischen Mittel, um den Zugang zu diesen Daten im Datenverarbeitungssystem sowie zu den Kopien dieser Daten, die Personen, die berechtigt sind, das Datenverarbeitungssystem zu benutzen, zur Verfügung stehen, zu verhindern und ihre Unversehrtheit zu gewährleisten.

Wenn die Daten den Gegenstand der Straftat bilden oder aus der Straftat hervorgegangen sind und wenn sie gegen die öffentliche Ordnung oder die Sittlichkeit verstoßen oder eine Gefahr für die Unversehrtheit der Datenverarbeitungssysteme oder für durch solche Systeme gespeicherte, verarbeitete oder übermittelte Daten darstellen, verwendet der Prokurator des Königs alle geeigneten technischen Mittel, um diese Daten unzugänglich zu machen oder um sie zu entfernen, nachdem er sie kopiert hat.

Er kann jedoch, außer in dem in Absatz 4 vorgesehenen Fall, die spätere Verwendung der Gesamtheit oder eines Teils dieser Daten erlauben, wenn dies keine Gefahr für die Ausübung der Strafverfolgung darstellt.

In Fällen äußerster Dringlichkeit und wenn es sich offensichtlich um eine in den Artikeln 137 § 3 Nr. 6, 140*bis* oder 383*bis* § 1 des Strafgesetzbuches erwähnte Straftat handelt, kann der Prokurator des Königs mündlich anordnen, dass alle geeigneten Mittel verwendet werden, um die Daten, die den Gegenstand der Straftat bilden oder aus der Straftat hervorgegangen sind und die gegen die öffentliche Ordnung oder die Sittlichkeit verstoßen, unzugänglich zu machen. Diese Anordnung wird schnellstmöglich unter Angabe der Gründe für die äußerste Dringlichkeit schriftlich bestätigt.

3. Der Artikel wird um die folgendermaßen lautenden Paragraphen 7 und 8 ergänzt:

« § 7. Der Prokurator des Königs oder der Untersuchungsrichter informiert den Verantwortlichen des Datenverarbeitungssystems schnellstmöglich über die Suche im Datenverarbeitungssystem oder ihre Ausweitung, außer wenn seine Identität oder seine Adresse begründeterweise nicht herausgefunden werden können. Er übermittelt ihm gegebenenfalls eine Zusammenfassung der Daten, die kopiert, unzugänglich gemacht oder entfernt worden sind.

§ 8. Der Prokurator des Königs verwendet die geeigneten technischen Mittel, um die Unversehrtheit und die Vertraulichkeit dieser Daten zu gewährleisten.

Es werden geeignete technische Mittel für ihre Aufbewahrung bei der Kanzlei verwendet.

Dieselbe Regel gilt, wenn Daten, die in einem Datenverarbeitungssystem gespeichert oder verarbeitet sind oder in ein Datenverarbeitungssystem übermittelt werden, zusammen mit ihrem Datenträger gemäß den vorhergehenden Artikeln beschlagnahmt werden ».

B.3.1. Der so abgeänderte Artikel 39*bis* des Strafprozessgesetzbuches betrifft die sogenannten « nicht geheimen » Suchen in einem Datenverarbeitungssystem. Denn gemäß seinem Paragraphen 7 muss der Verantwortliche des Datenverarbeitungssystems « schnellstmöglich » über die Suche in dem System und gegebenenfalls die Ausweitung der Suche auf ein Datenverarbeitungssystem, das sich an einem anderen Ort befindet, informiert werden.

Laut der Begründung des Gesetzes vom 28. November 2000 über die Computerkriminalität, durch das der ursprüngliche Artikel 39*bis* in das Strafprozessgesetzbuch eingeführt wurde, ist unter « Datenverarbeitungssystem » « ein System, mit dem Daten gespeichert, verarbeitet oder übermittelt werden können, » zu verstehen (*Parl. Dok.*, Kammer, 1999-2000, DOC 50-0213/001 und 50-0214/001, S. 12).

B.3.2. Grundsätzlich kann eine Suche in einem Datenverarbeitungssystem oder einem Teil davon nur von einem Untersuchungsrichter angeordnet werden, wenn diese Suche für die Wahrheitsfindung mit Bezug auf die Straftat, die Gegenstand der Suche ist, notwendig ist und wenn andere Maßnahmen unverhältnismäßig wären oder wenn das Risiko besteht, dass ohne diese Suche Beweismaterial verloren geht (§ 4). Das Gleiche gilt für die Ausweitung der Suche auf ein Datenverarbeitungssystem, auf das von dem System zugegriffen werden kann, das Gegenstand der anfänglichen Suche war.

B.3.3. Die angefochtene Bestimmung sieht mehrere Ausnahmen von der grundsätzlichen Zuständigkeit des Untersuchungsrichters in Bezug auf nicht geheime Suchen vor.

Zum einen kann die Suche in den in einem Datenverarbeitungssystem oder einem Teil davon gespeicherten Daten, das Gegenstand einer Beschlagnahme ist, von einem Gerichtspolizeioffizier veranlasst werden, unter der Voraussetzung, dass es für den Zugriff auf die Daten nicht notwendig ist, eine Sicherung aufzuheben oder die Daten zu entschlüsseln oder zu dekodieren. Falls es für den Zugriff auf die gespeicherten Daten notwendig ist, eine Sicherung aufzuheben oder sie zu entschlüsseln oder zu dekodieren, muss der Gerichtspolizeioffizier zu diesem Zweck die Erlaubnis des Prokurators des Königs einholen.

Zweitens kann der Prokurator des Königs eine Suche in den in einem Datenverarbeitungssystem oder einem Teil davon gespeicherten Daten anordnen, das nicht Gegenstand einer Beschlagnahme war, das aber von ihm beschlagnahmt werden könnte. In diesem Fall kann er ebenfalls die Aufhebung der etwaigen Sicherung oder die Entschlüsselung oder Dekodierung der Daten anordnen.

Drittens kann die Ausweitung der Suche, die in einem beschlagnahmten Datenverarbeitungssystem oder in einem System, das beschlagnahmt werden könnte, begonnen wurde, auf Daten in einem anderen Datenverarbeitungssystem, auf das über eine Verbindung aus dem System, in dem die Suche begonnen wurde, zugegriffen werden kann, vom Prokurator des Königs angeordnet werden. Wenn jedoch der Zugang zu den Daten in diesem anderen Datenverarbeitungssystem gesichert ist, muss der Prokurator des Königs die Genehmigung des Untersuchungsrichters einholen, um die Sicherung aufzuheben oder eine technische Vorrichtung zu installieren, die es ihm ermöglicht, sie zu entschlüsseln oder zu dekodieren.

B.3.4. Die geheimen Suchen, auf die sich Artikel 90*ter* des Strafprozessgesetzbuches bezieht, dürfen nur von einem Untersuchungsrichter in Ausnahmefällen angeordnet werden, wenn die Untersuchung es erfordert, wenn schwerwiegende Indizien dafür bestehen, dass dies eine in diesem Artikel aufgeführte Straftat betrifft, und wenn die anderen Untersuchungsmittel nicht ausreichen, um die Wahrheit herauszufinden.

In Bezug auf das Recht auf Achtung des Privatlebens

B.4.1. Der Gerichtshof prüft zunächst den ersten, zweiten und vierten Teil des ersten Klagegrunds, die aus einer Verletzung des Rechts auf Achtung vor dem Privatleben, das durch Artikel 22 der Verfassung und Artikel 8 der Europäischen Menschenrechtskonvention gewährleistet wird, sowie hinsichtlich des ersten und zweiten Teils aus einer Verletzung des Grundsatzes der Gleichheit und Nichtdiskriminierung, der durch die Artikel 10 und 11 der Verfassung gewährleistet wird, abgeleitet sind.

B.4.2. Die klagenden Parteien bemängeln an Artikel 39*bis* des Strafprozessgesetzbuches, der durch die angefochtene Bestimmung eingeführt wurde, dass er Einmischungen in das Recht auf Achtung des Privatlebens durch die Gerichtspolizeioffiziere oder die Magistrate der Staatsanwaltschaft ohne Kontrolle durch einen unabhängigen und unparteiischen Richter erlaube. Sie sind der Auffassung, dass die in Artikel 39*bis* erwähnten Suchen in einem Datenverarbeitungssystem zu einer vergleichbaren Verletzung des Privatlebens führen wie die Verletzung, die durch eine Haussuchung verursacht wird, die jedoch nur durch einen Untersuchungsrichter genehmigt werden darf (vierter Teil des Klagegrunds). Sie vertreten auch die Auffassung, dass der Behandlungsunterschied zwischen den in Artikel 90*ter* desselben Gesetzbuches erwähnten geheimen Suchen, die stets von einem Untersuchungsrichter genehmigt werden müssen, und den nicht geheimen Suchen, auf die sich die angefochtene Bestimmung bezieht und die nicht von einem Untersuchungsrichter genehmigt werden müssen, auf einem Kriterium beruht, das weder objektiv noch sachdienlich ist (erster Teil des Klagegrunds). Zudem sind sie der Meinung, dass der Behandlungsunterschied zwischen den Suchen in einem beschlagnahmten Datenverarbeitungssystem, die von einem Gerichtspolizeioffizier beschlossen werden können, und den Suchen in einem nicht beschlagnahmten Datenverarbeitungssystem, das aber beschlagnahmt werden kann, die nur durch den Prokurator des Königs beschlossen werden können, auch auf einem Kriterium beruht, das weder objektiv noch sachdienlich ist (zweiter Teil des Klagegrunds).

B.5. Im Gegensatz zu dem, was der Ministerrat ausführt, zieht der Umstand, dass die Rechtsvorschriften vor dem angefochtenen Gesetz bereits in gewissem Maße die Zuständigkeit des Prokurators des Königs vorsahen, um die Beschlagnahme von Datenverarbeitungssystemen und die Suchen in diesen Systemen anzuordnen, nicht die Unzulässigkeit wegen verspäteten Einreichens des ersten Teils des Klagegrunds nach sich. Mit der angefochtenen Bestimmung hat der Gesetzgeber nämlich erneut Gesetzesbestimmungen auf diesem Gebiet erlassen und hat die Zuständigkeit des Prokurators des Königs bestätigt und ausgeweitet.

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 ».

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

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

B.6.3 Diese Bestimmungen erfordern es, dass jede behördliche Einmischung in das Recht auf Achtung des Privatlebens in einer ausreichend präzisen Gesetzesbestimmung festgelegt ist, einer zwingenden gesellschaftlichen Notwendigkeit entspricht und im Verhältnis zu dem darin angestrebten rechtmäßigen Ziel steht.

B.7.1. Wie die Gesetzgebungsabteilung des Staatsrats in ihrer Stellungnahme zum Vorentwurf des Gesetzes, das zu dem angefochtenen Gesetz geworden ist, unterstreicht, kann die Suche in einem Datenverarbeitungssystem einen erheblichen Eingriff in das Recht auf Achtung des Privatlebens darstellen (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-1966/001, S. 126).

B.7.2. Der Europäische Gerichtshof für Menschenrechte hat ebenfalls bereits mehrmals geurteilt, dass « das Durchsuchen und die Beschlagnahme elektronischer Daten einen Eingriff in das Recht auf Achtung des ‘Privatlebens’ und der ‘Korrespondenz’ im Sinne von [Art. 8

EMRK] » darstellen und dass « ein solcher Eingriff [...] Art. 8 [verletzt], es sei denn, er ist ‘gesetzlich vorgesehen’ und verfolgt ein legitimes Ziel oder mehrere legitime Ziele im Sinne von Abs. 2 und ist ferner in einer demokratischen Gesellschaft zu deren Erreichung notwendig » (EuGHMR, 2. April 2015, *Vinci Construction und GTM Génie Civil et Services gegen Frankreich*, §§ 63-64).

Vor diesem Hintergrund untersucht der Gerichtshof, « ob das innerstaatliche Recht und die innerstaatliche Praxis angemessene und ausreichende Garantien gegen Missbrauch und Willkür bieten ». Zu diesen Garantien gehört « eine vorhandene wirksame Kontrolle von Maßnahmen, die gegen Artikel 8 der Konvention verstoßen » (ebd., §§ 66-67).

B.7.3. In Anbetracht des Ausmaßes des Eingriffs in das Recht auf Achtung des Privatlebens, den die Suche in einem Datenverarbeitungssystem verursachen kann, muss ihre Anwendung der Kontrolle durch einen unabhängigen und unparteiischen Richter unterliegen.

In Bezug auf die Suche in einem Datenverarbeitungssystem, das Gegenstand einer Beschlagnahme ist

B.8.1. Die angefochtene Bestimmung ermöglicht in ihrem Paragraphen 2 Absatz 1, dass ein Gerichtspolizeioffizier die Durchführung einer Suche in einem Datenverarbeitungssystem beschließt, das Gegenstand einer Beschlagnahme ist. Die Suche darf sich nur auf die in dem beschlagnahmten Gerät gespeicherten Daten erstrecken, denn vor Beginn der Suche muss dieses daran gehindert werden, eine Verbindung zu externen Systemen herzustellen. Wenn die Suche die zeitweilige Aufhebung einer Sicherung oder die Entschlüsselung oder Dekodierung der Daten erfordert, muss der Gerichtspolizeioffizier zu diesem Zweck außerdem die Erlaubnis des Prokurators des Königs einholen (§ 5 Absatz 1).

B.8.2. Aus der Begründung geht hervor, dass mit der angefochtenen Bestimmung das Ziel verfolgt wird, in dem Gesetz die Rechtsprechung des Kassationshofs hinsichtlich der Suche in einem beschlagnahmten System zu bestätigen:

« Dans son arrêt du 11 février 2015 (AR P.14 1739.F), la Cour de cassation a en effet indiqué que le droit actuel permet déjà à l’officier de police judiciaire de prendre

connaissance des données d'un GSM qui a été saisi. Bien entendu, l'exploitation de ces données se déroule toujours dans les limites de l'enquête pénale et sous le contrôle du magistrat en charge de celle-ci » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1966/001, p. 15).

B.8.3. In seinem vorerwähnten Entscheid vom 11. Februar 2015 hat der Kassationshof geurteilt:

« L'exploitation de la mémoire d'un téléphone portable, dont les messages qui y sont stockés sous forme de *sms*, est une mesure découlant de la saisie, laquelle peut être effectuée dans le cadre d'une information sans autres formalités que celles prévues pour cet acte d'enquête » (Cass., 11 février 2015, P.14.1739.F).

B.8.4. Die Beschlagnahme ist eine Untersuchungshandlung, die in den Fällen und unter den Bedingungen vorgenommen werden kann, die gemäß den Bestimmungen des Strafprozessgesetzbuches vorgesehen sind, insbesondere im Fall einer Entdeckung auf frischer Tat oder im Laufe einer ordnungsgemäß vom Untersuchungsrichter angeordneten Haussuchung. Sie kann sich auf alles beziehen, was dazu gedient zu haben oder dazu bestimmt gewesen zu sein scheint, eine Straftat zu begehen, was durch sie hervorgebracht worden zu sein scheint, und auf alles, was der Wahrheitsfindung dienlich sein kann (Art. 35 ff. des Strafprozessgesetzbuches).

B.8.5. Jeder, der glaubt, dass ihm durch die Beschlagnahme Schaden zugefügt worden ist, kann je nach Fall beim Prokurator des Königs (Artikel 28*sexies* § 1 des Strafprozessgesetzbuches) oder beim Untersuchungsrichter (Artikel 61*quater* § 1 desselben Gesetzbuches) Aufhebung davon beantragen. Im Fall einer Abweisung kann die Anklagekammer von der geschädigten Person mit der Sache befasst werden.

B.8.6. Die Suche in den Daten, die im Speicher des beschlagnahmten Geräts gespeichert sind, ist eine Ergänzung der Beschlagnahme selbst, ebenso wie die Kenntnisnahme des Inhalts von Büchern, Aufzeichnungen oder Dokumenten auf beschlagnahmten physischen Trägern durch den Gerichtspolizeioffizier. Da das beschlagnahmte Gerät, das Gegenstand der Suche ist, keine Verbindung zu anderen Systemen hat, sodass der Polizeioffizier, der die Suche durchführt, nur Zugang zu dem Inhalt hat, den der Eigentümer oder Besitzer des Geräts dort aufgezeichnet oder gespeichert hat, unterscheidet sich die Suche nicht von der Auswertung des Inhalts von Dokumenten, die Gegenstand einer Beschlagnahme sind, durch die Ermittler.

B.8.7. Aus dem Vorstehenden ergibt sich, dass die Suche in einem Datenverarbeitungssystem, das ordnungsgemäß beschlagnahmt wurde, ebenso wie die Auswertung von ordnungsgemäß beschlagnahmten Dokumenten, mit ausreichenden rechtlichen Garantien versehen ist, mit denen sichergestellt werden kann, dass der Eingriff in das Recht auf Achtung des Privatlebens, der durch diese Untersuchungshandlung verursacht wird, im Hinblick auf die Anforderungen von Artikel 22 der Verfassung und 8 der Europäischen Menschenrechtskonvention gerechtfertigt ist.

B.8.8. Die Prüfung anhand der Artikel 10 und 11 der Verfassung führt nicht zu einer anderen Schlussfolgerung, was die Suchen in einem beschlagnahmten Datenverarbeitungssystem betrifft. Der erste und vierte Teil des ersten Klagegrunds ist unbegründet, insofern er sich gegen die Suchen in einem ordnungsgemäß beschlagnahmten Datenverarbeitungssystem richtet.

In Bezug auf die Suche in einem Datenverarbeitungssystem, das Gegenstand einer Beschlagnahme sein kann

B.9.1. Die angefochtene Bestimmung ermöglicht es in ihrem Paragraph 2 Absatz 2 dem Prokurator des Königs, eine Suche in einem Datenverarbeitungssystem zu beschließen, das nicht beschlagnahmt wurde, aber « für das alle gesetzlichen Bedingungen einer Beschlagnahme erfüllt sind » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-1966/001, S. 16). Die Suche darf sich nur auf die in dem betreffenden Gerät gespeicherten Daten beziehen, denn dieses muss vorher daran gehindert werden, eine Verbindung zu externen Systemen herzustellen. Wenn die Suche die zeitweilige Aufhebung einer Sicherung oder die Entschlüsselung oder Dekodierung der Daten erfordert, muss der Gerichtspolizeioffizier zu diesem Zweck außerdem auch die Erlaubnis des Prokurators des Königs einholen (§ 5 Absatz 1).

B.9.2. In dem Fall, dass das Datenverarbeitungssystem, das Gegenstand der Untersuchung ist, vom Prokurator des Königs beschlagnahmt werden könnte, sind alle gesetzlichen Bedingungen, unter denen die Beschlagnahme beschlossen werden kann, erfüllt. Außerdem sind aufgrund von Artikel 39*bis* Paragraph 1 des Strafprozessgesetzbuches die Regeln mit Bezug auf die Beschlagnahme auf Maßnahmen anwendbar, die darin bestehen, in

einem Datenverarbeitungssystem oder einem Teil davon gespeicherte Daten zu kopieren, unzugänglich zu machen und zu entfernen. Das Kopieren von Daten, die eine Suche in einem Datenverarbeitungssystem ergeben hat, das aus Gründen der praktischen Zweckmäßigkeit nicht beschlagnahmt wurde, das aber gemäß den gesetzlichen Bedingungen für die Beschlagnahme hätte beschlagnahmt werden können, wird also hinsichtlich der Rechtsmittel und Garantien, die der betreffenden Person geboten sind, selbst als eine Beschlagnahme angesehen.

B.9.3. Da das Gerät, in dem die Suche durchgeführt wird, keine Verbindung zu anderen Systemen hat, sodass der Polizeioffizier, der die Suche durchführt, nur Zugang zu dem Inhalt hat, den der Eigentümer oder Besitzer des Geräts dort aufgezeichnet oder gespeichert hat, unterscheidet sich die Suche außerdem nicht von einer Suche in Dokumenten vor einer Beschlagnahme.

B.9.4. Daraus ergibt sich, das die Person, der durch die Beschlagnahme der Daten in einem nicht beschlagnahmten Datenverarbeitungssystem Schaden zugefügt wird, über dieselben Rechtsmittel und Garantien verfügt wie eine von einer nach den Rechtsvorschriften durchgeführten Haussuchung oder Durchsuchung betroffene Person.

B.9.5. Aus dem Vorstehenden ergibt sich, dass die Suche in einem Datenverarbeitungssystem, das nicht beschlagnahmt wurde, aber hätte beschlagnahmt werden können, mit ausreichenden rechtlichen Garantien versehen ist, mit denen sichergestellt werden kann, dass der Eingriff in das Recht auf Achtung des Privatlebens, der durch diese Untersuchungshandlung verursacht wird, im Hinblick auf die Anforderungen von Artikel 22 der Verfassung und 8 der Europäischen Menschenrechtskonvention gerechtfertigt ist.

B.9.6. Die Prüfung anhand der Artikel 10 und 11 der Verfassung führt nicht zu einer anderen Schlussfolgerung, was die Suchen in einem Datenverarbeitungssystem betrifft, das nicht beschlagnahmt wurde, aber hätte beschlagnahmt werden können. Der erste und vierte Teil des ersten Klagegrunds ist unbegründet, insofern er sich gegen die Suchen in einem Datenverarbeitungssystem richtet, das ordnungsgemäß beschlagnahmt werden kann.

In Bezug auf den Behandlungsunterschied zwischen der Suche in einem beschlagnahmten Datenverarbeitungssystem und der Suche in einem Datenverarbeitungssystem, das beschlagnahmt werden kann

B.10.1. Da die Möglichkeit des Gerichtspolizeioffiziers, die Durchführung einer Suche in einem beschlagnahmten Datenverarbeitungssystem selbst zu beschließen, durch die in B.8.1 ff. dargelegten Gründe gerechtfertigt ist, ist der Behandlungsunterschied, der sich daraus ergibt, dass die Suche durch den Prokurator des Königs in einem Datenverarbeitungssystem, das nicht beschlagnahmt ist, aber beschlagnahmt werden könnte, nur durch diesen beschlossen werden kann, durch dieselben Gründe gerechtfertigt.

B.10.2. Der zweite Teil des ersten Klagegrunds ist unbegründet.

In Bezug auf die Ausweitung der Suche

B.11.1. Der durch die angefochtene Bestimmung eingeführte Artikel 39*bis* § 3 des Strafprozessgesetzbuches ermöglicht es dem Prokurator des Königs zu beschließen, eine Suche, die in einem Datenverarbeitungssystem begonnen wurde, das beschlagnahmt wurde oder beschlagnahmt werden kann, auf ein Datenverarbeitungssystem oder einen Teil davon auszuweiten, das sich an einem anderen Ort als dem, wo die Suche durchgeführt wird, befindet und auf das über eine Verbindung zugegriffen werden kann. Ist jedoch der Zugriff auf die Daten gesichert, kann nur der Untersuchungsrichter die Aufhebung der Sicherung oder die Entschlüsselung oder Dekodierung der Daten genehmigen (§ 5 Absatz 2).

B.11.2. Die Ausweitung der Suche ermöglicht es den Ermittlern, nicht nur auf sämtliche aufgezeichneten oder gespeicherten Daten auf dem Gerät, das Ausgangspunkt der Suche ist, Zugriff zu haben, sondern auch auf alle in den Datenverarbeitungssystemen gespeicherten Dokumente, auf die durch eine Verbindung über dieses Gerät zugegriffen werden kann, sowie auf die gesamte Kommunikation, die sein Nutzer mit Dritten unterhalten hat, einschließlich der neu erhaltenen oder versandten Nachrichten, von denen der Nutzer noch keine Kenntnis genommen hat.

B.12.1. Vor dem Inkrafttreten der angefochtenen Bestimmung befand sich die Bestimmung zu Suchen in den Netzen, die durch Artikel 3 des Gesetzes vom 28. November 2000 über die Computerkriminalität eingefügt wurde, in Artikel 88*ter* des Strafprozessgesetzbuches. Dieser Artikel wurde durch Artikel 13 des angefochtenen Gesetzes aufgehoben.

B.12.2. In der Begründung des Gesetzes vom 28. November 2000 ist zu diesem Artikel 88*ter* angegeben:

« Une mesure coercitive traditionnelle, telle que la perquisition, est restrictive en ce sens que, par définition, elle ne peut être effectuée que sur le lieu pour lequel elle a été ordonnée. Ce qui caractérise les systèmes informatiques – qu'il s'agisse de systèmes importants dans des sociétés ou d'ordinateurs portables – c'est qu'ils sont de plus en plus connectés en réseaux.

Dans le contexte actuel, lorsque les systèmes informatiques pour lesquels une recherche semble nécessaire sont dispersés en divers endroits, plusieurs mandats de perquisition ou de saisie doivent être délivrés. Pareille approche suscite bien évidemment des problèmes : on court non seulement le risque de voir des éléments de preuve disparaître si l'intervention n'est pas simultanée mais en outre dans de nombreux cas, il ne sera pas possible *a priori* de déterminer les endroits où doivent s'effectuer les recherches, les fichiers pertinents ou même la localisation géographique des ordinateurs.

Pour pallier ces problèmes, le nouvel article fixe les conditions qui permettent l'extension de la recherche dans un système informatique vers des systèmes situés ailleurs. Il doit s'agir de systèmes liés entre eux.

La mesure doit avant tout être nécessaire à la manifestation de la vérité et il faut en outre qu'il y ait un risque de perdre les éléments de preuve ou que la prise d'autres mesures (par exemple plusieurs mandats de perquisition) soit disproportionnée. Il appartient au juge d'instruction d'apprécier raisonnablement ces considérations. En raison du caractère exceptionnel de l'extension de la recherche dans un système informatique, notamment en raison de ses éventuels effets extra-territoriaux, une telle recherche ne pourra être étendue que si elle apparaît nécessaire dans le cadre d'une affaire pénale concrète dont le juge est saisi » (*Doc. parl.*, 1999-2000, DOC 50-0213/001 et 50-0214/001, pp. 22-23).

B.13.1. Seit dem Inkrafttreten der angefochtenen Bestimmung erfordert die Ausweitung einer in einem Datenverarbeitungssystem begonnenen Suche auf Netze, die mit ihm verbunden sind, nicht mehr die Befassung und Genehmigung des Untersuchungsrichters. Der Prokurator des Königs ist dafür zuständig, diese Ausweitung der Suche anzuordnen, sofern der Zugang zu den Netzen nicht gesichert ist.

B.13.2. In der Begründung des angefochtenen Gesetzes ist hierzu angegeben:

« L'extension de la recherche dans un système informatique peut désormais être ordonnée par le procureur du Roi ou l'auditeur du travail.

Cette extension vise par exemple les situations où un smartphone a été saisi et où il apparaît nécessaire d'avoir accès au compte Hotmail, Facebook ou Dropbox auquel ce smartphone est connecté. Comme indiqué précédemment, le droit actuel permet seulement à l'autorité qui a décidé la saisie de l'appareil de faire une recherche dans l'appareil lui-même, pas dans les données auxquelles cet appareil est connecté dans le cloud par exemple.

Même si l'intervention du juge d'instruction inclut une garantie essentielle en matière d'intrusion dans la vie privée, la modification de loi est justifiée parce que l'article 39*bis* se limite aux recherches non secrètes. Comme il a été dit, l'article 39*bis* est utilisé de manière réactive à la suite du fait que l'on a pu s'emparer légalement d'un système informatique. Il n'y a en aucun cas d'approche ou d'exploitation secrète d'éléments de la vie privée des personnes. Dans ces circonstances, le contrôle du magistrat du parquet offre une garantie suffisante.

En revanche, la pénétration en secret dans un système informatique et sa mise sous surveillance restent soumises à l'intervention du juge d'instruction, conformément aux articles 90*ter* et suivants ou à l'article 89*ter* du Code d'instruction criminelle.

Par ailleurs, le transfert de cette mesure (c'est-à-dire l'extension de la recherche) de l'article 88*ter* vers l'article 39*bis* et donc du juge d'instruction vers le procureur du Roi se justifie par le fait que, avec le développement des nouvelles technologies, la distinction entre ce qui se trouve sur l'appareil et ce qui se trouve dans le cloud devient en partie artificielle.

Toutefois, cette modification doit être lue en combinaison avec le nouveau paragraphe 5 qui concerne l'utilisation de ' fausses clés ' etc. pour accéder aux données. Le dernier alinéa du paragraphe 5 prévoit que seul le juge d'instruction peut ordonner l'usage de ' fausses clés ' dans le cadre de l'application spécifique du § 3 » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1966/001, pp. 18-19).

B.14.1. Angesichts der bedeutenden Entwicklung der von Datenverarbeitungssystemen aus zugänglichen Netze und ihrer intensiven Nutzung durch die überwiegende Mehrheit der Bürger, sowohl um dort Dokumente und Daten zu speichern, die zu ihrem Privatleben gehören, einschließlich sehr persönlicher Dinge, als auch um miteinander zu kommunizieren, kann zum gegenwärtigen Zeitpunkt davon ausgegangen werden, dass eine Untersuchungsmaßnahme, die es ermöglicht, auf sämtliche Daten und Nachrichten zuzugreifen, die sich in den Netzen befinden, die mit einem Datenverarbeitungssystem verbunden sind, das einer Einzelperson gehört, einen Eingriff in ihr Recht auf Achtung des Privatleben darstellt, der mindestens vergleichbar mit den Eingriffen ist, die einerseits durch

eine Durchsuchung in einem Haus oder an einem privaten Ort und andererseits durch ein Abhören ihrer Telefongespräche oder ein Abfangen ihrer Post verursacht werden.

B.14.2. Aufgrund der Artikel 87 und 88 des Strafprozessgesetzbuches ist für Haussuchungen der Untersuchungsrichter zuständig. Nach Artikel 88*sexies* desselben Gesetzbuches darf außer in Fällen der Entdeckung auf frischer Tat nur der Untersuchungsrichter Kenntnis vom Inhalt der Post nehmen, die einem Postbetreiber anvertraut und vom Prokurator des Königs in Anwendung von Artikel 46*ter* desselben Gesetzbuches abgefangen und beschlagnahmt wurde. Nach Artikel 90*ter* desselben Gesetzbuches kann der Untersuchungsrichter im Rahmen seiner Zuständigkeit, « der Öffentlichkeit nicht zugängliche Nachrichten oder Daten eines Datenverarbeitungssystems oder eines Teils davon anhand technischer Mittel […] abfangen, von ihnen Kenntnis nehmen, sie durchsuchen und aufzeichnen oder die Suche in einem Datenverarbeitungssystem oder einem Teil davon ausweiten ».

B.14.3. Wie der Staatsrat in der Stellungnahme, die er zu der angefochtenen Bestimmung abgegeben hat, bemerkt hat, « ist der Untersuchungsrichter ein unabhängiger Magistrat, der eine objektive Untersuchung sowohl im belastenden als auch entlastenden Sinne führt, während die Staatsanwaltschaft eine am Strafprozess beteiligte Partei ist » (*Parl. Dok.*, Kammer, 2015-2016, DOC 54-1966/001, S. 127).

B.14.4. Die Ermittlungshandlungen dürfen grundsätzlich nicht die individuellen Rechte und Freiheiten beeinträchtigen, sodass die Untersuchungsmaßnahmen, die im Laufe der strafrechtlichen Ermittlung durchgeführt werden und eine solche Beeinträchtigung mit sich bringen, nur im Rahmen einer gerichtlichen Untersuchung durchgeführt werden können. Zumindest dürfen die Handlungen, auf die sich Artikel 28*septies* des Strafprozessgesetzbuches bezieht, der die sogenannte « Mini-Untersuchung » regelt, nur mit der Genehmigung und unter der Kontrolle eines Untersuchungsrichters durchgeführt werden, auch wenn in der Sache keine gerichtliche Untersuchung eingeleitet wird.

B.14.5. Die Ermittlung ist gekennzeichnet durch ihre ausgesprochen geheime und nicht kontradiktorische Beschaffenheit, wobei die Betroffenen über weniger Garantie zum Schutz der Rechte der Verteidigung verfügen als während der gerichtlichen Untersuchung.

Zwar haben die direkt Betroffenen bereits während der Ermittlung das Recht, Zugang zur Strafakte zu beantragen (Artikel 21*bis* des Strafprozessgesetzbuches). Im Unterschied zur gerichtlichen Untersuchung (Artikel 61*ter* des Strafprozessgesetzbuches) ist dieses Recht auf Zugang zur Akte für die Ermittlung jedoch nicht verfahrensrechtlich geregelt, sodass die Staatsanwaltschaft - in Ermangelung von gesetzlich festgelegten Ablehnungsgründen - den Antrag auf Zugang zu einer Akte ohne weiteres ablehnen kann und kein Rechtsmittel gegen eine Verweigerungsentscheidung oder das Ausbleiben einer Entscheidung besteht. In seinem Entscheid Nr. 6/2017 vom 25. Januar 2017 hat der Gerichtshof geurteilt, dass dieses Fehlen eines Rechtsmittels gegen die Verweigerung oder das Fehlen einer Entscheidung der Staatsanwaltschaft in Bezug auf einen von einem Beschuldigten verfassten Antrag auf Zugang zu einer Akte in der Ermittlung gegen die Artikel 10 und 11 der Verfassung verstößt. Da diese Verfassungswidrigkeit ausreichend präzise und vollständig formuliert ist, damit Artikel 21*bis* des Strafprozessgesetzbuches unter Einhaltung der Referenznormen, auf deren Grundlage der Gerichtshof seine Kontrolle ausübt, angewandt werden kann, hat der Gerichtshof auch geurteilt, dass es in Erwartung des Auftretens des Gesetzgebers dem Richter obliegt, dem Verstoß gegen diese Normen ein Ende zu setzen, indem er Artikel 61*ter* des Strafprozessgesetzbuches sinngemäß anwendet.

Ferner verfügen die Betroffenen während der Ermittlung nicht über ein formales Recht, eine bestimmte Ermittlungshandlung zu beantragen, während das Recht, zusätzliche gerichtliche Untersuchungshandlungen zu beantragen, wohl dem Beschuldigten und der Zivilpartei während der gerichtlichen Untersuchung zuerkannt wird (Artikel 61*quinquies* des Strafprozessgesetzbuches). Die Betroffenen können zwar immer einen informellen Antrag an die Staatsanwaltschaft richten, doch diese ist keineswegs verpflichtet, auf einen solchen Antrag einzugehen, und die Parteien besitzen keinerlei Rechtsmittel gegen eine Verweigerungsentscheidung oder das Fehlen einer Entscheidung.

Schließlich gibt es während der Ermittlung keine Kontrolle von Amts wegen über die Regelmäßigkeit des Verfahrens durch einen unabhängigen und unparteilichen Richter, der die Akte von etwaigen Nichtigkeiten bereinigen kann, während eine solche Kontrolle wohl während der gerichtlichen Untersuchung besteht (Artikel 235*bis* des Strafprozessgesetzbuches).

B.14.6. Aus dem Vorstehenden ergibt sich, dass diese Ermittlungsmaßnahme, insofern die angefochtene Bestimmung es ermöglicht, dass die Ausweitung der Suche, die in einem beschlagnahmten Gerät oder einem Gerät, das beschlagnahmt werden könnte, begonnen wurde, auf ein Datenverarbeitungssystem, das sich an einem anderen Ort als das Gerät selbst

befindet oder mit dem das Gerät verbunden ist, vom Prokurator des Königs ohne Beteiligung eines Untersuchungsrichters angeordnet wird, mit weniger Garantien für den Rechtsunterworfenen versehen ist, dessen Datenverarbeitungssystem Gegenstand der Untersuchungsmaßnahme ist, als die Haussuchung, die Öffnung der Post, das Abfangen von elektronischen Nachrichten und das Abhören von Telefongesprächen und die geheime Suche in einem Datenverarbeitungssystem.

B.15.1. Dieser Behandlungsunterschied wurde durch den Gesetzgeber mit dem nicht geheimen Charakter der Untersuchung gerechtfertigt:

« Même si l'intervention du juge d'instruction inclut une garantie essentielle en matière d'intrusion dans la vie privée, la modification de la loi est justifiée parce que l'article 39*bis* se limite aux recherches non secrètes. Comme il a été dit, l'article 39*bis* est utilisé de manière réactive à la suite du fait que l'on a pu s'emparer légalement d'un système informatique. Il n'y a en aucun cas d'approche ou d'exploitation secrète d'éléments de la vie privée des personnes. Dans ces circonstances, le contrôle du magistrat du parquet offre une garantie suffisante.

En revanche, la pénétration en secret dans un système informatique et sa mise sous surveillance restent soumises à l'intervention du juge d'instruction, conformément aux articles 90*ter* et suivants ou à l'article 89*ter* du Code d'instruction criminelle.

Par ailleurs, le transfert de cette mesure (c'est-à-dire l'extension de la recherche) de l'article 88*ter* vers l'article 39*bis* et donc du juge d'instruction vers le procureur du Roi se justifie par le fait que, avec le développement des nouvelles technologies, la distinction entre ce qui se trouve sur l'appareil et ce qui se trouve dans le cloud devient en partie artificielle » (*Doc. parl.*, 2015-2016, DOC 54-1966/001, p. 19).

B.15.2. Der in B.14.6 dargelegte Behandlungsunterschied beruht somit auf dem Kriterium des geheimen oder nicht geheimen Charakters der in den Netzen durchgeführten Suche, mit denen das beschlagnahmte Gerät oder das Gerät, das beschlagnahmt werden könnte, verbunden ist.

Der nicht geheime Charakter des Eingriffs in das Recht auf Achtung des Privatlebens der von der Maßnahme betroffenen Person ist durch die Pflicht gewährleistet, die dem Prokurator des Königs durch Paragraph 7 der angefochtenen Bestimmung auferlegt wird, den Verantwortlichen des Datenverarbeitungssystems, das Gegenstand der Untersuchung ist, « schnellstmöglich » zu informieren.

Da die Pflicht, den Verantwortlichen des Datenverarbeitungssystems der Suche zu informieren, dazu benutzt wird, den geheimen und den nicht geheimen Charakter einer Untersuchung voneinander zu unterscheiden und dies im Hinblick auf den Schutz der Rechtsunterworfenen erfolgt, ist davon auszugehen, dass die Mitteilung an den Verantwortlichen des Datenverarbeitungssystem auch den Verdächtigen betrifft, dessen in dem System gespeicherte Daten Gegenstand dieser Suche sind, wenn der Verdächtige nicht die tatsächliche Kontrolle über das fragliche Datenverarbeitungssystem hat.

B.15.3. Der Umstand, dass der Eingriff in das Recht auf Achtung des Privatlebens einer Person ohne deren Wissen vorgenommen wird, macht ihn noch schwerwiegender, was bedeutet, dass er mit den höchsten Garantien versehen sein muss und infolgedessen nur im Rahmen einer strafrechtlichen gerichtlichen Untersuchung durchgeführt werden darf (EuGHMR, 4. Dezember 2015, *Zakharov gegen Russland*, §§ 233, 249 und 259; 12. Januar 2016, *Szabó und Vissy gegen Ungarn*, § 77; 30. Mai 2017, *Trabajo Rueda gegen Spanien*, § 33). Der Umstand, dass dieselbe Untersuchungsmaßnahme der betroffenen Person mitgeteilt wurde, gegebenenfalls nachdem sie beendet wurde, beinhaltet jedoch ebenfalls einen erheblichen Eingriff in das Recht auf Achtung des Privatlebens dieser Person. Dass sie darüber informiert wurde, bedeutet nämlich nicht, dass sie dem zugestimmt hätte.

B.15.4. Durch das vorherige Eingreifen eines unabhängigen und unparteiischen Richters kann gewährleistet werden, dass der Eingriff in das Recht auf Achtung des Privatlebens im Verhältnis zu den Anforderungen von Artikel 22 der Verfassung und von Artikel 8 der Europäischen Menschenrechtskonvention steht.

Daher hat der Gerichtshof mit seinem Entscheid Nr. 202/2004 vom 21. Dezember 2004 geurteilt, dass die Observation mit technischen Mitteln mit dem Zweck, Einblick in eine Wohnung zu erlangen und für die diskrete Sichtkontrolle eines privaten Ortes, Maßnahmen sind, die hinsichtlich der Schwere des Eingriffs in das Recht auf Achtung vor dem Privatleben mit einer Haussuchung sowie mit Abhörungen und mit Aufzeichnungen von privaten Kommunikationen und Telekommunikationen verglichen werden können und nur unter den gleichen Bedingungen, das heißt im Rahmen einer gerichtlichen Untersuchung, genehmigt werden können.

Durch seinen Entscheid Nr. 178/2015 vom 17. Dezember 2015 hat der Gerichtshof zur Ausweitung der Suche in einem Datenverarbeitungssystem geurteilt:

« Die Ausweitung der Suche in einem Datenverarbeitungssystem unterliegt der vorherigen Genehmigung durch den Strafvollstreckungsrichter, der prüfen muss, ob die Erfordernisse bezüglich der Rechtmäßigkeit, der Verhältnismäßigkeit und der Subsidiarität erfüllt sind, und der insbesondere darüber wachen muss, dass die Grundrechte der Betreffenden nicht auf unverhältnismäßige Weise verletzt werden.

Um eine tatsächliche gerichtliche Kontrolle zu gewährleisten, muss der SVE-Magistrat, wenn er eine Genehmigung bei dem Strafvollstreckungsrichter beantragt, auch die Reichweite der Ausweitung der Suche in einem Datenverarbeitungssystem angeben, um zu verhindern, dass die Verletzung des Privatlebens potenziell unbegrenzt und folglich unverhältnismäßig ist (EuGHMR, 9. Dezember 2004, *Van Rossem* gegen Belgien, § 45), und damit eine Kontrolle darüber durch den Strafvollstreckungsrichter möglich ist. Eine andere Auslegung der angefochtenen Bestimmungen wäre nicht mit dem Recht auf Achtung des Privatlebens und der Wohnung vereinbar » (B.48.4).

Durch seinen Entscheid Nr. 148/2017 vom 21. Dezember 2017 hat der Gerichtshof zur Haussuchung einer Wohnung, die im Übrigen nicht unbedingt einen geheimen Charakter hat, geurteilt:

« Wegen der Schwere der dadurch verursachten Einmischung in das Recht auf Achtung des Privatlebens und die Unverletzlichkeit der Wohnung kann die Haussuchung bei dem heutigen Stand der Regelung bezüglich des Strafverfahrens nur erlaubt werden im Rahmen einer gerichtlichen Untersuchung, wobei die Betroffenen über ein organisiertes Recht verfügen, Zugang zur Akte und zusätzliche Untersuchungshandlungen zu beantragen, und wobei eine Aufsicht durch die Anklagekammer über die Regelmäßigkeit des Verfahrens vorgesehen ist.

Indem die Haussuchung, beim heutigen Stand der Regelung bezüglich des Strafverfahrens, in den Anwendungsbereich der Mini-Untersuchung aufgenommen wird, ohne zusätzliche Garantien zum Schutz der Rechte der Verteidigung vorzusehen, verletzt die angefochtene Bestimmung auf diskriminierende Weise das Recht auf Achtung des Privatlebens und das Recht auf die Unverletzlichkeit der Wohnung » (B.22.4).

B.15.5. Aus dem Vorstehenden ergibt sich, dass der Behandlungsunterschied zwischen den Personen, die Gegenstand einer Untersuchungsmaßnahme in den mit ihrem Datenverarbeitungssystem verbundenen Netzen sind, je nachdem, ob die Suche im Sinne der angefochtenen Bestimmung als geheim oder nicht geheim angesehen wird, nicht auf einem sachdienlichen Kriterium hinsichtlich des Grundsatzes beruht, dass im Laufe der strafrechtlichen Ermittlung durchgeführte Untersuchungsmaßnahmen, die eine Beeinträchtigung der individuellen Rechte und Freiheiten mit sich bringen, grundsätzlich nur

im Rahmen einer gerichtlichen Untersuchung durchgeführt werden können (Artikel 28*bis* § 3 Absatz 1 des Strafprozessgesetzbuches).

B.16.1. Außerdem rechtfertigt der Umstand, dass der Prokurator des Königs, wenn der Zugriff auf die mit dem Datenverarbeitungssystem verbundenen Netze durch einen Schlüssel gesichert ist oder wenn die Daten in den Netzen oder in einem verbundenen Datenverarbeitungssystem kodiert oder verschlüsselt sind, nur mit Genehmigung des Untersuchungsrichters von falschen Schlüsseln oder Dekodierungs- oder Entschlüsselungstechniken Gebrauch machen kann, es auch nicht, dass der Eingriff in das Recht auf Achtung des Privatlebens, der in diesem Fall nicht geringer ist, nicht mit denselben Garantien versehen ist, wenn solche Sicherungen nicht installiert worden sind.

B.16.2. Zudem wurde die Übertragung der Zuständigkeit des Untersuchungsrichters auf den Prokurator des Königs durch die angefochtene Bestimmung nicht mit zusätzlichen Garantien versehen, die dazu bestimmt sind, das Privatleben und die Verteidigungsrechte der betroffenen Person wirksam zu schützen, und die geeignet sind, die Abschaffung des vorherigen Eingreifens eines unabhängigen und unparteiischen Richters auszugleichen (EuGHMR, 30. September 2014, *Prezhdarovi gegen Bulgarien*, §§ 45 bis 47; 30. Mai 2017, *Trabajo Rueda gegen Spanien*, § 37). In dieser Hinsicht geht aus der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte hervor, dass das Vorhandensein einer wirksamen Beschwerde davon abhängt, ob sie angemessen ist; der fragliche Rechtsbehelf muss daher in Bezug zu der geltend gemachten Verletzung stehen, um geeignete und gleichwertige Garantien zu bieten, die die fraglichen Rechte des Einzelnen gewährleisten. Daraus folgt, dass die nationale Beschwerdeinstanz befugt sein muss, im Wesentlichen über die auf die Konvention gestützte Beschwerde zu befinden, um zu entscheiden, ob der Eingriff in das Recht des Betroffenen auf Achtung seines Privatlebens mit Artikel 8 Absatz 2 im Einklang stand (EuGHMR, 1. April 2008, *Varga gegen Rumänien*, §§ 72-73; 3. Juli 2012, *Robathin gegen Österreich*, § 21; 30. September 2014, *Prezhdarovi gegen Bulgarien*, § 47; 2. April 2015, *Vinci Construction und GTM Génie Civil et Services gegen Frankreich*, §§ 66-67).

B.16.3. Artikel 28*sexies* des Strafprozessgesetzbuches ist zwar auf Maßnahmen anwendbar, die darin bestehen, in einem Datenverarbeitungssystem oder einem Teil davon gespeicherte Daten zu kopieren, unzugänglich zu machen und zu entfernen. Diese

Bestimmung ermöglicht es jedem, dem durch eine Ermittlungshandlung in Bezug auf seine Güter Schaden zugefügt worden ist, beim Prokurator des Königs Aufhebung davon zu beantragen, gegen dessen Entscheidung bei der Anklagekammer Rechtsbehelf eingelegt werden kann. Dieses Verfahren, das ebenfalls vor dem Untersuchungsrichter anwendbar ist (Artikel 61*quater* § 1 des Strafprozessgesetzbuches), beschränkt sich also auf die Möglichkeit der betreffenden Person, die Aufhebung der Beschlagnahme und somit die Rückgabe der IT-Geräte und der Daten zu erreichen, die mit einer Suche in einem Datenverarbeitungssystem erlangt wurden. Sie verhindert aber nicht den Eingriff in das Privatleben, der stattgefunden hat und der durch die Rückgabe des Geräts und der darauf gespeicherten Daten nicht beseitigt wird, was nicht den in B.16.2 aufgeführten Anforderungen der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte entspricht.

B.16.4. Aufgrund der Schwere des Eingriffs in das Recht auf Achtung des Privatlebens, den sie mit sich bringt, kann die Maßnahme, die darin besteht, eine Suche in einem Datenverarbeitungssystem oder einem Teil davon, die in einem Datenverarbeitungssystem begonnen wurde, das beschlagnahmt wurde oder das vom Prokurator des Königs beschlagnahmt werden kann, auf ein Datenverarbeitungssystem oder einen Teil davon auszuweiten, das sich an einem anderen Ort als dem, wo die Suche durchgeführt wird, befindet, nur unter den gleichen Bedingungen wie denen, die für die in B.14.2 erwähnten Untersuchungshandlungen gelten, genehmigt werden.

B.17.1. Der erste und vierte Teil des ersten Klagegrunds ist in diesem Maße begründet.

Artikel 39*bis* Paragraph 3 des Strafprozessgesetzbuches, der durch Artikel 2 des angefochtenen Gesetzes vom 25. Dezember 2016 eingefügt wurde, ist für nichtig zu erklären. Um ein Rechtsvakuum hinsichtlich der betreffenden Suchmaßnahme zu vermeiden, ist auch Artikel 13 des Gesetzes vom 25. Dezember 2016, der untrennbar mit der angefochtenen Bestimmung verbunden ist, insofern er Artikel 88*ter* des Strafprozessgesetzbuches aufhebt, für nichtig zu erklären.

B.17.2. Um die Rechtsunsicherheit zu vermeiden, die bezüglich der Gültigkeit von Maßnahmen zur Ausweitung der Suchen in Datenverarbeitungssystemen, die gemäß der für nichtig erklärten Bestimmung durchgeführt wurden, entstehen würde, sind die Folgen dieser

Bestimmung bis zum Datum der Veröffentlichung des vorliegenden Entscheids im *Belgischen Staatsblatt* aufrechtzuerhalten.

In Bezug auf die Information des Verantwortlichen des Datenverarbeitungssystems

B.18.1. Der dritte Teil des ersten Klagegrunds ist aus einer Verletzung der Artikel 12 und 14 der Verfassung in Verbindung mit Artikel 7 der Europäischen Menschenrechtskonvention abgeleitet. Er richtet sich gegen den Begriff des « Verantwortlichen des Datenverarbeitungssystems », der in Artikel 39*bis* Paragraph 7 des Strafprozessgesetzbuches enthalten ist, der durch Artikel 2 des angefochtenen Gesetzes vom 25. Dezember 2016 eingeführt wurde. Die klagenden Parteien werfen dem Gesetzgeber vor, den Inhalt dieses Begriffs nicht näher bestimmt zu haben, sodass die Identität der Personen, die über die Suche oder ihre Ausweitung informiert werden müssen, nicht eindeutig definiert und unklar sei.

B.18.2. Im Gegensatz zu dem, was der Ministerrat ausführt, führt der Umstand, dass die Rechtsvorschriften vor dem angefochtenen Gesetz bereits auf den « Verantwortlichen des Datenverarbeitungssystems » Bezug nahmen, nicht zur Unzulässigkeit wegen verspäteten Einreichens des dritten Teils des Klagegrunds. Durch die angefochtene Bestimmung hat der Gesetzgeber nämlich erneut Gesetzesbestimmungen auf diesem Gebiet erlassen und hat die dem Prokurator des Königs und dem Untersuchungsrichter auferlegte Pflicht, den « Verantwortlichen des Datenverarbeitungssystems » zu informieren, bestätigt.

B.19.1. Artikel 12 Absatz 2 der Verfassung bestimmt:

« Niemand darf verfolgt werden, es sei denn in den durch Gesetz bestimmten Fällen und in der dort vorgeschriebenen Form ».

Artikel 14 der Verfassung bestimmt:

« Eine Strafe darf nur aufgrund des Gesetzes eingeführt oder angewandt werden ».

Artikel 7 Absatz 1 der Europäischen Menschenrechtskonvention bestimmt:

« Niemand kann wegen einer Handlung oder Unterlassung verurteilt werden, die zur Zeit ihrer Begehung nach inländischem oder internationalem Recht nicht strafbar war. Ebenso darf keine höhere Strafe als die im Zeitpunkt der Begehung der strafbaren Handlung angedrohte Strafe verhängt werden ».

B.19.2. Insofern er das Legalitätsprinzip in Strafsachen gewährleistet, hat Artikel 7 Absatz 1 der Europäischen Menschenrechtskonvention eine ähnliche Tragweite wie die Artikel 12 Absatz 2 und 14 der Verfassung.

B.19.3. Aus den vorerwähnten Bestimmungen geht hervor, dass das Strafgesetz so formuliert werden muss, dass jeder zu dem Zeitpunkt, wo er ein Verhalten annimmt, wissen kann, ob dieses Verhalten strafbar ist oder nicht, und die gegebenenfalls die drohende Strafe kennen kann. Das Legalitätsprinzip und der Grundsatz der Vorhersehbarkeit gelten für das gesamte Strafverfahren. Somit soll durch die vorerwähnten Bestimmungen jegliche Gefahr eines willkürlichen Eingreifens der ausführenden oder der rechtsprechenden Gewalt bei der Festlegung und Anwendung der Strafen ausgeschlossen werden.

Das Legalitätsprinzip in Strafsachen reicht nicht so weit, dass der Gesetzgeber verpflichtet wäre, selbst jeden Aspekt der Unterstrafestellung, der Strafe oder des Strafverfahrens zu regeln. Es verhindert es insbesondere nicht, dass der Gesetzgeber dem Richter oder der Staatsanwaltschaft eine Ermessensbefugnis gewährt. Die allgemeine Beschaffenheit der Gesetzesbestimmungen, die Verschiedenartigkeit der Situationen, auf die sie Anwendung finden, und die Entwicklung der durch sie geahndeten Verhaltensweisen müssen nämlich berücksichtigt werden.

B.19.4. Im vorliegenden Fall wird nicht die Legalität der Unterstrafestellung oder der Strafe, sondern diejenige des Strafverfahrens in Frage gestellt.

Eine Ermächtigung der ausführenden Gewalt verletzt nicht dieses Prinzip, insofern die Ermächtigung ausreichend genau beschrieben ist und sich auf die Ausführung von Maßnahmen bezieht, deren wesentliche Elemente vorher durch den Dekretgeber festgelegt wurden.

Das Erfordernis der Vorhersehbarkeit des Strafverfahrens garantiert jedem Rechtsunterworfenen, dass er nur Gegenstand einer Ermittlung, einer gerichtlichen Untersuchung oder einer Verfolgung gemäß einem Verfahren sein kann, von dem er vor dessen Anwendung Kenntnis nehmen kann.

B.20. Da die angefochtene Bestimmung vorschreibt, den « Verantwortlichen des Datenverarbeitungssystems » über die Suche zu informieren, ermöglicht sie es dieser Person, die notwendigen Vorkehrungen zur Wahrung ihrer Rechte zu treffen, sodass dieser Begriff ein wesentliches Element des Strafverfahrens auf dem Gebiet von Suchen in den Datenverarbeitungssystemen ist.

B.21.1. Diesbezüglich hat die Gesetzgebungsabteilung des Staatsrates bemerkt:

« Mais la disposition ne donne pas une définition de ce qu'il faut entendre par ' le responsable du système informatique '.

Au sens de la recommandation n° R(95)13 [du Comité des ministres du Conseil de l'Europe du 11 septembre 1995], la notion englobe toutes les personnes qui, lors de la perquisition ou de la saisie, paraissent disposer formellement ou réellement du contrôle sur le système informatique, objet de la perquisition. Il peut s'agir du propriétaire du système, d'un opérateur de ce système ou même du gardien (locataire ou occupant) des locaux abritant le système informatique.

La disposition en projet doit, en conséquence, définir expressément les personnes concernées par l'information.

Par ailleurs, la saisie de données peut également concerner des tierces personnes. C'est ainsi que la recommandation n° R(95)13, précitée, invite les Etats membres à organiser ce type d'information et ce dans le respect des impératifs de l'enquête.

Cette exigence est importante car, en vertu des articles 28*sexies* et 61*quater* du Code d'instruction criminelle, toute personne qui s'estime lésée par un acte d'information ou par un acte d'instruction relatif à ses biens peut en demander la levée soit au procureur du Roi, soit au juge d'instruction » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1966/001, pp. 129-130).

B.21.2. In der Begründung ist zu dieser Bemerkung angegeben:

« Le Conseil d'Etat estime également (et renvoie à cet égard à l'avis n° 28 029/2 du 31 mai 1999) que le texte de l'avant-projet de loi doit lui-même contenir une définition du ' responsable du système informatique '. Le but de la communication de la mesure est toutefois d'établir clairement qu'il ne s'agit pas d'une mesure secrète (cf. la compétence de perquisitionner). La terminologie de l'avant-projet comporte dans cette optique une certaine

souplesse pour ce qui est de la personne à contacter : en effet, il n'est pas possible de déterminer *a priori* pour tous les cas et de manière univoque qui exerce le contrôle réel ou juridique sur le système (*Doc. parl.*, Chambre, 1999-2000, n° 0213/001, p. 21) » (*Doc. parl.*, 2015-2016, DOC 54-1966/001, p. 24).

B.22.1. Über die Feststellung des geheimen oder nicht geheimen Charakters der Untersuchungsmaßnahme hinaus hat die Mitteilung der Durchführung dieser Maßnahme außerdem zur Folge, dass es der betroffenen Person oder den betroffenen Personen möglich ist, die Verfahrensrechte wahrzunehmen, die insbesondere dazu dienen, die Verhältnismäßigkeit der in das Recht auf Achtung des Privatlebens dieser Person oder Personen verursachten Einmischung zu kontrollieren.

B.22.2. Daraus ergibt sich, dass der Begriff des « Verantwortlichen des Datenverarbeitungssystems » als Bezeichnung der Person oder Personen verstanden werden muss, die für die Daten oder Nachrichten, die auf dem beschlagnahmten Gerät oder dem Gerät, das beschlagnahmt werden kann, gespeichert sind, und für die Daten und Nachrichten, von denen über die Netze Kenntnis genommen werden kann, die von der Ausweitung der in dem vorerwähnten Gerät begonnenen Suche betroffen sind, verantwortlich sind, wobei diese Person oder Personen nicht zwangsläufig die Eigentümer oder Besitzer der betreffenden Geräte sind. Wie in B.15.2 erwähnt, bezieht sich dieser Begriff ebenfalls auf den Verdächtigen, dessen Daten Gegenstand der Suche sind, wenn er nicht selbst die tatsächliche Kontrolle über das fragliche Datenverarbeitungssystems ausübt.

B.23. Vorbehaltlich der Auslegung des Begriffs des « Verantwortlichen des Datenverarbeitungssystems » wie in B.15.2 und B.22.2 angegeben, ist der dritte Teil des ersten Klagegrunds unbegründet.

In Bezug auf Datenverarbeitungssysteme von Rechtsanwälten und Ärzten

B.24.1. Der fünfte Teil des ersten Klagegrunds ist aus einer Verletzung der Artikel 10, 11 und 22 der Verfassung in Verbindung mit Artikel 6 der Europäischen Menschenrechtskonvention abgeleitet. Die klagenden Parteien werfen dem Gesetzgeber vor, in Artikel 39*bis* des Strafprozessgesetzbuches, der die nicht geheimen Suchen in einem Datenverarbeitungssystem regelt, keine gleichwertigen Garantien wie die, die in

Artikel 90*octies* desselben Gesetzbuches festgelegt sind und die die geheimen Suchen in einem Datenverarbeitungssystem betreffen, vorgesehen zu haben.

B.24.2. Artikel 90*octies* des Strafprozessgesetzbuches bestimmt:

« § 1. Die Maßnahme darf sich nur dann auf zu Berufszwecken benutzte Räumlichkeiten, den Wohnort, Kommunikationsmittel oder Datenverarbeitungssysteme eines Rechtsanwalts oder Arztes beziehen, wenn dieser selber verdächtigt wird, eine der in Artikel 90*ter* erwähnten Straftaten begangen zu haben oder daran beteiligt gewesen zu sein, oder wenn genaue Tatsachen vermuten lassen, dass Dritte, die verdächtigt werden, eine der in Artikel 90*ter* erwähnten Straftaten begangen zu haben, seine Räumlichkeiten, seinen Wohnort, seine Kommunikationsmittel oder seine Datenverarbeitungssysteme benutzen.

§ 2. Die Maßnahme darf nicht durchgeführt werden, ohne dass - je nach Fall - der Präsident der Rechtsanwaltskammer oder der Vertreter der provinzialen Ärztekammer davon in Kenntnis gesetzt worden ist.

Diese Personen unterliegen der Schweigepflicht. Jegliche Verletzung der Schweigepflicht wird gemäß Artikel 458 des Strafgesetzbuches geahndet.

§ 3. Der Untersuchungsrichter beurteilt nach Konzertierung mit dem Präsidenten der Rechtsanwaltskammer oder dem Vertreter der provinzialen Ärztekammer, welche Teile der in Artikel 90*sexies* § 3 erwähnten der Öffentlichkeit nicht zugänglichen Nachrichten oder Daten eines Datenverarbeitungssystems, die er für die Untersuchung als relevant erachtet, unter das Berufsgeheimnis fallen und welche nicht.

Nur die Teile der Nachrichten oder Daten, die in Absatz 1 erwähnt sind und nicht unter das Berufsgeheimnis fallen, werden niedergeschrieben oder wiedergegeben und gegebenenfalls übersetzt. Der Untersuchungsrichter lässt davon ein Protokoll erstellen. Die Dateien mit diesen Nachrichten oder Daten werden unter versiegeltem Umschlag bei der Kanzlei hinterlegt.

Alle anderen Nachrichten oder Daten werden in einer anderen Datei unter getrenntem, versiegeltem Umschlag bei der Kanzlei hinterlegt ».

B.24.3. Diese Bestimmung wurde durch Artikel 22 des angefochtenen Gesetzes in das Strafprozessgesetzbuch aufgenommen. In der Begründung ist hierzu angegeben:

« L’exception pour les avocats et les médecins était dictée par la considération que ces catégories professionnelles sont par excellence exposées au risque d’être confrontées à des suspects avec qui, en raison de leur situation professionnelle, elles entretiennent une relation de confiance qui doit tout particulièrement être préservée. Il s’agit de la clause de protection classique telle qu’elle apparaît également dans des mesures d’investigation similaires comme l’ouverture de courrier (article 88*sexies* du Code d’instruction criminelle), une observation afin d’avoir une vue dans un domicile (article 56*bis* du Code d’instruction criminelle) ou un

contrôle visuel discret (article 89*ter* du Code d'instruction criminelle) » (*Doc. parl*., 2015-2016, DOC 54-1966/001, pp. 72-73).

B.25. Das Berufsgeheimnis, an das Rechtsanwälte und Ärzte gebunden sind, dient nicht dazu, ihnen irgendein Vorrecht zu gewähren, sondern bezweckt hauptsächlich, das Grundrecht auf Achtung des Privatlebens derjenigen, die sie in bisweilen sehr persönlichen Dingen ins Vertrauen ziehen, zu schützen. Zudem genießen die vertraulichen Informationen, die einem Rechtsanwalt bei der Ausübung seines Berufes und wegen dieser Eigenschaft anvertraut werden, in bestimmten Fällen auch den Schutz, der sich für den Rechtsuchenden aus den Garantien ergibt, die in Artikel 6 der Europäischen Menschenrechtskonvention festgelegt sind, da die dem Rechtsanwalt auferlegte Regel des Berufsgeheimnisses ein fundamentales Element der Rechte der Verteidigung des Rechtsuchenden, der ihn ins Vertrauen zieht, ist.

B.26.1. Es ist nicht gerechtfertigt, dass die Bestimmung zur Wahrung des Berufsgeheimnisses von Rechtsanwälten und Ärzten nur vorgesehen ist, wenn die Suche in einem von ihnen zu Berufszwecken genutzten Datenverarbeitungssystem geheim durchgeführt wird, und nicht, wenn sie ihnen mitgeteilt wird. Der Eingriff in das Recht auf Achtung des Privatlebens von Personen, die ihnen unter das Berufsgeheimnis fallende Informationen anvertraut haben, erfolgt nämlich in der gleichen Weise, unabhängig davon, ob die Suche ohne Wissen des betroffenen Rechtsanwalts oder Arztes durchgeführt wird oder nicht.

B.26.2. Es ist richtig – wie es der Ministerrat ausführt –, dass, wenn die Suche in einem Datenverarbeitungssystem im Rahmen einer Haussuchung stattfindet, die Bestimmungen zu Haussuchungen in den beruflichen Räumlichkeiten von Rechtsanwälten oder Ärzten anwendbar sind und es ermöglichen, das Berufsgeheimnis zu gewährleisten. Die Möglichkeiten der nicht geheimen Suche, die durch Artikel 39*bis* des Strafprozessgesetzbuches vorgesehen sind, gehen jedoch über diesen konkreten Fall hinaus und können nicht nur im Fall der Haussuchung in beruflichen Räumlichkeiten angewandt werden.

B.27. Der fünfte Teil des ersten Klagegrunds ist begründet. Artikel 39*bis* des Strafprozessgesetzbuches, der durch Artikel 2 des angefochtenen Gesetzes eingeführt wurde, ist für nichtig zu erklären, insofern er keine besondere Bestimmung im Hinblick auf die Wahrung des Berufsgeheimnisses von Ärzten und Rechtsanwälten vorsieht.

Um die Rechtssicherheit in Bezug auf durchgeführte Suchen in Datenverarbeitungssystemen, die Ärzten oder Rechtsanwälten gehören, zu gewährleisten, müssen die Folgen der für nichtig erklärten Bestimmung, wie im Tenor angegeben, aufrechterhalten werden.

In Bezug auf den zweiten Klagegrund

Was die angefochtene Bestimmung betrifft

B.28.1. Der zweite Klagegrund bezieht sich auf Artikel 7 des Gesetzes vom 25. Dezember 2016, durch den in das Strafprozessgesetzbuch ein Artikel 46*sexies* eingeführt wird, der bestimmt:

« Art. 46*sexies*. § 1. Bei der Ermittlung von Verbrechen und Vergehen kann der Prokurator des Königs, wenn die Untersuchung dies erfordert und wenn die anderen Untersuchungsmittel nicht auszureichen scheinen, um die Wahrheit herauszufinden, die in Absatz 2 erwähnten Polizeidienste dazu ermächtigen, im Internet gegebenenfalls unter einer fiktiven Identität Kontakt zu einer oder mehreren Personen zu unterhalten, bei denen es schwerwiegende Indizien dafür gibt, dass sie Straftaten begehen oder begehen könnten, die eine Hauptkorrektionalgefängnisstrafe von einem Jahr oder eine schwerere Strafe zur Folge haben können.

Der König bestimmt die Bedingungen, auch für die Ausbildung, und die Modalitäten zur Bestimmung der Polizeidienste, die ermächtigt sind, die in vorliegendem Artikel erwähnte Maßnahme durchzuführen.

Unter außergewöhnlichen Umständen und mit der ausdrücklichen Erlaubnis des Prokurators des Königs kann der Beamte der in Absatz 2 erwähnten Polizeidienste im Rahmen eines bestimmten Einsatzes kurzzeitig auf die Fachkompetenz einer Person zurückgreifen, die nicht den Polizeidiensten angehört, wenn dies für das Gelingen seines Auftrags als absolut notwendig erscheint. Die Erlaubnis und die Identität dieser Person werden in der in § 3 Absatz 7 erwähnten Akte aufbewahrt.

Vorliegender Artikel findet keine Anwendung auf die persönliche Interaktion von Polizeibeamten bei der Ausführung ihrer gerichtspolizeilichen Aufträge mit einer oder

mehreren Personen im Internet, die nur eine gezielte Überprüfung oder eine Festnahme zum unmittelbaren Zweck hat, und zwar ohne Verwendung einer glaubwürdigen fiktiven Identität.

§ 2. Die in § 1 erwähnte Maßnahme wird vom Prokurator des Königs durch eine vorherige schriftliche und mit Gründen versehene Erlaubnis angeordnet. Diese Erlaubnis gilt für einen Zeitraum von drei Monaten, unbeschadet einer Erneuerung.

Im Dringlichkeitsfall kann die Erlaubnis mündlich erteilt werden. Sie muss so schnell wie möglich in der in Absatz 1 vorgesehenen Form bestätigt werden.

§ 3. Straffrei bleiben Polizeibeamte, die im Rahmen ihres Auftrags und im Hinblick auf dessen Gelingen oder zur Gewährleistung ihrer eigenen Sicherheit oder der anderer von der Maßnahme betroffenen Personen absolut notwendige Straftaten mit ausdrücklicher Zustimmung des Prokurators des Königs begehen.

Diese Straftaten dürfen nicht schwerwiegender sein als die Straftaten, für die die Maßnahme angewandt wird, und müssen notwendigerweise im Verhältnis zum angestrebten Ziel stehen.

Die Absätze 1 und 2 sind ebenfalls auf die Personen anwendbar, die direkte zur Durchführung dieses Auftrags notwendige Hilfe oder Unterstützung geleistet haben, sowie auf die in § 1 Absatz 3 erwähnten Personen.

Straffrei bleibt auch der Magistrat, der unter Einhaltung des vorliegenden Gesetzbuches einen Polizeibeamten und die in Absatz 3 erwähnten Personen dazu ermächtigt, im Rahmen der Durchführung der Maßnahme Straftaten zu begehen.

Die Polizeibeamten teilen dem Prokurator des Königs die Straftaten, die sie selbst oder die in Absatz 3 erwähnten Personen zu begehen beabsichtigen, vor Durchführung der Maßnahme schriftlich mit.

Wenn diese Notifizierung nicht vorab hat erfolgen können, informieren die Polizeibeamten den Prokurator des Königs unverzüglich über die Straftaten, die sie selbst oder die in Absatz 3 erwähnten Personen begangen haben, und bestätigen dies anschließend schriftlich.

Der Prokurator des Königs vermerkt in einer getrennten schriftlichen Entscheidung die Straftaten, die von den Polizeidiensten und den in Absatz 3 erwähnten Personen im Rahmen der von ihm angeordneten Maßnahme begangen werden dürfen. Diese Entscheidung wird in einer getrennten und vertraulichen Akte aufbewahrt. Er hat als Einziger Zugang zu dieser Akte, unbeschadet des in Artikel 56*bis* beziehungsweise in den Artikeln 235*ter* § 3 und 235*quater* § 3 erwähnten Rechts auf Einsichtnahme des Untersuchungsrichters und der Anklagekammer. Der Inhalt dieser Akte fällt unter das Berufsgeheimnis.

§ 4. Der mit der Ermittlung beauftragte Gerichtspolizeioffizier erstellt ein Protokoll über die verschiedenen Phasen der Durchführung dieser Maßnahme, einschließlich der relevanten Kontakte. Diese Protokolle werden der Akte spätestens nach Beendigung der Maßnahme beigefügt.

Die in § 1 erwähnten Kontakte werden mit den geeigneten technischen Mitteln registriert und spätestens nach Beendigung der Maßnahme der Akte beigefügt oder in elektronischer oder nicht elektronischer Form bei der Kanzlei hinterlegt.

§ 5. Der Prokurator des Königs ist mit der Ausführung der Genehmigungen in Bezug auf die in § 1 Absatz 1 erwähnte Maßnahme, die im Rahmen einer gerichtlichen Untersuchung gemäß Artikel 56*bis* vom Untersuchungsrichter erteilt wurden, beauftragt.

Der Prokurator des Königs vermerkt zu diesem Zeitpunkt in einer getrennten schriftlichen Entscheidung die Straftaten, die von den Polizeidiensten und den in § 3 Absatz 3 erwähnten Personen im Rahmen der vom Untersuchungsrichter angeordneten Maßnahme begangen werden dürfen. Diese Entscheidung wird in der in § 3 Absatz 7 erwähnten Akte aufbewahrt ».

B.28.2. In der Begründung zu dieser Bestimmung heißt es:

« Cet article introduit la possibilité de procéder à une infiltration ou à une interaction sur Internet qui ne vise pas uniquement une vérification ciblée ou une arrestation.

Étant donné que l'infiltration sur Internet a un caractère moins intrusif que l'infiltration ' classique ' et que les différents contacts durant l'exécution de cette mesure sont enregistrés, un régime plus souple est justifié » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1966/001, p. 36).

Was den Unterschied der Regelung gegenüber der Infiltrierung in der realen Welt betrifft

B.29.1. Der erste Teil des zweiten Klagegrunds ist abgeleitet aus einer Verletzung der Artikel 10 und 11 der Verfassung. Die klagenden Parteien sind der Auffassung, dass das aus dem virtuellen oder realen Charakter der Infiltrierungsmaßnahme hergeleitete Kriterium nicht rechtfertigen kann, dass einerseits der Prokurator des Königs im Rahmen einer Infiltrierung im Internet keine Maßnahmen zur Gewährleistung der Sicherheit sowie der körperlichen, geistigen und moralischen Unversehrtheit des Infiltranten ergreifen kann, und dass andererseits die Kontrolle über die Anwendung der Methode, die in den Artikeln 235*ter* und 235*quater* des Strafprozessgesetzbuches vorgesehen ist, nicht auf die Infiltrierung im Internet anwendbar ist.

B.29.2. Da die klagenden Parteien ein Interesse an der Nichtigerklärung der angefochtenen Bestimmung haben, ist die Frage nach ihrem Interesse am ersten Teil dieses Klagegrunds entgegen den Ausführungen des Ministerrats nicht zu stellen.

Die Sicherheit der « Cyberinfiltranten »

B.30.1. In Artikel 47*octies* des Strafprozessgesetzbuches, der sich auf die Infiltrierung in der realen Welt bezieht, ist in Paragraph 2 Absatz 3 präzisiert, dass der Prokurator des Königs, wenn dies gerechtfertigt ist, die Genehmigung zur Ergreifung der notwendigen Maßnahmen zur Gewährleistung der Sicherheit sowie der körperlichen, geistigen und moralischen Unversehrtheit des Infiltranten erteilt.

B.30.2. In Beantwortung einer Bemerkung des Staatsrates zu diesem Punkt ist in der Begründung erläutert:

« Le Conseil d'Etat se demande aussi, au point 25 de l'avis, pourquoi le procureur du Roi, contrairement à ce qui est le cas pour l'infiltration classique, ne peut pas prendre des mesures en vue de garantir la sécurité, ainsi que l'intégrité physique, psychique et morale du cyberinfiltrant (voir l'article 47*octies*, § 2, dernier alinéa, du Code d'instruction criminelle). Le gouvernement estime que ceci est superflu lorsqu'une infiltration est réalisée uniquement via Internet. Il n'y a tout d'abord pas de contact physique avec d'éventuels suspects. En outre, il va de soi que les cyberinfiltrants continueront de faire l'objet d'un suivi. Aucune base légale n'est requise pour garantir leur intégrité psychique et morale » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1966/001, p. 42).

B.30.3. Die allein im Internet durchgeführte Infiltrierung weist nicht die gleichen Gefahren für die körperliche Sicherheit des Infiltranten auf wie eine Infiltrierung in der realen Welt. Der Gesetzgeber konnte daher vernünftigerweise den Standpunkt vertreten, dass es nicht notwendig ist, die gleichen Möglichkeiten zur Ergreifung von Maßnahmen zur Gewährleistung der körperlichen Sicherheit des Infiltranten, der nur in der virtuellen Welt handelt, vorzusehen. Der beanstandete Behandlungsunterschied beruht somit in diesem Zusammenhang auf einem sachdienlichen Kriterium.

B.30.4. Zudem untersagt die Bestimmung nicht die Anwendung von Maßnahmen zur Begleitung und psychologischen Unterstützung innerhalb der betroffenen Polizeidienste, die für die Situation der Personen geeignet sind, die die Infiltrierungen im Internet durchführen, sodass die angefochtenen Bestimmung keine unverhältnismäßigen Folgen für die Cyberinfiltranten hinsichtlich ihrer geistigen und moralischen Sicherheit hat.

Die Kontrolle durch die Anklagekammer

B.31.1. Durch Artikel 235*ter* des Strafprozessgesetzbuches wird die Anklagekammer beauftragt, unter anderem die Anwendung der Infiltrierungen in der realen Welt zu kontrollieren. Aufgrund derselben Bestimmung kontrolliert die Anklagekammer die Anwendung der Infiltrierungen im Internet nur, wenn in diesem Rahmen eine vertrauliche Akte angelegt worden ist.

Eine vertrauliche Akte muss bei der Genehmigung einer Infiltrierung in der realen Welt immer angelegt werden. Sie enthält die Genehmigung zur Infiltrierung, die Entscheidungen zur Änderung, Ergänzung oder Verlängerung sowie die Berichte, die vom Gerichtspolizeioffizier über jede Phase der Durchführung der Infiltrierungen erstellt werden, die er leitet. Hingegen muss bei einer Infiltrierung im Internet eine vertrauliche Akte nur in zwei Fällen angelegt werden: wenn der Infiltrant auf die Fachkompetenz einer nicht den Polizeidiensten angehörenden Person zurückgreift und wenn der Prokurator des Königs die Begehung einer Straftat genehmigt.

B.31.2. Die Erstellung der vertraulichen Akte rührt aus der Notwendigkeit her, in bestimmten Strafprozessen die Anonymität von Zeugen zu wahren oder die eingesetzten Ermittlungsmethoden geheim zu halten; diese Interessen und die Verteidigungsrechte des Angeklagten, die grundsätzlich beinhalten, dass dieser jedes gegen ihn verwandte Beweismittel in Kenntnis des Sachverhalts anfechten kann, müssen gegeneinander abgewogen werden. Die Beteiligung der Anklagekammer aufgrund der Artikel 235*ter* und 235*quater* des Strafprozessgesetzbuches bezieht sich besonders auf die vertrauliche Akte und stellt die Garantie dafür dar, dass ein unabhängiger und unparteiischer Richter eine Kontrolle über die Ordnungsmäßigkeit der Anwendung von besonderen Ermittlungsmethoden und der Beweise, die mit ihnen erlangt wurden, ausübt, wenn die vorerwähnten Interessen es rechtfertigen, dass der Angeklagte keinen Zugang zu der gesamten Strafakte hat.

B.31.3. Im Gegensatz zu dem, was in der realen Welt der Fall ist, werden aufgrund von Paragraph 4 Absatz 2 der angefochtenen Bestimmung alle Kontakte im Rahmen der Infiltrierung im Internet registriert und der Akte beigefügt oder bei der Kanzlei hinterlegt. Personen, die auf der Grundlage von Beweisen verfolgt werden, die im Laufe einer Infiltrierung im Internet gewonnen wurden, haben also Zugang zu der gesamten

Durchführung der Infiltrierung. Sie sind in der Lage, den Einsatz dieser Methode und ihre Ausführungsmodalitäten anzufechten und sie können das Untersuchungsgericht oder das erkennende Gericht auffordern, deren Ordnungsmäßigkeit zu kontrollieren. Es ist also in diesem Fall nicht notwendig, dass eine vertrauliche Akte angelegt und dass eine besondere Kontrolle über sie durch die Anklagekammer ausgeübt wird. Der Behandlungsunterschied beruht in diesem Zusammenhang ebenfalls auf einem sachdienlichen Kriterium.

B.31.4. Der erste Teil des zweiten Klagegrunds ist unbegründet.

Was die Modalitäten zur Bestimmung der Polizeidienste betrifft, die ermächtigt sind, eine Infiltrierung im Internet durchzuführen

B.32.1. Der zweite Teil des zweiten Klagegrunds ist aus einer Verletzung der Artikel 12 und 14 der Verfassung in Verbindung mit Artikel 6 der Europäischen Menschenrechtskonvention abgeleitet und richtet sich gegen Paragraph 1 Absatz 2 des angefochtenen Artikels 7. Die klagenden Parteien werfen dem Gesetzgeber vor, dem König unter Verstoß gegen das Legalitätsprinzip in Strafsachen die Befugnis erteilt zu haben, die Modalitäten zur Bestimmung der Polizeidienste festzulegen, die ermächtigt sind, die Infiltrierungsmaßnahme im Internet durchzuführen.

B.32.2. In der Begründung ist zu dieser Ermächtigung angegeben:

« S'agissant des services de police qui vont pouvoir réaliser la nouvelle mesure, il n'est pas nécessaire d'avoir un régime aussi strict que pour l'infiltration telle qu'elle existe actuellement. Cette dernière est réservée aux membres des unités spéciales de la police fédérale (DSU). Cela est justifié par la dangerosité de la mesure, y compris et surtout pour l'agent infiltrant. Cette limitation n'est pas justifiée pour la mesure se déroulant uniquement sur Internet. Cela ne signifie toutefois pas que tout enquêteur pourra se voir charger d'exécuter une telle interaction ou infiltration. Seuls les services de police spécifiquement désignés pourront exécuter la mesure. Une formation spécifique sera prévue tant pour protéger la vie privée des personnes visées que pour assurer le bon déroulement des enquêtes. Dans l'avant-projet, cette désignation était déléguée au ministre de la Justice. Le Conseil d'Etat observe qu'une telle délégation n'est pas autorisée et que les services de police compétents devraient être repris dans la loi. Le gouvernement fait remarquer qu'une telle délégation au ministre de la Justice existe déjà dans le cadre de l'application des méthodes particulières de recherche (art. 47*ter*, § 1er, alinéa 2, CIC) et qu'il n'appartient pas au législateur d'élaborer un règlement détaillé. Une formation spécifique sera en effet prévue pour les services de police visés, en vue aussi bien de la protection de la vie privée des

personnes visées que de l'assurance du bon déroulement des enquêtes. Pour ces raisons, le gouvernement prend l'option de faire déterminer les conditions, y compris pour ce qui concerne la formation, et modalités de la désignation des services de police compétents par le Roi » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1966/001, p. 40).

B.33.1. Indem die Artikel 12 Absatz 2 und 14 der Verfassung der gesetzgebenden Gewalt die Zuständigkeit verleihen, einerseits festzulegen, in welchen Fällen und in welcher Form eine Strafverfolgung möglich ist, und andererseits ein Gesetz anzunehmen, aufgrund dessen eine Strafe festgelegt und angewandt werden kann, gewährleisten sie jedem Rechtsuchenden, dass ein Verhalten nur strafbar gemacht werden und eine Strafe nur auferlegt werden kann auf der Grundlage von Regeln, die durch eine demokratisch gewählte beratende Versammlung angenommen wurden.

B.33.2. Das Legalitätsprinzip in Strafsachen geht nicht soweit, dass es den Gesetzgeber verpflichtet, jeden Aspekt des Strafverfahrens selbst zu regeln. Eine Ermächtigung der ausführenden Gewalt verletzt nicht dieses Prinzip, insofern die Ermächtigung ausreichend genau beschrieben ist und sich auf die Ausführung von Maßnahmen bezieht, deren wesentliche Elemente vorher durch den Gesetzgeber festgelegt wurden.

B.34.1. Im vorliegenden Fall kann angenommen werden, dass der Gesetzgeber der Auffassung war, es sei notwendig, den König zu ermächtigen, die für die Durchführung von Infiltrierungen im Internet zuständigen Polizeidienste zu bestimmen. In einem sich fortwährend weiterentwickelnden Bereich wie dem Internet ist es in der Tat angezeigt, dass eine gewisse Flexibilität es den Behörden ermöglicht, den Inhalt der Ausbildung, mit der die Polizisten die Infiltrierungsmaßnahme im Internet durchführen können, regelmäßig anzupassen, was ebenfalls voraussetzt, die Bestimmung der ermächtigten Polizeioffiziere entsprechend der Ausbildungen, über die die Mitglieder der betroffenen Dienste verfügen und die sie absolviert haben, anpassen zu können.

Außerdem legt Artikel 46*sexies* des Strafprozessgesetzbuches die Bedingungen fest, unter denen die Infiltrierung im Internet angeordnet werden kann. Der Gesetzgeber hat durch die angefochtene Bestimmung den König ermächtigt, Bestimmungen zu erlassen, die sich auf Maßnahmen beziehen, deren wesentliche Elemente er also selbst festgelegt hat.

B.34.2. Der zweite Teil des zweiten Klagegrunds ist unbegründet.

Was den Ausschluss von bestimmten zielgerichteten Maßnahme aus dem Begriff der Infiltrierung betrifft

B.35.1. Der dritte Teil des zweiten Klagegrunds ist aus einer Verletzung der Artikel 12 und 14 der Verfassung abgeleitet und richtet sich gegen Artikel 46*sexies* Paragraph 1 Absatz 4 des Strafprozessgesetzbuches. Die klagenden Parteien werfen dem Gesetzgeber vor, dass er es unter Verstoß gegen das Legalitätsprinzip in Strafsachen unterlassen hat, zu definieren, welche im Internet durchgeführten Ermittlungshandlungen nicht vom Prokurator des Königs erlaubt werden müssen und somit auf Initiative der Polizisten vorgenommen werden können. Sie sind der Auffassung, dass es der Ausdruck « Interaktion, die nur eine gezielte Überprüfung oder eine Festnahme zum unmittelbaren Zweck hat, » den Gerichtspolizeioffizieren ermöglicht, die strengen Bedingungen für die Infiltrierung im Internet zu umgehen oder zu missachten.

B.35.2. Das in Artikel 12 Absatz 2 der Verfassung festgelegte Erfordernis der Vorhersehbarkeit des Strafverfahrens garantiert jedem Rechtsunterworfenen, dass er nur Gegenstand einer Ermittlung, einer gerichtlichen Untersuchung oder einer Verfolgung gemäß einem Verfahren sein kann, von dem er vor dessen Anwendung Kenntnis nehmen kann.

B.36. In der Begründung zu der angefochtenen Bestimmung ist angegeben:

« Cette précision vise à éviter de créer une situation où les services de police voient leur capacité d'action sur Internet réduite par rapport à ce qui existe actuellement que ce soit sur Internet ou dans le monde physique » (*Doc. parl*., Chambre, 2015-2016, DOC 54-1966/001, p. 38).

Die folgenden Beispiele werden anschließend genannt: ein Kontakt für die Vereinbarung eines Treffens, um einen Gegenstand anzusehen, der über eine « Kleinanzeige » zum Verkauf angeboten wurde, die in einer Zeitung veröffentlicht oder auf einer Internetseite für den Verkauf von Gebrauchtartikeln platziert wurde; eine kurze Interaktion mit einer Person, die eine Nachricht im Internet gepostet hat, um festzustellen, ob es sich um eine ernsthaft radikalisierte Person oder einen unbedeutenden Witzbold handelt; die Festlegung eines Treffpunkts mit einer Person, um sie festzunehmen zu können. In dem Text wird erläutert,

dass in diesen Fällen der Polizist seine Stellung nicht erwähnt, aber auch keine falsche Identität benutzt, und dass diese Art der Interaktion « sich nur auf einen spezifischen und sehr beschränkten Aspekt bezieht » (ebd., S. 39).

B.37.1. Aus dem Text der angefochtenen Bestimmung, der durch die Präzisierungen in der vorerwähnten Begründung erläutert wird, ist ausreichend ersichtlich, dass die Infiltrierung im Internet, die nur mit der Genehmigung des Prokurators des Königs durchgeführt werden kann, in der « Unterhaltung » von Kontakten mit einem oder mehreren Verdächtigen unter Vorspiegelung einer fiktiven Identität besteht. Ebenso definiert Artikel 47*octies* des Strafprozessgesetzbuches, der sich auf die Infiltrierung in der realen Welt bezieht, diese als den « unter einer fiktiven Identität unterhaltenen dauerhaften Kontakt » zu einem oder mehreren Verdächtigen. Die Infiltrierung in diesen beiden Formen setzt also einerseits die Entwicklung einer glaubwürdigen fiktiven Identität für den Infiltranten und andererseits eine Interaktion von einer gewissen Dauer mit einer oder mehreren Personen voraus, die im Verdacht stehen, Straftaten einer bestimmten Schwere zu begehen oder begehen zu können. Punktuelle Kontakte, um ein Treffen zu vereinbaren oder eine gezielte Überprüfung vorzunehmen, die es der Gerichtspolizei ermöglichen, gemäß Artikel 15 des Gesetzes vom 5. August 1992 über das Polizeiamt ihre Aufgaben zu erfüllen, fallen nicht unter diese Definition und müssen daher nicht vorher vom Prokurator des Königs genehmigt werden.

B.37.2. Der dritte Teil des zweiten Klagegrunds ist unbegründet.

Aus diesen Gründen:

Der Gerichtshof

1. erklärt für nichtig:

- Artikel 39*bis* § 3 des Strafprozessgesetzbuches, eingefügt durch Artikel 2 des Gesetzes vom 25. Dezember 2016 « zur Festlegung verschiedener Abänderungen des Strafprozessgesetzbuches und des Strafgesetzbuches im Hinblick auf die Verbesserung der besonderen Ermittlungsmethoden und bestimmter Ermittlungsmaßnahmen in Sachen Internet, elektronische Nachrichten und Telekommunikation und zur Schaffung einer Datenbank der Stimmabdrücke »;

- Artikel 13 des vorerwähnten Gesetzes vom 25. Dezember 2016;

- Artikel 39*bis* des Strafprozessgesetzbuches, eingefügt durch Artikel 2 des vorerwähnten Gesetzes vom 25. Dezember 2016, insofern er keine besondere Bestimmung im Hinblick auf die Wahrung des Berufsgeheimnisses von Ärzten und Rechtsanwälten vorsieht;

2. erhält die Folgen der für nichtig erklärten Bestimmungen bis zum Datum der Veröffentlichung des vorliegenden Entscheids im *Belgischen Staatsblatt* aufrecht;

3. weist die Klage, vorbehaltlich der in B.15.2 und B.22.2 erwähnten Auslegungen, im Übrigen zurück.

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

Der Kanzler, Der Präsident,

F. Meersschaut F. Daoût