

VERNEHMLASSUNGSBERICHT

DER REGIERUNG

BETREFFEND

**DIE ABÄNDERUNG DES KOMMUNIKATIONSGESETZES UND DER
STRAFPROZESSORDNUNG**

(Vorratsdatenspeicherung)

Ministerium für Inneres, Justiz und Wirtschaft

Vernehmlassungsfrist: 31. August 2016

INHALTSVERZEICHNIS

	Seite
Zusammenfassung	4
Zuständiges Ministerium.....	5
Betroffene Stellen	5
1. Ausgangslage	6
1.1 Das Urteil des Gerichtshofes der Europäischen Union	6
1.2 Die liechtensteinischen Bestimmungen zur Speicherung von Daten auf Vorrat.....	10
2. Begründung der Vorlage.....	11
3. Schwerpunkte der Vorlage	15
3.1 Speicherung von Daten auf Vorrat.....	15
3.2 Definition von schweren Straftaten	15
3.3 Speicherdauer (Löschfrist)	16
3.4 Richtervorbehalt.....	16
3.5 Datensicherheit	16
3.6 Unabhängigkeit der Überwachung / Rechtsschutz und Kontrolle / Sanktionen.....	17
3.7 Zeugnisverweigerungsrecht / Berufsgeheimnisträger.....	18
4. Erläuterungen zu den einzelnen Artikeln	20
4.1 Allgemeines	20
4.2 Abänderung des KomG	21
4.3 Abänderung der StPO.....	34
5. Verfassungsmässigkeit / Rechtliches.....	35
6. Regierungsvorlagen	37
6.1 Kommunikationsgesetz	37
6.2 Strafprozessordnung	47

Beilage:

Urteil des Gerichtshofes vom 8. April 2014 C-293/12 und C-594/12

ZUSAMMENFASSUNG

Mit seinem Urteil vom 8. April 2014 in der Rechtssache C-293/12 erklärte der Gerichtshof der Europäischen Union (EuGH) die Richtlinie über die Vorratsspeicherung von Daten (2006/24/EG) für ungültig, da sie einen Eingriff von grossem Ausmass und besonderer Schwere in die Grundrechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten beinhaltet, der sich nicht auf das absolut Notwendige beschränke.

Die liechtensteinischen Bestimmungen zur Speicherung von Daten auf Vorrat („Vorratsdatenspeicherung“) sind im Kommunikationsgesetz (KomG) normiert. Sie setzen die in das EWR-Abkommen übernommene Richtlinie 2002/58/EG und – freiwillig – auch die nunmehr vom Europäischen Gerichtshof als ungültig erklärte Richtlinie 2006/24/EG um.

Das Urteil des EuGH ist insofern für Liechtenstein von Bedeutung, als die in der Grundrechtscharta der Europäischen Union normierten Grundrechte weitgehend identisch mit den von der Liechtensteinischen Verfassung und der in Liechtenstein anwendbaren Europäischen Menschenrechtskonvention normierten Grundrechten sind und das Urteil somit weitgehend auch auf die liechtensteinischen Verhältnisse übertragbar ist. Nach dem Ergehen des Urteils des EuGH war deshalb zu prüfen, in wie weit die liechtensteinischen Bestimmungen den grundrechtlichen Anforderungen vollumfänglich zu genügen vermögen.

Mit dem vorliegenden Vernehmlassungsbericht sollen der weitere Bedarf sowie der Umfang an einer Vorratsdatenspeicherung in Liechtenstein aufgezeigt werden und die notwendigen gesetzlichen Anpassungen vorgenommen werden. Die Anpassungen umfassen folgende Schwerpunkte:

- Schaffung einer eindeutigen und abschliessenden Definition von „schweren“ Straftaten, also jener Straftaten, bei welchen die Verwertung von auf Vorrat gespeicherten Daten zur Anwendung kommen kann.*
- Ausbau der Bestimmungen zur Datensicherheit, zur Gewährleistung eines Sicherheitsniveaus, welches der Bedeutung der auf Vorrat gespeicherten Daten bzw. dem potentiellen Risiko einer Verletzung der Privatsphäre Rechnung trägt.*

- *Sicherstellung einer unabhängigen Überwachung durch die Datenschutzstelle und die Schaffung von Instrumenten zur Kontrolle.*
- *Rechtsschutz und Kontrolle im Zusammenhang mit der Speicherung und der Verwertung von auf Vorrat gespeicherten Daten.*
- *Einführung eines Systems von Sanktionen bei Zuwiderhandlungen gegen Vorschriften über die Speicherung auf Vorrat von Daten und den dazugehörenden Datenschutzbestimmungen.*
- *Berücksichtigung von Zeugnisverweigerungsrechten und Berufsgeheimnisträgern bei der Speicherung von Daten auf Vorrat bzw. deren Verwertung.*

Es sollen ausserdem notwenige gesetzliche Anpassungen im Zusammenhang mit der Übernahme von zwei EU Rechtsakten ins EWR Abkommen - namentlich Verordnung (EU) 2015/2120 über Massnahmen zum Zugang zum offenen Internet und über das Roaming sowie Richtlinie 2014/53/EU über die Bereitstellung von Funkanlagen - behandelt werden.

ZUSTÄNDIGES MINISTERIUM

Ministerium für Inneres, Justiz und Wirtschaft

BETROFFENE STELLEN

Amt für Kommunikation

Datenschutzstelle

Landespolizei

Staatsanwaltschaft

Fürstliches Landgericht

Fürstliches Obergericht

Fürstlicher Oberster Gerichtshof

Vaduz, 5. Juli 2016

LNR 2016-760

1. AUSGANGSLAGE

1.1 Das Urteil des Gerichtshofes der Europäischen Union

Mit seinem Urteil vom 8. April 2014 in der Rechtssache C-293/12 erklärte der Gerichtshof der Europäischen Union (EuGH) die Richtlinie über die Vorratsspeicherung von Daten (2006/24/EG)¹ für ungültig, da sie einen Eingriff von grossem Ausmass und besonderer Schwere in die Grundrechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten beinhalte, der sich nicht auf das absolut Notwendige beschränke.

Zusammengefasst kam der EuGH zu folgendem Ergebnis: Mit der Richtlinie über die Vorratsspeicherung von Daten (2006/24/EG) sollen in erster Linie die Vorschriften der Mitgliedstaaten über die Vorratsspeicherung bestimmter, von den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder den Betreibern eines öffentlichen Kommunikationsnetzes erzeugter oder verarbeiteter Daten harmonisiert werden. Damit solle sichergestellt werden, dass die Daten zwecks Verhütung, Ermittlung, Feststellung und Verfolgung von schweren Straftaten wie organisierter Kriminalität und Terrorismus zur Verfügung stünden. Die Richtlinie sehe daher vor, dass die genannten Anbieter und Betreiber die Verkehrs- und Standortdaten sowie alle damit in Zusammenhang stehenden Daten, die zur Feststellung des Teilnehmers oder Benutzers erforderlich sind, auf

¹ Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG.

Vorrat speichern müssen. Dagegen gestatte die Richtlinie keine Speicherung des Inhalts einer Nachricht und der abgerufenen Informationen auf Vorrat.

Der EuGH stellte zunächst fest, dass nach der Richtlinie alle Verkehrsdaten betreffend Telefonfestnetz, Mobilfunk, Internetzugang, Internet-E-Mail und Internet-Telefonie auf Vorrat zu speichern seien. Ausserdem erfasse die Richtlinie alle Teilnehmer und registrierten Benutzer. Sie führe daher zu einem Eingriff in die Grundrechte fast der gesamten europäischen Bevölkerung.

Der EuGH sah in der Verpflichtung zur Speicherung dieser Daten auf Vorrat und der Gestattung des Zugriffs der zuständigen nationalen Behörden auf dieselben einen besonders schwerwiegenden Eingriff in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten. Ausserdem sei der Umstand, dass die Speicherung der Daten auf Vorrat und ihre spätere Nutzung vorgenommen würden, ohne dass die Teilnehmer oder die registrierten Benutzer darüber informiert werden, geeignet, bei den Betroffenen das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung sei.

Der EuGH prüfte sodann, ob ein solcher Eingriff in die fraglichen Grundrechte gerechtfertigt sei.

Er stellte fest, dass die nach der Richtlinie vorgeschriebene Speicherung von Daten auf Vorrat nicht geeignet sei, den Wesensgehalt der Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten anzutasten. Die Richtlinie gestatte nämlich nicht die Kenntnisnahme des Inhalts elektronischer Kommunikation als solches und sehe vor, dass die Dienstanbieter bzw. Netzbetreiber bestimmte Grundsätze des Datenschutzes und der Datensicherheit einhalten müssten.

Die Speicherung der Daten auf Vorrat zur etwaigen Weiterleitung an die zuständigen nationalen Behörden stelle auch eine Zielsetzung dar, die dem Gemein-

wohl diene, und zwar der Bekämpfung schwerer Kriminalität und somit letztlich der öffentlichen Sicherheit.

Der EuGH kam jedoch im Weiteren zu dem Ergebnis, dass bei der Richtlinie die Wahrung des Grundsatzes der Verhältnismässigkeit nicht eingehalten sei.

Zwar sei die nach der Richtlinie vorgeschriebene Speicherung der Daten auf Vorrat zur Erreichung des mit ihr verfolgten Ziels geeignet, doch beinhalte sie einen Eingriff von grossem Ausmass und von besonderer Schwere in die fraglichen Grundrechte, ohne dass sie Bestimmungen enthalte, die zu gewährleisten vermögen, dass sich der Eingriff tatsächlich auf das absolut Notwendige beschränke.

Erstens erstrecke sich die Richtlinie nämlich generell auf sämtliche Personen, elektronische Kommunikationsmittel und Verkehrsdaten, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des Ziels der Bekämpfung schwerer Straftaten vorzusehen.

Zweitens sehe die Richtlinie kein objektives Kriterium vor, das es ermögliche, den Zugang der zuständigen nationalen Behörden zu den Daten und deren Nutzung zwecks Verhütung, Feststellung oder strafrechtlicher Verfolgung auf Straftaten zu beschränken, die im Hinblick auf das Ausmass und die Schwere des Eingriffs in die fraglichen Grundrechte als so schwerwiegend angesehen werden können, dass sie einen solchen Eingriff rechtfertigen. Die Richtlinie nehme im Gegenteil lediglich allgemein auf die von jedem Mitgliedstaat in seinem nationalen Recht bestimmten „schweren Straftaten“ Bezug.

Drittens enthalte die Richtlinie keine materiell- und verfahrensrechtlichen Voraussetzungen für den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung. Vor allem unterläge der Zugang zu den Daten keiner vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle.

Viertens schreibe die Richtlinie eine Dauer der Vorratsspeicherung der Daten von mindestens sechs Monaten vor, ohne dass eine Unterscheidung zwischen den Datenkategorien anhand der betroffenen Personen oder nach Massgabe des etwaigen Nutzens der Daten für das verfolgte Ziel getroffen werde. Die Speichungsfrist liege zudem zwischen mindestens sechs und höchstens 24 Monaten, ohne dass die Richtlinie objektive Kriterien festlege, die gewährleisten, dass die Speicherung auf das absolut Notwendige beschränkt werde.

Fünftens stellte der EuGH fest, dass die Richtlinie keine hinreichenden Garantien dafür biete, dass die Daten wirksam vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang und jeder unberechtigten Nutzung geschützt seien. Unter anderem gestatte sie es den Diensteanbietern, bei der Bestimmung des von ihnen angewandten Sicherheitsniveaus wirtschaftliche Erwägungen (insbesondere hinsichtlich der Kosten für die Durchführung der Sicherheitsmassnahmen) zu berücksichtigen, und gewährleiste nicht, dass die Daten nach Ablauf ihrer Speichungsfrist unwiderruflich vernichtet würden.

Schliesslich rügte der EuGH, dass die Richtlinie keine Speicherung der Daten im Unionsgebiet vorschreibe. Sie gewährleiste damit nicht in vollem Umfang, dass die Einhaltung der Erfordernisse des Datenschutzes und der Datensicherheit durch eine unabhängige Stelle überwacht werde, obwohl die Charta dies ausdrücklich fordere. Eine solche Überwachung auf der Grundlage des Unionsrechts sei aber ein wesentlicher Bestandteil der Wahrung des Schutzes der Betroffenen bei der Verarbeitung personenbezogener Daten.

1.2 Die liechtensteinischen Bestimmungen zur Speicherung von Daten auf Vorrat

Die liechtensteinischen Bestimmungen zur Speicherung von Daten auf Vorrat („Vorratsdatenspeicherung“) sind im Kommunikationsgesetz (KomG)² normiert. Sie setzen die in das EWR-Abkommen übernommene Richtlinie 2002/58/EG³ und auch die nunmehr vom Europäischen Gerichtshof als ungültig erklärte Richtlinie 2006/24/EG um.

Konkret finden sich die einschlägigen Bestimmungen in den Artikeln 52 bis 53 KomG im Abschnitt „XI. Kommunikationsgeheimnis; Datenschutz; Mitwirkungspflichten“ unter dem Unterabschnitt „Mitwirkung bei einer Überwachung“. In Artikel 52 sind die grundsätzlichen Bestimmungen enthalten; in Artikel 52a die Bestimmungen über die Speicherung von Daten auf Vorrat; in Artikel 52b die Bestimmungen über die Datenschutzkontrolle und in Artikel 53 die Bestimmungen über die Teilnehmerdaten.

Gemäss heutiger Praxis der Strafverfolgungsbehörden erfolgt der Zugriff auf die auf Vorrat gespeicherten Daten nach Art. 52a KomG durch die Strafverfolgungsbehörden im Weg der Beschlagnahme. Diese ist in den §§ 96 ff. der Strafprozessordnung (StPO)⁴ in deren „IX. Hauptstück Von der Identitätsfeststellung, der Haus- und Personendurchsuchung, der körperlichen und molekulargenetischen Untersuchung, der Beschlagnahme, der Überwachung der elektronischen Kommunikation, der Observation, der verdeckten Ermittlung und dem Scheingeschäft sowie vom Schutz der geistlichen Amtsverschwiegenheit und der Berufsgeheim-

² Gesetz vom 17. März 2006 über die elektronische Kommunikation (Kommunikationsgesetz; KomG), LGBL. 2006 Nr. 91.

³ Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

⁴ Strafprozessordnung (StPO) vom 18. Oktober 1988, LGBL. 1968 Nr. 62.

nisse“ im Unterabschnitt „II. Beschlagnahme“ geregelt. Die Verwertung von auf Vorrat gespeicherten Daten stellt allerdings einen Sonderfall dar, der weder als Überwachung im Sinne von § 103 StPO noch als Beschlagnahme im Sinne des §§ 96 ff. StPO zu qualifizieren ist. Diesem Umstand soll durch die vorliegende Gesetzesrevision Rechnung getragen werden, indem mit § 98b StPO eine entsprechende Sonderbestimmung eingeführt werden soll.

2. BEGRÜNDUNG DER VORLAGE

Das Urteil des EuGH ist insofern für Liechtenstein von Bedeutung, als die in der Grundrechtscharta der Europäischen Union normierten Grundrechte weitgehend identisch mit den von der Liechtensteinischen Verfassung und der in Liechtenstein anwendbaren Europäischen Menschenrechtskonvention normierten Grundrechten sind und das Urteil somit weitgehend auch auf die liechtensteinischen Verhältnisse übertragbar ist.

Dies bedeutet allerdings nicht, dass die liechtensteinischen Bestimmungen zur Speicherung von Daten auf Vorrat mit dem Urteil des EuGH automatisch und vollständig grundrechtswidrig sind. Die liechtensteinischen Bestimmungen stellen eine Umsetzung der genannten Richtlinien dar. Die Staaten geniessen bei der Umsetzung von Richtlinien in das nationale Recht einen gewissen Spielraum. Im Rahmen dieses Spielraums kann die liechtensteinische Umsetzung durchaus grundrechtskonform ausgestaltet worden sein. Nach dem Ergehen des Urteils des EuGH war deshalb zu prüfen, in wie weit die liechtensteinischen Bestimmungen den grundrechtlichen Anforderungen vollumfänglich zu genügen vermögen.

Aus diesem Grund setzte die Regierung mit LNR 2014-1176 BNR 2014/1263 eine Arbeitsgruppe ein, welche sich aus Vertretern des Amts für Kommunikation (Vorsitz), des Amts für Justiz, der Datenschutzstelle, der Landespolizei, der Staatsanwaltschaft und des Landgerichts zusammensetzten. Die Arbeitsgruppe war be-

auftrag, im Licht des genannten EuGH-Urteils den allfälligen weiteren Bedarf an einer Speicherung von Daten auf Vorrat in Liechtenstein aufzuzeigen; zu prüfen, in welchem Umfang eine Speicherung von Daten auf Vorrat in Liechtenstein noch möglich ist; allfällige Alternativen zur Speicherung von Daten auf Vorrat aufzuzeigen und mit Bezug auf ihre Erkenntnisse zu den vorstehenden Aufgaben der Regierung einen Bericht mit einer Empfehlung über das weitere Vorgehen abzugeben.

Die Arbeitsgruppe kam zusammengefasst zu dem Ergebnis, dass die liechtensteinischen Bestimmungen zur Speicherung von Daten auf Vorrat einer Normenkontrolle durch den Staatsgerichtshof wohl zumindest nicht vollumfänglich standhalten würden, dass aber weiterhin unzweifelhaft Bedarf an einer Vorratsdatenspeicherung besteht. Konkret führte die Arbeitsgruppe aus:

Die im Rahmen der Speicherung von Daten auf Vorrat für die Strafverfolgungsbehörden verfügbaren Informationen seien jedenfalls in vielen Verfahren ein wesentlicher und unverzichtbarer Bestandteil der Ermittlungen und der Beweisführung. Je nach Sachverhalt sei dabei eine Aufklärung eines Tatverdächtigen ohne Verwertung dieser Daten nur schwer möglich, wenn nicht gar unmöglich.

Dies insbesondere, wenn zwischen Täter und Opfer lediglich telefonischer Kontakt bestehe. Dies treffe in klassischer Weise auf den Tatbestand der beharrlichen Verfolgung (Stalking) zu, bei dem eine Aufklärung des Tatverdächtigen bzw. eine Beweisführung ohne Vorratsdaten regelmässig unmöglich sein werde. Dazu gehören aber auch andere, regelmässig unter Verwendung von Mitteln der elektronischen Kommunikation begangene Delikte, wie Betrügereien (z.B. „Enkeltrick“) oder Drohungen/Nötigungen. Darüber hinaus könne selbst dann in vielen Fällen durch die Verwertung der auf Vorrat gespeicherten Daten relevante Erkenntnisse gewonnen werden, wenn es nicht um eine Kommunikation zwischen Täter und Opfer gehe. Dies anhand des Bewegungsprofils (Zellenstandort),

der Kontakte zwischen Tatverdächtigen (insbesondere im Betäubungsmittelbereich) oder zur Unterstützung bewilligter Observationen.

In diesem Zusammenhang dürfe auch nicht vergessen werden, dass Liechtenstein aufgrund des hiesigen Finanzplatzes und des kleinen Grenzverkehrs im Dreiländereck FL-CH-A vielfach auch mit Anfragen zu Vorratsdaten im Weg der internationalen Rechtshilfe konfrontiert werde. Diese Rechtshilfeleistung sei nicht mehr möglich, wenn Liechtenstein die Vorratsdatenspeicherung abschaffen würde.

Der EuGH habe die Speicherung von Daten auf Vorrat nicht als grundsätzlich unzulässig angesehen, sondern die Ausgestaltung einzelner Punkte in der Richtlinie als nicht konform mit grundrechtlichen Anforderungen befunden.

Der EuGH habe dabei ein weitgehend identisches Prüfungsraster angewendet, wie es analog auch vom liechtensteinischen Staatsgerichtshof angewendet werde. Nach diesem sei eine Beschränkung von Grundrechten zulässig, wenn (summarische Darstellung):

- sie durch eine klare gesetzliche Grundlage, welche die Beschränkung präzise definiert, erfolge;
- sie durch ein überwiegendes öffentliches Interesse gerechtfertigt sei;
- die gewählten Mittel zum verfolgten Zweck verhältnismässig seien (Geeignetheit, Erforderlichkeit, Übermassverbot) und
- die getroffene Beschränkung das betroffene Grundrecht nicht seines Kerngehaltes beraube.

Dieses Raster sei auf sämtliche zu prüfenden Punkte anzuwenden. Im Licht der Erkenntnisse des EuGH hat die Arbeitsgruppe die folgenden massgeblichen Punk-

te identifiziert und in Bezug auf die aktuelle Vorratsdatenspeicherung in Liechtenstein einer näheren Prüfung unterzogen:

- Definition von schweren Straftaten
- Löschfrist (Speicherdauer)
- Richtervorbehalt
- Datensicherheit
- Unabhängigkeit der Überwachung
- Rechtsschutz und Kontrolle
- Sanktionen
- Zeugnisverweigerungsrecht / Berufsgeheimnisträger

Dabei ist Arbeitsgruppe zu dem Ergebnis gekommen, dass die folgenden Bereiche auch heute schon als grundrechtskonform anzusehen sind und somit keiner (materiellen) Gesetzesanpassung bedürfen:

- Speicherdauer (Löschfrist)
- Richtervorbehalt
- Zeugnisverweigerungsrecht

In den restlichen Bereichen verortete die Arbeitsgruppe materiellrechtliche Defizite und empfahl der Regierung in ihrem Bericht deren Behebung. Dem wird mit dem vorliegenden Vernehmlassungsbericht nachgekommen.

3. SCHWERPUNKTE DER VORLAGE

3.1 Speicherung von Daten auf Vorrat

Die Vorlage bezweckt die Behebung der von der Arbeitsgruppe erkannten materiellrechtlichen Defizite und eine grundrechtskonforme Normierung der Speicherung von Daten auf Vorrat. Die Anpassungen umfassen folgende Schwerpunkte:

- Schaffung einer eindeutigen und abschliessenden Definition von „schweren“ Straftaten, also jener Straftaten, bei welchen die Verwertung von auf Vorrat gespeicherten Daten zur Anwendung kommen kann.
- Ausbau der Bestimmungen zur Datensicherheit, zur Gewährleistung eines Sicherheitsniveaus, welches der Bedeutung der auf Vorrat gespeicherten Daten bzw. dem potentiellen Risiko einer Verletzung der Privatsphäre Rechnung trägt.
- Sicherstellung einer unabhängigen Überwachung durch die Datenschutzstelle und die Schaffung von Instrumenten zur Kontrolle.
- Rechtsschutz und Kontrolle im Zusammenhang mit der Speicherung und der Verwertung von auf Vorrat gespeicherten Daten.
- Einführung eines Systems von Sanktionen bei Zuwiderhandlungen gegen Vorschriften über die Speicherung auf Vorrat von Daten und den dazugehörenden Datenschutzbestimmungen.
- Berücksichtigung von Zeugnisverweigerungsrechten und Berufsgeheimnisträgern bei der Speicherung von Daten auf Vorrat bzw. deren Verwertung.

3.2 Definition von schweren Straftaten

Weder die Richtlinie noch die höchstgerichtliche Rechtsprechung geben im Detail vor, was unter einer „schweren“ Straftat zu verstehen ist. Es liegt daher in der Kompetenz des Gesetzgebers, was als „schwere“ Straftat angesehen und damit

der Verwendung von Vorratsdaten zugänglich sein soll. Es erscheint dabei aufgrund von § 17 Abs. 1 StGB zulässig, sämtliche „Verbrechen“ gemäss StGB als „schwere“ Straftaten anzusehen: Denn das StGB definiert Verbrechen als mit mehr als dreijähriger Freiheitsstrafe bedrohte Straftaten. Damit besteht zum einen auch ohne explizite Aufzählung ein klarer Katalog der in Frage kommenden Straftaten, welche zudem infolge der Strafdrohung nachvollziehbar als „schwer“ zu taxieren sind. Mit einer solchen Definition würde auch der höchstgerichtlichen Rechtsprechung entsprochen, welche genau definierte Straftaten verlangt.

3.3 Speicherdauer (Löschfrist)

Im Licht der genannten Rechtsprechung ist eine Speicherdauer / Löschfrist von 6 Monaten – wie sie aktuell gilt – zu rechtfertigen und soll daher beibehalten werden.

3.4 Richtervorbehalt

Auch der bereits heute existierende Richtervorbehalt soll beibehalten bleiben.

3.5 Datensicherheit

Als Leitfaden wurden hierfür die höchstgerichtlichen Urteile herangezogen, z.B. das Bundesverfassungsgericht, aber auch bestehende (ausländische) gesetzliche Regelungen, wie zum Beispiel die österreichische Datensicherheitsverordnung (Datensicherheitsverordnung zum TKG (TKG-DSVO)), die u.a. Folgendes vorsieht: logische Unterscheidung (nicht physikalisch) zwischen Betriebsdaten und Vorratsdaten; Zugriff auf Vorratsdaten nur durch besonders ermächtigte Mitarbeiter; Transport-/Inhaltsverschlüsselung bei Übermittlung der Daten sowie Identifizierung und Authentifizierung über eine fortgeschrittene elektronische Signatur; Verwendung eines einheitlichen Formblatts für die Übermittlung der Daten; Revisions-sichere Protokollierung und die Pflicht zur Erstellung interner Richtlinien.

Die einzuhaltenden Sicherheitsstandards, Rechte und Pflichten sollen auf gesetzlichebene (KomG) vorgegeben werden. Die technische Konkretisierung kann dagegen der Regelung auf Verordnungsebene vorbehalten bleiben (z.B. getrennte Speicherung der Daten, Verschlüsselung, Zugriffsregime unter Nutzung eines Vier-Augen-Prinzips, Protokollierung, Speicherort, unwiederbringliche Löschung, etc.).

3.6 Unabhängigkeit der Überwachung / Rechtsschutz und Kontrolle / Sanktionen

Unter Verweis auf die bereits zitierte höchstgerichtliche Rechtsprechung ist zur Sicherstellung der Grundrechtskonformität ein hinreichender Rechtsschutz (Beschwerdemöglichkeit) notwendig. Der Rechtsschutz ist bereits heute gewährleistet. Die betroffene Person wird im Rahmen eines Strafverfahrens in jedem Fall über die getroffene Massnahme bzw. den Zugriff auf Vorratsdaten informiert (§§ 96, 103 StPO, bei § 103 StPO jedoch erst nach Abschluss; dafür erfolgt eine doppelte Eingriffsprüfung bei Anordnung des Untersuchungsrichters infolge Genehmigungspflicht durch den Präsidenten des Obergerichtes) und ihr steht die Rechtsmittelerhebung offen. Der Rechtsschutz ist demnach gemäss derzeit gültigen StPO-Bestimmungen und infolge des Richtervorbehalts hinreichend gewährleistet.

Bei datenschutzrechtlichen bzw. datensicherheitsrelevanten Verstössen der Anbieter i.S.d. KomG kann zudem eine Anzeige durch die betroffene Person an die Datenschutzstelle gerichtet werden, was zu einer behördlichen Überprüfung (Empfehlung der Datenschutzstelle) und allfälligen Massnahmen (Antrag an die Datenschutzkommission) in einem Verwaltungsverfahren führen kann, jedenfalls soweit der Betroffene davon Kenntnis erhält. Damit ist der Rechtsschutz des Betroffenen gewährleistet. Allfällige Sanktionsbestimmungen im KomG sollen ergänzt werden.

Eine Pflicht zur Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten („data breach notification“), wie sie durch Verordnung (EU) Nr. 611/2013 vorgesehen ist, soll zum jetzigen Zeitpunkt (noch) nicht eingeführt werden. Die Verordnung (EU) Nr. 611/2013 basiert auf Richtlinie 2002/58/EG und insbesondere dessen Art. 4 Abs. 5, welche durch Richtlinie 2009/136/EG (Teil des sog. Telekom Pakets 2009) abgeändert wurde. Das sog. Telekom Paket 2009 befindet sich noch im Übernahmeverfahren und ist mithin noch nicht ins EWR-Abkommen übernommen worden. Die der Verordnung (EU) Nr. 611/2013 zugrundeliegende Richtlinie ist demnach noch nicht verbindlich. Der Entwurf des Gemeinsamen EWR-Beschlusses zur Übernahme der Verordnung (EU) Nr. 611/2013 sieht daher auch vor, dass dieser Beschluss erst mit der Übernahme des sog. Telekom Pakets 2009 in Kraft treten soll. Es ist mit einer Übernahme noch im Jahr 2016 zu rechnen. Sobald das sog. Telekom Paket 2009 ins EWR-Abkommen übernommen ist, ist die rechtliche Grundlage für die Übernahme der Verordnung (EU) Nr. 611/2013 geschaffen, so dass auch diese verbindlich wird. Die dort geregelte Pflicht zur Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten („data breach notification“) kann sodann in nationales Recht übernommen werden.

3.7 Zeugnisverweigerungsrecht / Berufsgeheimnisträger

Das Aussageverweigerungsrecht für Berufsgeheimnisträger ist im Strafverfahren in § 108 StPO geregelt, wobei in dessen Abs. 3 und in § 104d Abs. 2 StPO (eingeführt mit LGBI. 2012 Nr. 26) ein Umgehungsverbot statuiert wird. Es stellt sich die Frage, ob es darüber hinaus eine Bestimmung braucht, wonach die Vorratsdaten zwischen einer verdächtigten Person und einem Berufsgeheimnisträger nicht ausgewertet resp. herausgegeben werden dürfen.

In Österreich gab es Überlegungen, wonach Telekombetreiber separate Listen zu führen haben („whitelist“). Dies wurde vor allem aus Datenschutzgründen abgelehnt.⁵

Eine sog. „white list“ ist auch aus Sicht der Regierung aufgrund folgender Argumente abzulehnen:

- Es kann nicht im Verantwortungsbereich des Betreibers liegen oder diesem aufgebürdet werden, zu entscheiden, wer Geheimnisträger ist und wer nicht.
- Es ist ausserdem problematisch, dass eine solche Entscheidung durch den Betreiber bereits im Vorfeld (bevor eine behördliche Anfrage auf Herausgabe der Daten eingegangen ist) und für alle Daten getroffen werden müsste.
- Und schliesslich ist der Berufsgeheimnisträger nicht schützenswert, der selbst einer Straftat verdächtigt wird. Für ihn gilt das Zeugnisverweigerungsrecht nicht. Insofern kann nicht allein auf die Telefonnummer (Geschäftsanschluss) abgestellt werden, zumal diese auch privat oder bewusst für deliktische Zwecke genutzt werden könnte.
- Es stellt sich zudem die Frage, welche Konsequenz eine solche „white list“ hätte: Muss der Anbieter die Daten trotzdem speichern, kann aber die Herausgabe unter Verweis verweigern, oder darf er bei Berufsgeheimnisträgern gar keine Speicherung vornehmen (mit Ausnahme der rechnungsrelevanten Daten)?

In Deutschland wird vorgeschlagen, dieses Problem mit einem dreistufigen Verfahren zu lösen.⁶

⁵ Christof Tsohl, Vorratsdatenspeicherung – Aufstieg und Fall in Österreich, Seite 97f.; publiziert in: Datenschutzrecht Jahrbuch 2014, Wien, 2014.

Nach Ansicht der Regierung ist § 108 Abs. 3 StPO (i.V.m § 104d Abs. 2 StPO) völlig ausreichend. Danach darf das Recht, die Aussage zu verweigern, nicht umgangen werden, insbesondere nicht durch Sicherstellung und Beschlagnahme von Unterlagen und auf Datenträgern gespeicherten Informationen. Wer zur Verweigerung der Aussage berechtigt ist, ergibt sich aus § 108 Abs. 1 StPO. Das sind neben Personen, die sich durch die Aussage selbst oder einen Angehörigen belasten würden, insbesondere auch Angehörige bestimmter Berufsgruppen (wie z.B. Rechtsanwälte, Fachärzte, etc.). Durch die Ergänzung in § 108 Abs. 3 StPO („Verwertung von Vorratsdaten und auf Datenträgern gespeicherten Informationen“) ist nach Ansicht der Regierung ausreichend gewährleistet, dass die Vorratsdaten zwischen einer verdächtigen Person und einem Berufsheimnisträger nicht ausgewertet werden dürfen.

Eine darüber hinausgehende Regelung ist im Hinblick auf Vorratsdaten daher weder notwendig noch sinnvoll.

4. ERLÄUTERUNGEN ZU DEN EINZELNEN ARTIKELN

4.1 Allgemeines

Regelungsgegenstand sind die Speicherung und Bearbeitung der auf Vorrat gespeicherten Daten durch die Anbieter im Sinne des Art. 3 Abs. 1 Ziff. 2 KomG (Diensteanbieter und Betreiber) einerseits sowie die Verwertung dieser Daten durch die Strafverfolgungsbehörden andererseits. Die entsprechenden Verpflichtungen der Anbieter im Zusammenhang mit der Speicherung und Bearbeitung der auf Vorrat gespeicherten Daten sind bereits heute in Art. 49 ff. KomG geregelt, wobei diese Bestimmungen im Lichte der einschlägigen Rechtsprechung

⁶ Interessenausgleich im Rahmen der Vorratsdatenspeicherung – Analysen und Empfehlungen, A. Rossnagel (Hrsg.), S 155f.

präzisiert werden sollen. Die entsprechenden Vorgaben im Zusammenhang mit der Verwertung der auf Vorrat gespeicherten Daten durch die Strafverfolgungsbehörden sind heute in der StPO nicht spezifisch geregelt, weshalb eine Sonderbestimmung für diesen praxisrelevanten Fall geschaffen werden soll. Dabei war zu berücksichtigen, dass es sich bei der Verwertung der auf Vorrat gespeicherten Daten weder um einen Fall der Beschlagahme nach §§ 96 ff. StPO noch um einen Fall der Überwachung einer elektronischen Kommunikation nach §§ 103 f. StPO handelt. Dies insbesondere deshalb, weil auf Vorrat gespeicherte Daten nie Inhaltsdaten umfassen.

Im Übrigen soll die gegenständliche Gesetzesrevision zum Anlass genommen werden, die aufgrund der geänderten Rahmenbedingungen im Bereich der Funkanlagen sowie des Roaming und der Netzneutralität notwendigen Anpassungen vorzunehmen. Die Bestimmungen im Zusammenhang mit Funkanlagen sind neu abschliessend im Gesetz über die Verkehrsfähigkeit von Waren in Verbindung mit der neu zu schaffenden Modulverordnung zu regeln, was die Aufhebung der Art. 1 Abs. 3 Bst. g, Art. 35 bis 38, Art. 56 Abs. 1 Bst. n, Art. 60 Abs. 1 Bst. b Ziff. 8 sowie Art. 70 Abs. 2 Bst. f und g KomG bedingt, während die Bestimmungen betreffend Roaming und Netzneutralität aufgrund der jüngsten Novelle der Verordnung (EU) 2015/2120 in Art. 1 Abs. 4, Art. 3 Abs. 1 Ziff. 69 und 70, Art. 56 Abs. 1 Bst. s, Art. 70 Abs. 2 Bst. v, v bis, v ter und v quater KomG geregelt werden sollen.

4.2 Abänderung des KomG

Zu Art. 1 Abs. 3 Bst. g, i und Abs. 4

Mit seinem Urteil vom 8. April 2014 in der Rechtssache C-293/12 erklärte der Gerichtshof der Europäischen Union (EuGH) die Richtlinie über die Vorratsspeicherung von Daten (2006/24/EG) für ungültig. Der Verweis auf diese Richtlinie in Art. 1 Abs. 3 Bst. i) KomG ist daher aufzuheben.

Am 29. April 2016 hat der Gemeinsame EWR–Ausschuss beschlossen, die Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG in das EWR-Abkommen zu übernehmen (Beschluss des Gemeinsamen EWR-Ausschusses Nr. 89/2016). Diese Richtlinie wird mittels Verweisteknik durch das Gesetz vom 22. März 1995 über die Verkehrsfähigkeit von Waren (LR 947.1) umgesetzt. Zu diesem Gesetz wird eine neue Modulverordnung über den Verkehr mit Funkanlagen im Europäischen Wirtschaftsraum erstellt. Ausserdem wird die Verordnung vom 3. April 2007 über Funkanlagen und Kommunikations-einrichtungen (LR 784.101.9), die der Umsetzung u.a. der Richtlinie 1999/5/EC dient, überarbeitet. Der Verweis in Art. 1 Abs. 3 Bst. g) KomG ist daher aufzuheben.

Absatz 4 betrifft die Abänderung in Bezug auf die neue Verordnung (EU) 2015/2120 des Europäischen Parlaments und des Rates vom 25. November 2015 über Massnahmen zum Zugang zum offenen Internet und zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten sowie der Verordnung (EU) Nr. 531/2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union. Am 29. April 2016 hat der Gemeinsame EWR–Ausschuss beschlossen, die Verordnung (EU) 2015/2120 in das EWR-Abkommen zu übernehmen (Beschluss des Gemeinsamen EWR-Ausschusses Nr. 92/2016).

Zu Art. 3 Abs. 1 Ziff. 39, 40, 69 und 70

Art. 3 Abs. 1 Ziff. 39 und 40 KomG sind aufgrund der Neuordnung im Bereich der Funkanlagen aufzuheben.

Die neuen Legaldefinitionen zu „Roaminganbieter“ und „Inländischer Anbieter“ ergeben sich aus der neuen Roaming Verordnung.

Zu Art. 35 bis 38

Die Art. 35 bis 38 KomG betreffen die alte „RTTE-Richtlinie“ 1999/5/EG, die durch die Richtlinie 2014/53/EU aufgehoben wurde. Die neue Richtlinie soll nun mittels Verweisteknik durch das Gesetz vom 22. März 1995 über die Verkehrsfähigkeit von Waren umgesetzt werden. Zu diesem Gesetz wird eine neue Modulverordnung über den Verkehr mit Funkanlagen im Europäischen Wirtschaftsraum erstellt. Die materiellrechtlichen Bestimmungen sollen neu ausschliesslich im Gesetz über die Verkehrsfähigkeit von Waren respektive in der neu zu schaffenden Modulverordnung geregelt werden. Art. 35 bis 38 KomG sind daher aufzuheben.

Zu Art. 44 Abs. 4

Der Verweis auf die vom EuGH für ungültig erklärte Richtlinie 2006/24/EG betreffend die Vorratsdatenspeicherung ist aufzuheben.

Zu Überschrift vor Art. 52

Mit der Revision der Bestimmungen über die Speicherung von Daten auf Vorrat wurde eine klare Trennung der betreffenden Bestimmungen von weiteren Bestimmungen – wie jener der Überwachung – angestrebt. Derzeit sind die Bestimmungen über die Speicherung von Daten auf Vorrat unter dem Unterabschnitt „Mitwirkung bei einer Überwachung“ eingeordnet. Diese Einordnung ist insofern unrichtig, als die Speicherung von Daten auf Vorrat keine „Überwachung“ darstellt. Die Speicherung von Daten auf Vorrat stellt lediglich ein Verbot dar, Daten vor einem bestimmten Zeitpunkt zu löschen und eine Verpflichtung, den Strafverfolgungsbehörden diese Daten auf Verlangen auszufolgen. Unter „Überwachung“ wird hingegen das Ab- bzw. Mithören des Inhalts einer Kommunikation verstanden (z.B. durch eine Fangschaltung). Die Überschrift war daher missverständlich und kann entfallen. Um die Übersicht weiterhin zu gewährleisten wurden die Sachtitel der folgenden Artikel neu gefasst.

Zu Art. 52 Sachtitel, Abs. 1 Bst. c, Abs. 4 Bst. b

Art. 52 wurde derart angepasst, dass er nur noch Bestimmungen über die inhaltliche Überwachung enthält. Die Sachüberschrift von Art. 52 wurde deshalb in „Mitwirkung bei einer Überwachung“ abgeändert.

Die in Art. 52 Abs. 1 Bst. c enthaltene Verpflichtung betreffend die Speicherung von Daten auf Vorrat hat keinen Bezug zu der in Art. 52 geregelten Überwachung und ist deshalb aufzuheben. Die Verpflichtung erlischt jedoch nicht, sondern ergibt sich weiterhin aus Art. 52a Abs. 1.

Art. 52 Abs. 4 Bst. b soll ausserdem eine sprachliche Anpassung an die Bestimmungen des Datenschutzgesetzes (DSG)⁷ erfahren. Art. 4 Abs. 1 DSG hält fest, dass Personendaten „nur rechtmässig bearbeitet werden“ dürfen. Konsequenterweise soll in dieser Bestimmung anstelle von „unbefugt“ der Begriff „unrechtmässig“ verwendet werden.

Zu Art. 52a

Aufgrund der systematischen Trennung der Bestimmungen zur Speicherung von Daten auf Vorrat von denjenigen zur Überwachung ist die bisherige Formulierung in Abs. 1 „zum Zwecke der Mitwirkung bei einer Überwachung“ hinfällig und wird durch einen Verweis auf den neu einzuführenden § 98b StPO ersetzt.

Auf Vorrat gespeicherte Daten sollen künftig nur noch zum Zwecke der Aufklärung eines Verbrechens oder eines Vergehens gemäss Katalog in § 98b StPO gespeichert werden. Weiterhin wird neu ausdrücklich festgehalten, dass die Verwendung von auf Vorrat gespeicherten Daten über diesen Zweck hinaus unzulässig ist. Damit wird eine klar definierte Abgrenzung und Einschränkung der Ver-

⁷ Datenschutzgesetz (DSG) vom 14. März 2002, LGBl. 2002 Nr. 55.

wendung der auf Vorrat gespeicherten Daten im Strafverfahren nach der StPO geschaffen.

An der bisher schon geltenden sechsmonatigen Frist, binnen welcher die auf Vorrat gespeicherten Daten nicht gelöscht werden dürfen, sondern für die Strafverfolgungsbehörden vorgehalten werden müssen, wurde unverändert festgehalten. Hierzu ist anzumerken, dass seitens der Strafverfolgungsbehörden durchaus ein Interesse an einer längeren Frist – z.B. von zwölf Monaten – besteht. Dies mit durchaus nachvollziehbaren Begründungen. So kann sich z.B. insbesondere in Fällen von eingehenden Rechtshilfeersuchen, auf Grund der zeitraubenden Übermittlung der Ersuchen im diplomatischen Weg, eine sechsmonatige Frist als zu knapp erweisen und die gewünschten Daten drohen im Zeitablauf des ausländischen Verfahrens einschliesslich des Rechtshilfeweges bereits der Löschung anheim zu fallen. Umgekehrt ist zu erwähnen, dass die Datenschutzstelle eine eher kürzere Frist bevorzugen würde. Auch dies mit durchaus nachvollziehbaren Argumenten. Ist doch z.B. bei einer kürzeren Vorhaltung der auf Vorrat gespeicherten Daten das Risiko einer potentiellen Verletzung der relevanten Grundrechte entsprechend geringer. Nach Abwägung dieser Interessen erschien das Verbleiben bei einer Frist von sechs Monaten als idealer Kompromiss. Auch bewegt sich Liechtenstein damit im internationalen Vergleich auf demselben Niveau. So war z.B. in der Schweiz im Rahmen der aktuellen Totalrevision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)⁸, zunächst eine Ausweitung der Speicherfrist von sechs auf zwölf Monate angedacht. In den parlamentarischen Beratungen wurde diese Frist im verabschiedeten Gesetzeswortlaut⁹ dann jedoch auf sechs Monate reduziert.

⁸ Botschaft zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BBl 2013 2683) und Entwurf (BBl 2013 2789).

⁹ Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), (BBl 2016 1991, Referendumsvorlage, Ablauf der Referendumsfrist: 7. Juli 2016).

Die bisher schon normierte Verpflichtung zur Löschung der auf Vorrat gespeicherten Daten nach Ablauf der Vorhaltefrist wurde um den Zusatz „binnen sieben Tagen“ ergänzt. Dadurch wird dem Umstand Rechnung getragen, dass die Bereinigung der Daten um den zu löschenden Teil aus technischer Sicht nicht in einer logischen Sekunde geschehen kann. Mit der Einführung eines Zeitraums wird den Anbietern und Betreibern ein angemessener Zeitspanne und die notwendige Flexibilität eingeräumt. Im Gegensatz zu einer Formulierung wie „unverzüglich“ – welche Interpretationsspielraum offen lässt – wird so ein klarer Termin geschaffen, welcher für die Anbieter Rechtssicherheit schafft.

Auch in Abs. 2 wird die Speicherung von Daten auf Vorrat mit einer Überwachung in Verbindung gebracht, was zu korrigieren ist. Die Bestimmung wurde neu gefasst und regelt nunmehr ausschliesslich auf Vorrat gespeicherte Daten. Die Bekanntgabe von auf Vorrat gespeicherten Daten an die Strafverfolgungsbehörden stellt eine Datenbekanntgabe im Sinne des Datenschutzgesetzes dar. Die Neufassung orientiert sich an den Begrifflichkeiten des Datenschutzgesetzes. Die Bekanntgabe hat unverzüglich, also alsbald, ohne schuldhaftes Zögern, zu erfolgen. Die Bekanntgabe erfolgt durch einen Datenträger, welcher zum Behörden- bzw. Gerichtsakt genommen wird.

Aufgrund der systematischen Trennung gilt Art. 52 Abs. 4 Bst. c KomG nunmehr nur noch für die (inhaltliche) Überwachung der elektronischen Kommunikation. Eine Entschädigung für die Bekanntgabe der Vorratsdaten soll aber weiterhin bestehen. Daher ist in Absatz 3 eine Entschädigungsregelung auch für die Bekanntgabe der Vorratsdatenspeicherung aufzunehmen. Der bisherige Regelungsinhalt des Abs. 3 (Datenschutzbestimmungen) wurde in den Art. 52b überführt.

In Abs. 4 wird der Bezug auf die für ungültig erklärte Richtlinie gestrichen.

Zu Art. 52b

Der bisherige Art. 52b normiert die „Kontrolle des Datenschutzes“. Die Datenschutzstelle wird als Kontrollinstanz bezeichnet, den Anbietern eine Verpflichtungen zur Protokollierung auferlegt und damit für die Kontrollinstanz ein Kontrollinstrument bereitgestellt.

Im Hinblick auf die Urteilsbegründung des EuGH zur Speicherung von Daten auf Vorrat sollen in Art. 52b ein umfangreicher Katalog konkreter Pflichten der Anbieter eingeführt werden, um die von der Speicherung von Daten auf Vorrat betroffenen Personen wirksam und angemessen vor datenschutzrechtlichen Verstößen zu schützen. Der EuGH stellte in diesem Sinne in seinem Urteil fest, dass die Richtlinie 2006/24/EG keine hinreichenden Garantien dafür biete, dass die Daten wirksam vor Missbrauchsrisiken sowie jedem unberechtigten Zugang und jeder unberechtigten Nutzung geschützt seien. Der Gerichtshof rügte ausserdem explizit, dass die Richtlinie keine Speicherung der Daten im Unionsgebiet vorschreibe. Sie gewährleiste damit nicht in vollem Umfang, dass die Einhaltung der Erfordernisse des Datenschutzes und der Datensicherheit durch eine unabhängige Stelle überwacht wird.

Da Art. 52b Ergänzungen betreffend den Datenschutz erfahren soll, wird die Sachüberschrift des Artikels neu auf „Datenschutz und Kontrolle des Datenschutzes“ angepasst.

Der bisherige Art. 52a Abs. 3 wurde als Abs. 1 in diese Bestimmung überführt und angepasst. Dadurch wird eine Regelung des Datenschutzes an einem einheitlichen Ort erreicht.

Der von den Anbietern zu gewährleistende Datenschutz hat in Bezug auf die durch die Speicherung von Daten entstehenden Eingriff in die Grundrechte und des daraus erwachsenden potentiellen Schadens grundsätzlich angemessen zu

sein. Dem hohen Grundrechtseingriff und dem potentiell hohen Schaden aus einer Datenschutzverletzung haben also entsprechend umfangreiche und starke Massnahmen zur Vermeidung solcher Schäden entgegenzustehen. Die Angemessenheit einer Massnahme leitet sich also vor allem vom konkreten Schutzbedarf der bearbeiteten Daten ab. Zu diesem Zweck werden die wichtigsten Anforderungen in einem nicht abschliessenden Katalog in das Gesetz aufgenommen:

Es ist ein besonders sicheres Verschlüsselungsverfahren einzusetzen. Die Formulierung bringt zum Ausdruck, dass die gehandhabten Daten – also z.B. die auf Vorrat gespeicherten Daten, wie auch die daraus an die Strafverfolgungsbehörden auf einem Datenträger bekanntgegebenen Daten – mit einer Verschlüsselung zu versehen sind, welche der Bedeutung der Daten und dem Sicherheitsrisiko Rechnung trägt. An die Verschlüsselung werden daher höchste Ansprüche zu stellen sein. Unter dem Begriff des besonders sicheren Verschlüsselungsverfahrens ist nicht alleinig das Verschlüsselungsverfahren im engeren Sinn zu verstehen (wie bspw. der eingesetzte Algorithmus oder die Schlüssellänge), sondern es wird darunter vielmehr das gesamte Verfahren der Verschlüsselung der Daten im weitesten Sinn erfasst. Dazu gehört z.B. ebenso das Schlüsselmanagement.

Die auf Vorrat gespeicherten Daten sind auf speziellen, nur dafür verwendeten und von der restlichen Infrastruktur getrennten Speichereinrichtungen zu bearbeiten. Diese Trennung vermindert das Risiko von Manipulationen und fördert die Zugriffskontrolle.

Soweit eine Vernetzung der Speichereinrichtung über das Internet überhaupt notwendig ist – ist eine solche nicht notwendig, hat sie zu unterbleiben – hat eine solche Vernetzung einen hohen Schutz vor dem Zugriff aus dem Internet zu gewährleisten.

Der Zutritt zu den Speichereinrichtungen ist grundsätzlich zu beschränken. Die Anbieter haben sicherzustellen, dass nur wenige, von ihnen speziell ermächtigte Personen Zutritt haben. Die Anbieter sind im Rahmen der Ermächtigung jener Personen auch für deren angemessene Instruktion verantwortlich.

Die Speichereinrichtung ist im Inland zu installieren. Dem Inland gleichgestellt sind die EWR-Mitgliedstaaten und die Schweiz. Die Gleichstellung resultiert aus dem Diskriminierungsverbot und der Gleichwertigkeit des Datenschutzes.

Der Zugriff auf die auf Vorrat gespeicherten Daten hat nach dem Vieraugenprinzip durch mindestens zwei Personen gleichzeitig zu erfolgen. Beide Personen müssen über die besondere Ermächtigung des Anbieters verfügen. Dadurch können nicht nur Fehler vermieden sondern kann auch böswilligen Manipulationen entgegengewirkt werden.

Die bei der Speicherung von Daten auf Vorrat oder Daten aus der Überwachung einzuhaltenden Sicherheitsstandards, Rechte und Pflichten müssen vom Gesetzgeber vorgegeben werden; die technische Konkretisierung kann dagegen der Regelung auf Verordnungsebene vorbehalten bleiben, weshalb in Absatz 4 eine Verordnungsermächtigung eingeführt werden soll. Vorbild für eine solche Verordnung kann die österreichische Datensicherheitsverordnung¹⁰ sein.

In Absatz 2 wird die bereits bestehende Bestimmung über die Protokollierungspflicht präzisiert. Die Protokolldaten dienen einerseits der Datenschutzstelle als Kontrollinstrument und andererseits dem Anbieter als internes Instrument zur Sicherstellung der Datensicherheit. Der Inhalt des Protokolls hat neu den Zeitpunkt, die bearbeitenden Personen und Zweck und Art der Bearbeitung zu umfassen. Der Begriff „Personen“ ist dabei weit auszulegen. Er umfasst nicht nur

¹⁰Verordnung der Bundesministerin für Verkehr, Innovation und Technologie betreffend die Datensicherheit (Datensicherheitsverordnung TKG-DSVO, BGBl. II Nr. 402/2011.

natürliche Personen, sondern auch automatisierte technische Prozesse. In solchen Fällen ist sowohl der technische Prozess (die Bezeichnung des Programms) als auch jene Person zu protokollieren, welcher die Verantwortlichkeit für diesen zukommt.

In Absatz 3 wird neu eine Pflicht zur Zertifizierung eingeführt. Anbieter haben ihre Datenbearbeitungen zu zertifizieren. Diese Verpflichtung führt dazu, dass die Datenbearbeitungen für den Zertifizierungsvorgang gründlich durchdacht und ausführlich dokumentiert werden müssen, damit die Zertifizierung ursprünglich erreicht und anschliessend auch weiterhin eingehalten werden kann. Dies bewirkt erfahrungsgemäss eine Steigerung der Qualität des Datenschutzes beim Anbieter, was dem notwendigen hohen Niveau zuträglich ist. In diesem Zusammenhang ist auf die am 1. Februar 2014 in Kraft getretene Verordnung über die Datenschutzzertifizierungen (VDSZ), welche unter anderem Vorschriften über die Akkreditierung und des Zertifizierungsverfahrens enthält, zu verweisen.

In Absatz 4 werden Informationspflichten rund um die Zertifizierung normiert. Diese verschaffen der Datenschutzstelle den nötigen Überblick über den Stand der Zertifizierungen und fördern ihre Kontrolltätigkeit.

Absatz 5 entspricht dem bisherigen Absatz 1. Da die Bestimmungen über den Datenschutz sowohl Anwendung auf die Überwachung wie auch die Speicherung von Daten auf Vorrat finden, war die Bestimmung entsprechend anzupassen. Die Bestimmung wurde neu nach den nunmehrigen Absätzen 1 bis 4 eingereiht, deren Einhaltung durch die Datenschutzstelle zu kontrollieren ist. Mit der Datenschutzstelle steht eine unabhängige Stelle zur Verfügung, bei welcher die Handhabung des Datenschutzes durch die Anbieter oder Strafverfolgungsbehörden gerügt werden kann, soweit die Handhabung nicht im Strafprozess einem Rechtsmittel zugänglich ist.

Zu Art. 52c

Mit dem neu eingeführten Art. 52c wird ein Instrument eingeführt, mit welchem die Anwendung der auf Vorrat gespeicherten Daten durch die Strafverfolgungsbehörden einer Analyse zugänglich gemacht werden können. Da die Speicherung von Daten auf Vorrat anerkanntermassen einen grossen Eingriff in die Grundrechte darstellt, erscheint es als notwendig über ein Instrument zur Sichtbarmachung der Eingriffe zu verfügen.

Die Bestimmung sieht vor, dass der Gebrauch von auf Vorrat gespeicherten Daten zu erheben und auszuwerten ist. Damit wird sowohl den Strafverfolgungsbehörden, den Aufsichtsbehörden wie auch der Legislative ein Instrument in die Hand gegeben um die Auswirkungen des Grundrechtseingriffs zu erfassen und nötigenfalls Änderungen vorzuschlagen.

Zu Art. 53 Abs. 2 und 3

Art. 53 regelt die Aufzeichnung von und Auskunft über Teilnehmerdaten. Teilnehmerdaten sind gemäss Legaldefinition des Art. 1 Abs. 1 Ziff. 48 KomG „alle personenbezogenen Daten, die für die Begründung, Abwicklung, Änderung oder Beendigung der vertraglichen Beziehung zwischen dem Nutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind, insbesondere Name oder Firma und Zustelladresse des Teilnehmers sowie entsprechende Identifikationsmittel“. Sie sind zwar auch Teil der Vorratsdaten, haben darüber hinaus allerdings auch eine eigenständige Funktion und dienen insbesondere dazu, die Ermittlungen überhaupt erst in Gang zu bringen. Da die Eingriffsintensität im Gegensatz zur Gesamtheit der Vorratsdaten (Verkehrs-, Standort- und Teilnehmerdaten) geringer ist, sind auch an die Voraussetzungen im Hinblick auf die Herausgabe im strafrechtlichen Sinn geringere Anforderungen zu stellen.

Aufgrund der immer wiederkehrenden Diskussionen um Absatz 2 soll allerdings dieser Artikel eine Klarstellung erfahren. Die heutige Formulierung des Absatzes 2 ist sehr offen und es besteht ausserdem eine Diskrepanz zwischen der Anordnung des Untersuchungsrichters und dem schriftlichen Ersuchen der Landespolizei. Tatsächlich geht es in der Praxis insbesondere um die Fälle, bei denen die Polizei über eine IP-Adresse die Identität einer Person für weitere Ermittlungen (z.B. Hausdurchsuchungen) feststellen will. Künftig sollen daher Diensteanbieter hinsichtlich der aufgezeichneten Teilnehmerdaten im Sinne des Art. 3 Abs. 1 Ziff. 48 KomG verpflichtet sein, der Landespolizei über deren schriftliches Ersuchen unverzüglich Auskunft zu erteilen.

Die Entschädigungsregelung in Art. 53 Abs. 3 KomG soll aufgehoben werden. Zum einen handelt es sich dabei lediglich um eine Auskunftserteilung von Teilnehmerdaten, die ohne grossen Aufwand betrieben werden kann, da es sich lediglich um jene personenbezogene Daten handelt, die für die Begründung, Abwicklung, Änderung oder Beendigung der vertragliche Beziehung zwischen Nutzer und Anbieter anfallen. Zum anderen hat der Vergleich mit der Schweiz gezeigt, dass dieser Dienst auch dort nur eine Entschädigung von lediglich vier Franken (inklusive Mehrwertsteuer) zur Folge hat (Art. 2 Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehr). Der Aufwand der Gebührenerhebung stünde damit ausser Verhältnis zu den Einnahmen.

Zu Art. 56 Abs. 1 Bst. n) und s)

Neu sollen die materiellrechtlichen Bestimmungen betreffend die Aufsicht über das Inverkehrbringen, die Inbetriebnahme und den Betrieb von Geräten nach Kapitel IX im Gesetz über die Verkehrsfähigkeit von Waren respektive in der neu zu schaffenden Modulverordnung geregelt werden. Art. 56 Abs. 1 Bst. n) KomG ist daher aufzuheben.

Art. 56 Abs. 1 Bst. s) KomG betrifft die neuen Zuständigkeiten der Regulierungsbehörde im Zusammenhang mit der Sicherstellung des Zugangs zu einem offenen Internet (Netzneutralität), die sich aus Art. 3, 4 und 5 der Verordnung (EU) 2015/2120 ergeben.

Zu Art. 60 Abs. 1 Bst. b Ziff. 8

Auch die Erhebung von Gebühren im Bereich der Funkanlagen wird neu ausschliesslich im Gesetz über die Verkehrsfähigkeit von Waren respektive in der neu zu schaffenden Modulverordnung geregelt werden. Art. 60 Abs. 1 Bst. b) Ziff. 8 KomG ist daher aufzuheben.

Zu Art. 70 Abs. 2 Bst. f, g, u, u bis, v, v bis, v ter und v quater

In Art. 70 Abs. 2 sollen zum einen neue Sanktionsbestimmungen aufgrund der neu eingeführten Datensicherheitsbestimmungen zum anderen aufgrund der neuen Verordnung (EU) 2015/2120 des Europäischen Parlaments und des Rates vom 25. November 2015 über Massnahmen zum Zugang zum offenen Internet und zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten sowie der Verordnung (EU) Nr. 531/2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union aufgenommen werden.

Art. 70 Abs. 2 Bst. f und g KomG sind aufgrund der Neuordnung im Bereich der Funkanlagen aufzuheben.

Übergangs- und Schlussbestimmungen

Mit einer angemessenen Übergangsfrist von 2 Jahren soll den Anbietern im Sinne des KomG genügend Zeit gegeben werden, eine Zertifizierung nach Art. 52b Abs. 3 KomG nachzukommen.

4.3 Abänderung der StPO

Zu § 98b StPO

Durch die Einführung eines neuen Paragraphen soll dem Umstand Rechnung getragen werden, dass es sich bei der Verwertung von Vorratsdaten um eine spezifische Form einer strafgerichtlichen Zwangsmassnahme handelt, die weder als inhaltliche Überwachung nach § 103 StPO noch als Beschlagnahme nach §§ 96 ff. StPO zu qualifizieren ist. Wesentliches Unterscheidungsmerkmal ist insbesondere, dass Vorratsdaten nie Inhaltsdaten umfassen. Aus diesem Grund sowie unter Berücksichtigung des Umstandes, dass die Intensität der Grundrechtseingriffe unterschiedlich ist, bedarf es spezifischer Voraussetzungen und einer besonderen Ermächtigungsgrundlage.

§ 98b stellt nun klar, dass Vorratsdaten den Strafverfolgungsbehörden nur zum Zwecke der Aufklärung der im Gesetz explizit und abschliessend genannten Verbrechen oder Vergehen bekannt gegeben werden dürfen. Und dies auch nur, wenn der Betroffene selbst verdächtig ist oder seine Zustimmung schriftlich erteilt. Im letztgenannten Fall ist der Betroffene vorher entsprechend zu belehren, und zwar insbesondere dahingehend, dass die Verwertung seiner Vorratsdaten auch zu einem Zufallsfund führen kann, der seinerseits eine Strafverfolgung nach sich ziehen kann.

Hinsichtlich des Straftatenkatalogs soll allerdings nicht nur das Strafmass und damit die Schwere der Tat Berücksichtigung finden, sondern auch die Erfolgsaussichten der Aufklärung. So gibt es Straftaten, die aufgrund ihrer Charakteristik ohne die erforderlichen Vorratsdaten nicht aufzuklären sind, beispielsweise Stalking oder die definitionsgemäss mit elektronischer Kommunikation verbundenen Delikte. Selbst wenn bei solchen Straftaten allenfalls nur eine geringe Strafan drohung vorliegt, so würde eine Verweigerung des Zugriffs auf Vorratsdaten bei

der Verfolgung solcher Delikte geradezu zu einer unverhältnismässigen Erschwerung der Strafverfolgung führen. In diesen Fällen ist daher das öffentliche Interesse an der Aufklärung höher zu gewichten, als die Höhe der Strafandrohung. Es ist somit eine Ausnahme von der Regel vorzusehen, wonach die Verwertung von Vorratsdaten nur bei schweren Straftaten zulässig sein soll.

Weiterhin ist darauf hinzuweisen, dass die Verwertung von auf Vorrat gespeicherten Daten durch die allgemeinen Datenschutzprinzipien beschränkt ist. So haben sich die Strafverfolgungsbehörden beim Zugriff auf die Vorratsdaten auf jene Daten zu beschränken, welche zur Aufklärung der Tat auch wirklich notwendig sind.

Zu § 108 Abs. 3 StPO

Durch den Einschub „Verwertung von Vorratsdaten“ soll klargestellt werden, dass das Umgehungsverbot auch und gerade im Zusammenhang mit § 98b StPO zu beachten ist. Dadurch ist für Berufsgeheimnisträger dasselbe Schutzniveau gewährleistet, wie heute bereits bei anderen strafgerichtlichen Zwangsmassnahmen, wie beispielsweise der Beschlagnahme von Unterlagen.

5. VERFASSUNGSMÄSSIGKEIT / RECHTLICHES

Die geltenden Bestimmungen und die heutige Praxis der Speicherung und Verwertung von Vorratsdaten waren bislang noch nicht Gegenstand einer Normenkontrolle durch den StGH. Vor diesem Hintergrund wurde die gegenständliche Gesetzesrevision weitgehend an den Implikationen der einschlägigen Rechtsprechung des EuGH (Urteil vom 8. April 2014 in der Rechtssache C-293/12) ausgerichtet. Dementsprechend ist davon auszugehen, dass sowohl die EWR-rechtlichen als auch die verfassungsrechtlichen Vorgaben erfüllt werden.

6. REGIERUNGSVORLAGEN

6.1 Kommunikationsgesetz

Gesetz

vom ...

über die Abänderung des Kommunikationsgesetzes

Dem nachstehenden vom Landtag gefassten Beschluss erteile Ich Meine Zustimmung:

I.

Abänderung bisherigen Rechts

Das Gesetz vom 17. März 2006 über die elektronische Kommunikation (Kommunikationsgesetz; KomG), LGBl. 2006 Nr. 91, in der geltenden Fassung, wird wie folgt abgeändert:

Art. 1 Abs. 3 Bst. g), i) und Abs. 4

3) Dieses Gesetz dient der Umsetzung folgender EWR-Rechtsvorschriften:

g) Aufgehoben

i) Aufgehoben

4) Es enthält zudem die notwendigen Bestimmungen zur Durchführung der:

a) Verordnung (EU) Nr. 531/2012 des Europäischen Parlaments und des Rates vom 13. Juni 2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union in der Fassung der Verordnung (EU) 2015/2120 des Europäischen Parlaments und des Rates vom 25. November 2015 ("Roamingverordnung"; EWR-Rechtssammlung: Anh. XI - 5cu.01);

b) Verordnung (EU) 2015/2120 des Europäischen Parlaments und des Rates vom 25. November 2015 über Massnahmen zum Zugang zum offenen Internet und zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten sowie der Verordnung (EU) Nr. 531/2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union (EWR-Rechtssammlung: Anh. XI - 5cu.01).

Art. 3 Abs. 1 Ziff. 39, 40, 69 und 70

1) Im Sinne dieses Gesetzes bedeutet:

39. Aufgehoben;

40. Aufgehoben;

69. „Roaminganbieter“: ein Unternehmen, das für einen Roamingkunden regulierte Endkunden-Roamingdienste bereitstellt;

70. „Inländischer Anbieter“: ein Unternehmen, das für einen Roamingkunden inländische Mobilfunkdienste bereitstellt.

Art. 35 bis 38

Aufgehoben

Art. 44 Abs. 4

4) Das Nähere über die Offenlegung von Informationen und ihrer Verwendung, insbesondere im Rahmen der Zusammenarbeit der Regulierungsbehörde mit anderen nationalen Regulierungsbehörden und mit der EFTA-Überwachungsbehörde, regelt die Regierung in Übereinstimmung mit Art. 5 der Rahmenrichtlinie und Art. 10 und 11 der Genehmigungsrichtlinie mit Verordnung.

Überschrift vor Art. 52

Aufgehoben

Art. 52 Sachtitel, Abs. 1 Bst. c, Abs. 4 Bst. b

Mitwirkung bei einer Überwachung

1) Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste und Betreiber eines öffentlichen Kommunikationsnetzes sind verpflichtet:

c) Aufgehoben

4) Die Regierung regelt mit Verordnung das Nähere, insbesondere über:

b) den Schutz der übermittelten Daten gegen die unrechtmässige Kenntnisnahme durch Dritte;

Art. 52a

Vorratsdatenspeicherung

1) Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste und Betreiber eines öffentlichen Kommunikationsnetzes haben Vorratsdaten, soweit diese im Zuge der Bereitstellung des Kommunikationsdienstes erzeugt oder verarbeitet werden, für einen Zeitraum von sechs Monaten ab dem Zeitpunkt der Beendigung des Kommunikationsvorganges zum Zwecke der Aufklärung eines Verbrechens oder eines Vergehens gemäss § 98b StPO zu speichern. Für andere Zwecke dürfen die gespeicherten Daten nicht verwendet werden. Diese Daten sind nach Ablauf dieser Frist, unbeschadet des Art. 49 Abs. 2, binnen sieben Tagen zu löschen.

2) Vorratsdaten sind so zu speichern, dass sie auf einem Datenträger unverzüglich an die Strafverfolgungsbehörden bekannt gegeben werden können.

3) Anbieter haben für die Bekanntgabe von Vorratsdaten nach Abs. 2 erbrachten Leistungen Anspruch auf eine angemessene Entschädigung.

4) Das Nähere über die Vorratsdatenspeicherung, insbesondere die zu speichernden Datenkategorien, sowie die Bekanntgabe von Vorratsdaten, regelt die Regierung mit Verordnung.

Art. 52b

Datenschutz und Kontrolle des Datenschutzes

1) Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste und Betreiber eines öffentlichen Kommunikationsnetzes haben sicherzustellen, dass Vorratsdaten durch technische und organisatorische Massnahmen in einer Weise bearbeitet werden, die eine angemessene Sicherheit der personenbezo-

genen Daten gewährleistet, einschliesslich Schutz vor unrechtmässiger Bearbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung geschützt werden. Die Massnahmen umfassen insbesondere:

- a) den Einsatz eines besonders sicheren Verschlüsselungsverfahrens;
- b) die Speicherung in gesonderten, von den für die üblichen betrieblichen Aufgaben getrennten Speichereinrichtungen;
- c) die Speicherung mit einem hohen Schutz vor dem Zugriff aus dem Internet;
- d) die Beschränkung des Zutritts zu den Datenbearbeitungsanlagen auf Personen, die durch den Anbieter besonders ermächtigt sind;
- e) die Speicherung im Inland, wobei die EWR-Mitgliedstaaten und die Schweiz dem Inland gleichgestellt sind und
- f) die notwendige Mitwirkung von mindestens zwei Personen beim Zugriff auf die Daten, die dazu durch den Anbieter besonders ermächtigt worden sind.

2) Anbieter haben sicherzustellen, dass für Zwecke der Datenschutzkontrolle jede Bearbeitung von Daten nach Art. 52 und 52a, protokolliert wird. Die Protokolldaten sind der Datenschutzstelle auf Ersuchen unverzüglich mitzuteilen. Protokolldaten dürfen ausschliesslich für die Zwecke der Kontrolle des Datenschutzes durch die Datenschutzstelle und zur Gewährleistung der Datensicherheit verwendet werden. Für andere Zwecke dürfen die Protokolldaten nicht verwendet werden. Die Protokolldaten sind nach einem Jahr zu löschen. Zu protokollieren sind:

- a) der Zeitpunkt der Bearbeitung,
- b) die die Daten bearbeitenden Personen und

c) Zweck und Art der Bearbeitung.

3) Anbieter müssen hinsichtlich der Datenbearbeitung nach Art. 52 und 52a nach Art. 14a des Datenschutzgesetzes zertifiziert sein oder ein von der Datenschutzstelle als gleichwertig anerkanntes Zertifikat vorweisen können.

4) Die Anbieter informieren die Datenschutzstelle nach Art. 28 des Datenschutzgesetzes unaufgefordert über die Zertifizierung oder Rezertifizierung hinsichtlich der Datenbearbeitung nach Art. 52 und 52a. Die Datenschutzstelle kann vom Anbieter oder von der Zertifizierungsstelle jederzeit die für die Zertifizierung oder Rezertifizierung relevanten Dokumente einfordern.

5) Die Datenschutzstelle kontrolliert die Anwendung der Bestimmungen betreffend Datenschutz in Bezug auf Daten, die nach Art. 52 und 52a bearbeitet werden.

6) Die Regierung regelt das Nähere über den Datenschutz, insbesondere die technischen und organisatorischen Massnahmen und die Kontrolle des Datenschutzes, mit Verordnung.

Art. 52c (neu)

Statistische Erfassung der Erhebung von Vorratsdaten

1) Über die Erhebung von Vorratsdaten nach § 98b StPO haben die Gerichte jährlich eine Statistik zu erstellen. In dieser sind anzugeben:

- a) unterschieden nach der Einteilung der strafbaren Handlungen und nach betroffenen Diensten
 - 1. die Anzahl der Erhebungen insgesamt;
 - 2. die Anzahl der Erhebungen die zu einer Verurteilung führten und

3. die Anzahl der Erhebungen die keiner Verurteilung führten.
 - b) die Anzahl der Erhebungen, die teilweise ergebnislos geblieben sind, weil die abgefragten Daten teilweise nicht verfügbar waren;
 - c) die Anzahl der Erhebungen, die ergebnislos geblieben sind, weil keine Daten verfügbar waren.
- 2) Die Statistik ist im Justizbericht aufzuführen.

Art. 53 Abs. 2 und 3

2) Diensteanbieter sind hinsichtlich der aufgezeichneten Teilnehmerdaten verpflichtet, der Landespolizei über deren schriftliches Ersuchen unverzüglich Auskunft zu erteilen, sofern sie die Daten zur Erfüllung ihrer gesetzlichen Aufgaben unbedingt benötigt.

3) Aufgehoben

Art. 56 Abs. 1 Bst. n und s

1) Der Regulierungsbehörde obliegt die Erfüllung aller regulatorischen Aufgaben, die ihr aufgrund des EWR-Rechts als nationale Regulierungsbehörde im Bereich der elektronischen Kommunikation, insbesondere aufgrund von Art. 7 und 8 der Rahmenrichtlinie, sowie aufgrund dieses Gesetzes übertragen sind. Dazu gehören insbesondere:

- n) Aufgehoben
- s) die Aufsicht und Durchsetzung der Art. 3, 4 und 5 der Verordnung (EU) 2015/2120.

Art. 60 Abs. 1 Bst. b Ziff. 8

1) Die Regulierungsbehörde erhebt Gebühren für:

- b) ihre Tätigkeiten (Verwaltungsgebühren), insbesondere im Zusammenhang mit:

8. Aufgehoben

Art. 70 Abs. 2 Bst. f, g, u, u bis, v, v bis, v ter und v quater

2) Von der Regulierungsbehörde ist wegen Übertretung mit einer Busse bis zu 50 000 Franken zu bestrafen, wer:

- f) Aufgehoben
- g) Aufgehoben
- u) Vorratsdaten entgegen Art. 52a nicht speichert, nicht rechtzeitig löscht oder für andere Zwecke verwendet;
- u bis) die Datenschutzpflichten betreffend die Einhaltung der technischen und organisatorischen Massnahmen, die Protokollierung und Auskunftserteilung oder die Zertifizierung und die zugehörigen Mitteilungen nach Art. 52b verletzt;
- v) als Betreiber gegen Art. 3, 7, 9, 11 oder 12 der Roamingverordnung verstösst;
- v bis) als inländischer Anbieter gegen Art. 4, 5 oder 11, der Roamingverordnung verstösst;
- v ter) als Roaminganbieter gegen Art. 4, 8, 10, 11, 13, 14 oder 15 der Roamingverordnung verstösst;
- v quater) als Anbieter gegen Art. 3, 4 oder 5 der Verordnung (EU) 2015/2120 verstösst.

II.

Übergangs- und Schlussbestimmungen

Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste und Betreiber eines öffentlichen Kommunikationsnetzes haben eine Zertifizierung nach Art. 52b Abs. 3 binnen 2 Jahren ab Inkrafttreten dieses Gesetzes nachzuweisen.

6.2 Strafprozessordnung

Gesetz

vom ...

über die Abänderung der Strafprozessordnung

Dem nachstehenden vom Landtag gefassten Beschluss erteile Ich Meine Zustimmung:

I.

Abänderung bisherigen Rechts

§ 98b StPO

1) Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste und Betreiber eines öffentlichen Kommunikationsnetzes sind, sofern dies zur Aufklärung eines Verbrechens oder eines Vergehens nach den §§ 105, 107a, 118a, 119, 119a, 123, 126a bis 126c, 131a, 168a, 225a, 278, 279 bis 283, 288, 289, 292, 293, 295, 299, 300, 301, 304 bis 308, 310, 311, 319 und 320 StGB, eines Vergehens nach dem 10. Abschnitt des Strafgesetzbuches, eines Vergehens nach den Art. 83 bis 85 des Ausländergesetzes, eines Vergehens nach den Art. 62 bis 65 des Personenfreizügigkeitsgesetzes, einem Vergehen nach dem Betäubungsmittelgesetz oder einem Vergehen nach dem Kommunikationsgesetz erforderlich erscheint, über gerichtlichen Beschluss verpflichtet, Vorratsdaten bekanntzuge-

ben, wenn der betroffene Teilnehmer selbst dringend verdächtig ist, die Straftat begangen zu haben, oder nach entsprechender Belehrung schriftlich einwilligt.

2) Ein Beschluss nach Abs. 1 ist jedenfalls dem Anbieter zuzustellen. Die Zustellung an den betroffenen Teilnehmer oder sonstige Bevollmächtigte kann aufgeschoben werden, solange durch sie der Zweck der Untersuchung gefährdet wäre. Hierüber ist der Anbieter zu informieren, der alle mit der gerichtlichen Anordnung verbundenen Tatsachen und Vorgänge gegenüber dem betroffenen Teilnehmer, Bevollmächtigten und Dritten vorläufig geheim zu halten hat. Diese Geheimhaltungspflicht trifft auch alle Personen, die an der Tätigkeit eines Anbieters mitwirken.

3) Wird die Bekanntgabe von Vorratsdaten durch den Anbieter rechtswidrig verweigert, so kann der Anbieter, falls er nicht selbst der strafbaren Handlung verdächtig erscheint oder von der Verbindlichkeit zur Ablegung des Zeugnisses befreit ist, durch Verhängung einer Beugestrafe bis zu 50 000 Franken dazu angehalten werden.

§ 108 Abs. 3 StPO

3) Das Recht der in Abs. 1 Zi ff. 2 bis 4 angeführten Personen, die Aussage zu verweigern, darf bei sonstiger Nichtigkeit nicht umgangen werden, insbesondere nicht durch Sicherstellung und Beschlagnahme von Unterlagen, Verwertung von Vorratsdaten und auf Datenträgern gespeicherten Informationen, die durch das Betreuungsverhältnis neu geschaffen wurden oder durch Vernehmung der Hilfskräfte oder der Personen, die zur Ausbildung an der berufsmässigen Tätigkeit nach Abs. 1 Zi ff. 2 bis 4 teilnehmen.

II.

Übergangs- und Schlussbestimmungen

Auf im Zeitpunkt des Inkrafttretens dieses Gesetzes hängige Verfahren ist das neue Recht anzuwenden.

III.

Inkrafttreten

Dieses Gesetz tritt unter Vorbehalt des ungenutzten Ablaufs der Referendumsfrist am ... in Kraft, andernfalls am Tage der Kundmachung.