Sammlung der Rechtsprechung

SCHLUSSANTRÄGE DES GENERALANWALTS
ANTHONY COLLINS
vom 8. Juni 2023[1]

Rechtssache C-178/22

Unbekannt,
Beteiligte:
Procura della Repubblica presso il Tribunale di Bolzano

(Vorabentscheidungsersuchen des Tribunale di Bolzano [Landesgericht Bozen, Italien])

„Vorlage zur Vorabentscheidung – Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation – Vertraulichkeit der Kommunikation – Betreiber elektronischer Kommunikationsdienste – Richtlinie 2002/58/EG – Art 1 Abs. 3 und Art. 15 Abs. 1 – Charta der Grundrechte der Europäischen Union – Art. 7, 8,11 und Art. 52 Abs. 1 – Antrag einer Staatsanwaltschaft auf Zugang zu Daten zur Ermittlung und Verfolgung schweren Diebstahls eines Mobiltelefons – Definition einer ‚schweren Straftat', die einen schwerwiegenden Eingriff in Grundrechte rechtfertigen kann – Umfang der vorherigen Kontrolle, mit der gewährleistet werden soll, dass die Voraussetzung der Begehung einer schweren Straftat eingehalten wird – Grundsatz der Verhältnismäßigkeit"

I. Einleitung

1. Die Procura della Repubblica presso il Tribunale di Bolzano (Staatsanwaltschaft beim Landesgericht Bozen, Italien) (im Folgenden: Staatsanwaltschaft [Bozen]) beantragt beim Tribunale di Bolzano (Landesgericht Bozen, Italien) die Genehmigung des Zugangs zu den von den Betreibern elektronischer Kommunikationsdienste nach nationalem Recht aufbewahrten Daten, die es u. a. ermöglichen, die Quelle und den Adressaten einer Mobiltelefonkommunikation zurückzuverfolgen und festzustellen.

2. Im Zusammenhang mit diesem Antrag ersucht das Tribunale di Bolzano (Landesgericht Bozen) den Gerichtshof um die Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58/EG[2]. Diese Bestimmung erlaubt den Mitgliedstaaten, durch Rechtsvorschriften Ausnahmen von der in dieser Richtlinie vorgesehenen Pflicht[3] zur Gewährleistung der Vertraulichkeit der

[1] Originalsprache: Englisch.

[2] Richtlinie 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) (ABl. 2002, L 201, S. 37) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (ABl. 2009, L 337, S. 11) geänderten Fassung.

[3] Vgl. Art. 5 der Richtlinie 2002/58. Der durch Art. 5 Abs. 1 dieser Richtlinie garantierte Schutz der Vertraulichkeit der elektronischen Kommunikation gilt für Maßnahmen sämtlicher anderer Personen als der Nutzer, unabhängig davon, ob sie dem öffentlichen oder dem privaten Sektor angehören. Urteil vom 2. Oktober 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, Rn. 36 und die dort angeführte Rechtsprechung).

elektronischen Kommunikation einzuführen. Im Urteil Prokuratuur[4] hat der Gerichtshof entschieden, dass der durch Maßnahmen gemäß Art. 15 Abs. 1 der Richtlinie 2002/58 erlangte Zugang zu Daten, aus denen genaue Schlüsse auf das Privatleben eines Nutzers gezogen werden können, einen schwerwiegenden Eingriff in die in den Art. 7, 8, 11 und in Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) verankerten Grundrechte und Grundsätze darstellt[5]. Ein solcher Zugang darf nicht zum Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von „Straftaten im Allgemeinen" bewilligt werden. Er darf nur in Verfahren zur Bekämpfung „schwerer Kriminalität"[6] gewährt werden und muss einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde unterliegen, damit die Einhaltung dieser Voraussetzung gewährleistet ist[7]. Das Tribunale di Bolzano (Landesgericht Bozen) bittet den Gerichtshof, zwei Aspekte des Urteils Prokuratuur zu klären: den Begriff der „schweren Kriminalität" und den Umfang der vorherigen Kontrolle, die einem Gericht gemäß einer nationalen Regelung obliegt, wonach es den Zugang zu den von Betreibern elektronischer Kommunikationsdienste gespeicherten Daten zu genehmigen hat.

II. Rechtlicher Rahmen

A. Unionsrecht

3. Art. 5 („Vertraulichkeit der Kommunikation") der Richtlinie 2002/58 bestimmt:

„(1) Die Mitgliedstaaten stellen die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicher. Insbesondere untersagen sie das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer, wenn keine Einwilligung der betroffenen Nutzer vorliegt, es sei denn, dass diese Personen gemäß Artikel 15 Absatz 1 gesetzlich dazu ermächtigt sind. …

…"

4. In Art. 6 („Verkehrsdaten") der Richtlinie 2002/58 heißt es:

„(1) Verkehrsdaten, die sich auf Teilnehmer und Nutzer beziehen und vom Betreiber eines öffentlichen Kommunikationsnetzes oder eines öffentlich zugänglichen Kommunikationsdienstes verarbeitet und gespeichert werden, sind unbeschadet der Absätze 2, 3 und 5 des vorliegenden Artikels und des Artikels 15 Absatz 1 zu löschen oder zu anonymisieren, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden.

…

[4] Urteil vom 2. März 2021, Prokuratuur (Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation) (C-746/18, EU:C:2021:152, im Folgenden: Urteil Prokuratuur).

[5] Unabhängig davon, für welchen Zeitraum der Zugang zu den betreffenden Daten begehrt wird und welche Menge oder Art von Daten für einen solchen Zeitraum verfügbar ist.

[6] Oder zur Verhütung ernster Bedrohungen der öffentlichen Sicherheit. Vgl. Urteil Prokuratuur, Rn. 35, 39 und 45. Vgl. auch Urteile vom 2. Oktober 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, Rn. 56), und vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 140).

[7] Urteil Prokuratuur (Rn. 48 bis 52).

(5) Die Verarbeitung von Verkehrsdaten gemäß den Absätzen 1, 2, 3 und 4 darf nur durch Personen erfolgen, die auf Weisung der Betreiber öffentlicher Kommunikationsnetze und öffentlich zugänglicher Kommunikationsdienste handeln und die für Gebührenabrechnungen oder Verkehrsabwicklung, Kundenanfragen, Betrugsermittlung, die Vermarktung der elektronischen Kommunikationsdienste oder für die Bereitstellung eines Dienstes mit Zusatznutzen zuständig sind; ferner ist sie auf das für diese Tätigkeiten erforderliche Maß zu beschränken.

…“

5. Art. 9 („Andere Standortdaten als Verkehrsdaten“) der Richtlinie 2002/58 sieht vor:

„(1) Können andere Standortdaten als Verkehrsdaten in Bezug auf die Nutzer oder Teilnehmer von öffentlichen Kommunikationsnetzen oder öffentlich zugänglichen Kommunikationsdiensten verarbeitet werden, so dürfen diese Daten nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn die Nutzer oder Teilnehmer ihre Einwilligung gegeben haben. Der Diensteanbieter muss den Nutzern oder Teilnehmern vor Einholung ihrer Einwilligung mitteilen, welche Arten anderer Standortdaten als Verkehrsdaten verarbeitet werden, für welche Zwecke und wie lange das geschieht, und ob die Daten zum Zwecke der Bereitstellung des Dienstes mit Zusatznutzen an einen Dritten weitergegeben werden. Die Nutzer oder Teilnehmer können ihre Einwilligung zur Verarbeitung anderer Standortdaten als Verkehrsdaten jederzeit zurückziehen.

…“

6. Art. 15 Abs. 1 der Richtlinie 2002/58 lautet:

„Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG[8] für die nationale Sicherheit (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. Alle in diesem Absatz genannten Maßnahmen müssen den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen.“

B. Nationales Recht

7. Art. 132 Abs. 3 des Decreto Legislativo 30 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali (gesetzesvertretendes Dekret Nr. 196 zur Einführung eines Gesetzbuchs zum Schutz personenbezogener Daten)[9] in der kürzlich durch Art. 1 des

[8] Richtlinie des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. 1995, L 281, S. 31).

[9] Supplemento ordinario Nr. 123 zur GURI Nr. 174 vom 29. Juli 2003, S. 11.

Decreto-legge 30 settembre 2021 n. 132 – Misure urgenti in materia di giustizia e di difesa, nonché proroghe in tema di referendum, assegno temporaneo e IRAP, convertito con modificazioni nella legge 23 novembre 2021 n. 178 (Gesetzesdekret Nr. 132 vom 30. September 2021[10], mit Änderungen in das Gesetz Nr. 178 vom 23. November 2021 umgewandelt)[11], geänderten Fassung (im Folgenden: Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003) sieht vor:

„(3) Bestehen innerhalb der gesetzlich vorgeschriebenen Aufbewahrungsfrist[, d. h. 24 Monate ab dem Zeitpunkt der Kommunikation,] hinreichende Anhaltspunkte für Straftaten, für die das Gesetz eine lebenslange Freiheitsstrafe oder eine Freiheitsstrafe im Höchstmaß von mindestens drei Jahren vorsieht, die gemäß Art. 4 des Codice di procedura penale [(Strafprozessordnung)] bestimmt wird, oder für Straftaten der Bedrohung, Belästigung oder Störung von Personen per Telefon und handelt es sich um eine ernsthafte Bedrohung, Belästigung oder Störung, so werden die Daten, wenn sie für die Aufklärung des Sachverhalts von Bedeutung sind, auf Antrag der Staatsanwaltschaft oder auf Ersuchen des Verteidigers des Angeklagten, des Beschuldigten, der verletzten Person oder anderer privater Beteiligter erhoben, nachdem der Richter durch mit Gründen versehenen Beschluss die Genehmigung hierzu erteilt hat.

…

(3-*quarter*) Die unter Verstoß gegen die Bestimmungen der Abs. 3 und 3-*bis* erlangten Daten dürfen nicht verwendet werden."

8. Art. 4 („Vorschriften zur Bestimmung der Zuständigkeit") der Strafprozessordnung lautet:

„Zur Bestimmung der Zuständigkeit ist die gesetzlich für jede vollendete oder versuchte Straftat festgelegte Strafe zu berücksichtigen. Nicht zu berücksichtigen ist, ob es sich um eine fortgesetzte Tat oder einen Wiederholungsfall handelt und unter welchen Umständen die Straftat begangen wird, es sei denn, es handelt sich um erschwerende Umstände, für die das Gesetz eine andere Strafe als die Regelstrafe vorsieht, und Umstände mit besonderen Wirkungen."

9. Nach den Angaben des vorlegenden Gerichts kann die Staatsanwaltschaft die Straftat des schweren Diebstahls von Amts wegen verfolgen[12]. Art. 625 des Codice penale (Strafgesetzbuch) sieht für schweren Diebstahl eine Strafe mit besonderer Wirkung vor, nämlich eine Freiheitsstrafe von zwei bis sechs Jahren und eine Geldstrafe von 927 Euro bis 1 500 Euro. Nach Art. 624 des Strafgesetzbuchs ist einfacher Diebstahl, der auf Antrag des Geschädigten verfolgt werden kann, mit einer Freiheitsstrafe von sechs Monaten bis drei Jahren und einer Geldstrafe von 154 Euro bis 516 Euro bedroht.

III. Ausgangsverfahren und Vorlagefrage

10. Die Staatsanwaltschaft (Bozen) ermittelte in zwei Strafsachen gegen Unbekannt wegen schweren Diebstahls eines Mobiltelefons gemäß den Art. 624 und 625 des Strafgesetzbuchs[13]. Um die Täter feststellen zu können, beantragte sie beim vorlegenden Gericht nach Art. 132

[10] GURI Nr. 234 vom 30. September 2021, S. 1.

[11] GURI Nr. 284 vom 29. November 2021, S. 1.

[12] Nach italienischem Recht gelten die Diebstähle, derentwegen vor dem vorlegenden Gericht ermittelt wird, als schwere Straftaten.

[13] Der erste Diebstahl wurde am 27. Oktober 2021 begangen (Aktenzeichen RGNR 9228/2021), der zweite am 20. November 2021 (Aktenzeichen RGNR 9794/2021). Die Mobiltelefone wurden in Bozen gestohlen; ihre Eigentümerinnen zeigten den Diebstahl bei den Carabinieri (Polizei) an.

Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003 „… die Genehmigung, bei allen Telefongesellschaften alle in deren Besitz befindliche Daten zu erheben zwecks Tracking und Ortung (insbesondere Nutzungen und eventuell IMEI-Codes des angerufenen/des anrufenden Anschlusses, besuchte/aufgerufene Websites, Uhrzeit und Dauer des Anrufs/der Verbindung und Angabe der Funkzellen und/oder betreffenden Mobilfunkmasten, Nutzungen und IMEI des Senders/Empfängers von SMS oder MMS und, wenn möglich, allgemeine Angaben zu den entsprechenden Anschlussinhabern) der ein- und ausgegangenen Telefongespräche/Kommunikationen und durchgeführten Verbindungen, auch im Roaming, auch wenn es sich um Anrufe handelt, die nicht berechnet wurden (Klingelzeichen), vom Zeitpunkt des Diebstahls bis zum Zeitpunkt der Antragstellung".

11. Das vorlegende Gericht bezweifelt, dass Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003 mit Art. 15 Abs. 1 der Richtlinie 2002/58 in der Auslegung durch das Urteil Prokuratuur vereinbar ist. Es weist darauf hin, dass die Corte suprema di cassazione (Kassationsgerichtshof, Italien) am 7. September 2021 [14] entschieden habe, dass das Urteil Prokuratuur von den nationalen Gerichten nicht unmittelbar angewandt werden könne, da diese bei der Feststellung, welche Straftaten „ernste Bedrohungen der öffentlichen Sicherheit oder eine schwere Kriminalität" darstellten, über einen Beurteilungsspielraum verfügten. Im Anschluss an das Urteil der Corte suprema di cassazione (Kassationsgerichtshof) habe der italienische Gesetzgeber das Gesetzesdekret Nr. 132 vom 30. September 2021 verabschiedet, in dessen Art. 132 Abs. 3 er als schwere Straftaten, für welche die Telefonverbindungsdaten erhoben werden dürften, u. a. solche einstufe, die „mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren …" bedroht seien.

12. Nach Ansicht des vorlegenden Gerichts umfasst der in Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003 für die Einstufung schwerer Kriminalität vorgesehene Strafrahmen auch Straftaten mit begrenzter sozialschädlicher Wirkung, die nur auf Antrag des Betroffenen verfolgt werden könnten [15]. Diese Vorschrift gestatte also die Erhebung von Telefonverbindungsdaten auch beim Diebstahl eines Gegenstands von geringem Wert, wie etwa eines Mobiltelefons oder eines Fahrrads. Der in Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003 festgelegte Strafrahmen verletze daher den Grundsatz der Verhältnismäßigkeit gemäß Art. 52 Abs. 1 der Charta, der immer eine Abwägung zwischen der Schwere der untersuchten Straftat und einer etwaigen Einschränkung der Ausübung eines Grundrechts verlange. Die Verfolgung derartiger Straftaten rechtfertige keine Einschränkung der Grundrechte auf Achtung des Privatlebens, auf Schutz personenbezogener Daten sowie auf Meinungs- und Informationsfreiheit [16].

13. Die italienischen Gerichte hätten nur ein sehr begrenztes Ermessen, um die Genehmigung für die Erhebung von Telefonverbindungsdaten abzulehnen, da sie bei Vorliegen „hinreichende[r] Anhaltspunkte für eine Straftat" erteilt werden müsse, wenn sie „für die Aufklärung der Straftat von Bedeutung" sei. Die Gerichte seien insbesondere nicht befugt, die Schwere der untersuchten Straftat zu bewerten. Diese Bewertung habe der Gesetzgeber vorgenommen, als er allgemein und

[14] Cass. Pen. Sez. II, n. 33116, ud. 7.9.2021, est. Pellegrino.

[15] Laut vorlegendem Gericht ist dies „z. B. bei Hausfriedensbruch der Fall, der nach Art. 614 des Strafgesetzbuchs mit einer Freiheitsstrafe von einem bis vier Jahren bedroht ist. Andere Straftaten, deren Strafrahmen der Erlangung von Telefonverbindungsdaten nicht entgegensteht und die nur auf Antrag verfolgt werden, weil sie gesellschaftlich nicht besonders besorgniserregend sind, sind Straftaten im Sinne von Art. 633 des Strafgesetzbuchs (Besetzung von Grundstücken und Gebäuden: Freiheitsstrafe von einem bis drei Jahren und Geldstrafe von 103 Euro bis 1 032 Euro) oder Art. 640 des Strafgesetzbuchs (einfacher Betrug: Freiheitsstrafe von sechs Monaten bis drei Jahren und Geldstrafe von 51 Euro bis 1 032 Euro)."

[16] Vgl. Art. 7, 8 und 11 der Charta.

ohne Differenzierung zwischen den verschiedenen Arten von Straftaten festgelegt habe, dass der Zugang zu Telefonverbindungsdaten u. a. für die Ermittlung aller Straftaten zu gestatten sei, die mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren bedroht seien.

14. Unter diesen Umständen hat das Tribunale di Bolzano (Landesgericht Bozen) beschlossen, die Verfahren auszusetzen und dem Gerichtshof die folgende Frage zur Vorabentscheidung vorzulegen:

Steht Art. 15 Abs. 1 der Richtlinie 2002/58 einer nationalen Regelung entgegen, die wie Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003 Folgendes vorsieht:

„Bestehen innerhalb der gesetzlich vorgeschriebenen Aufbewahrungsfrist ausreichende Anhaltspunkte für Straftaten, für die das Gesetz eine lebenslange Freiheitsstrafe oder eine Freiheitsstrafe im Höchstmaß von mindestens drei Jahren vorsieht, die gemäß Art. 4 der Strafprozessordnung bestimmt wird, oder für Straftaten der Bedrohung, Belästigung oder Störung von Personen per Telefon und handelt es sich um eine ernsthafte Bedrohung, Belästigung oder Störung, so werden die Daten, falls sie für die Aufklärung des Sachverhalts von Bedeutung sind, auf Antrag der Staatsanwaltschaft oder auf Ersuchen des Verteidigers des Angeklagten, des Beschuldigten, der verletzten Person oder anderer privater Beteiligter erhoben, nachdem der Richter durch mit Gründen versehenen Beschluss die Genehmigung hierzu erteilt hat“?

IV. Verfahren vor dem Gerichtshof

15. Die tschechische und die estnische Regierung, Irland, die französische, die italienische, die zyprische, die ungarische, die niederländische, die österreichische und die polnische Regierung sowie die Europäische Kommission haben schriftliche Erklärungen eingereicht.

16. Diese Verfahrensbeteiligten und die Staatsanwaltschaft (Bozen) haben in der Sitzung vom 21. März 2023 mündliche Ausführungen gemacht und Fragen des Gerichtshofs beantwortet.

V. Rechtliche Würdigung

A. Zulässigkeit

17. Die italienische Regierung und Irland halten das Ersuchen um Vorabentscheidung für teilweise unzulässig. Ausweislich der Sachverhaltsdarstellung in der Vorlageentscheidung beziehe sich der Antrag auf Datenzugang auf Ermittlungen wegen schweren Diebstahls von Mobiltelefonen. Die Staatsanwaltschaft könne, wie Irland hervorhebt, diese Straftat von Amts wegen verfolgen. Diese Befugnis sei Ausdruck der Vorstellung, dass die Art und die Wirkungen der Straftat die Gesellschaft im Allgemeinen berührten. Das Vorabentscheidungsersuchen sei daher insofern hypothetisch, als es sich auch auf Straftaten beziehe, die nur auf Antrag des Betroffenen verfolgt werden könnten. Das vorlegende Gericht verweise, wie die italienische Regierung bemerkt, auf mehrere Straftaten, die mit den bei ihm anhängigen Strafsachen nichts zu tun hätten. Die italienische Regierung und die Kommission tragen vor, entgegen dem im Vorabentscheidungsersuchen enthaltenen Hinweis auf „eine Freiheitsstrafe im Höchstmaß von mindestens drei Jahren“ sehe Art. 625 des Strafgesetzbuchs für schweren Diebstahl eine Freiheitsstrafe von zwei bis sechs Jahren vor. Die Kommission schlägt daher dem Gerichtshof

vor, die Frage umzuformulieren. Auch die französische Regierung spricht sich für eine Umformulierung aus. Während der Gerichtshof Bestimmungen des Unionsrechts auslegen dürfe, sei er nicht befugt, sich zur Vereinbarkeit nationaler Rechtsvorschriften mit dem Unionsrecht zu äußern.

18. Mit seiner Frage bittet das vorlegende Gericht den Gerichtshof ausdrücklich, über die Vereinbarkeit einer nationalen Regelung mit dem Unionsrecht zu entscheiden. Dies hindert an sich nicht daran, dem vorlegenden Gericht eine Auslegung des Unionsrechts, hier von Art. 15 Abs. 1 der Richtlinie 2002/58, zu unterbreiten, anhand deren es entscheiden kann, ob eine nationale Regelung, die Gegenstand des bei ihm anhängigen Verfahrens ist, mit dieser Bestimmung in Einklang steht [17].

19. Aus dem Vorabentscheidungsersuchen geht hervor, dass die Staatsanwaltschaft (Bozen) den Zugang zu den Daten u. a. zur Ermittlung und Verfolgung von zwei Fällen des schweren Diebstahls eines Mobiltelefons nach Art. 625 des Strafgesetzbuchs beantragt hat. Deshalb sind die in diesem Ersuchen enthaltenen Hinweise auf andere Straftatbestände, wie etwa Art. 624 des Strafgesetzbuchs (einfacher Diebstahl) [18], für die Entscheidung über die beim vorlegenden Gericht anhängigen Anträge unerheblich [19]. Soweit die Vorlagefrage den Antrag der Staatsanwaltschaft (Bozen) auf Datenzugriff zur Aufklärung etwaiger Straftaten des schweren Diebstahls betrifft, ist sie nicht hypothetisch. Ich werde mich daher bei der Prüfung der Anwendung von Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003 auf den vom vorlegenden Gericht geschilderten Sachverhalt – einen schweren Diebstahl von Mobiltelefonen – beschränken.

B. Beantwortung der Vorlagefrage

1. Vorbemerkungen

20. Das vorliegende Ersuchen geht auf einen Antrag der Staatsanwaltschaft (Bozen) auf Zugang zu den von den Betreibern elektronischer Kommunikationsdienste aufbewahrten Daten zurück. Sie betrifft weder die Speicherung dieser Daten an sich noch deren Rechtmäßigkeit u. a. nach Art. 15 Abs. 1 der Richtlinie 2002/58 [20]. Bei den Daten handelt es sich u. a. um detaillierte Angaben zu den mit den gestohlenen Mobiltelefonen getätigten ein- und ausgehenden Nachrichten [21] sowie um Standortdaten [22]. Obwohl die Daten nicht den Inhalt der Nachricht abdecken, lassen sie genaue Schlüsse auf das Privatleben der Personen zu, deren Daten betroffen

[17] Vgl. entsprechend Urteil vom 17. März 2021, Consulmarketing (C-652/19, EU:C:2021:208, Rn. 33). Nach ständiger Rechtsprechung obliegt es dem Gerichtshof gemäß Art. 267 AEUV, dem vorlegenden Gericht eine für die Entscheidung des bei diesem anhängigen Rechtsstreits sachdienliche Antwort zu geben. Zu diesem Zweck darf der Gerichtshof die Vorlagefragen umformulieren. Urteil vom 25. Juli 2018, Dyson (C-632/16, EU:C:2018:599, Rn. 47 und die dort angeführte Rechtsprechung).

[18] Wer einen einfachen Diebstahl begeht, dem droht eine Freiheitsstrafe von sechs Monaten bis drei Jahren und er fällt daher in den Anwendungsbereich von Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003.

[19] Soweit sich aus diesen Hinweisen ergibt, dass Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003 auch bei der Ermittlung von Delikten in Betracht kommt, die keine schweren Straftaten sind, verweise ich auf die Nrn. 35 bis 39 der vorliegenden Schlussanträge.

[20] Das Vorabentscheidungsersuchen beruht somit auf der Prämisse, dass die Speicherung der angeforderten Daten rechtmäßig ist. Die Speicherung von durch die Richtlinie 2002/58 erfassten Daten und der Zugang zu ihnen stellen unterschiedliche Eingriffe in die in den Art. 7, 8 und 11 der Charta garantierten Grundrechte dar und erfordern eine gesonderte Rechtfertigung nach Art. 52 Abs. 1 der Charta. Vgl. in diesem Sinne Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a. (C-140/20, EU:C:2022:258, Rn. 47). Die Rn. 29 bis 33 des Urteils Prokuratuur geben einen Überblick über die Vorschriften für die Speicherung solcher Daten.

[21] Nach Art. 2 Buchst. d der Richtlinie 2002/58 bezeichnet der Ausdruck „Nachricht" „jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlich zugänglichen elektronischen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. …"

[22] Nach Art. 2 Buchst. c der Richtlinie 2002/58 handelt es sich bei „Standortdaten" um „Daten, die … den geografischen Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen elektronischen Kommunikationsdienstes angeben".

sind; der Zugang zu diesen Daten stellt offensichtlich einen „schwerwiegenden" Eingriff in deren Grundrechte dar [23]. Der mit dem Zugang zu solchen Daten verbundene Eingriff kann durch das in Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58 genannte Ziel [24] der Verhütung, Ermittlung, Feststellung und Verfolgung „schwerer Straftaten", nicht aber von Straftaten im Allgemeinen, gerechtfertigt sein. Bei der Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 stellt der Gerichtshof einen Zusammenhang zwischen der Schwere des Eingriffs in die Grundrechte einer Person und der Schwere der untersuchten Straftat her [25].

2. Befugnis der Mitgliedstaaten, zu bestimmen, was unter einer „schweren Straftat" zu verstehen ist

21. Die Richtlinie 2002/58 regelt die Tätigkeiten der Betreiber elektronischer Kommunikationsdienste bei der Verarbeitung personenbezogener Daten [26]. Gemäß Art. 1 Abs. 3 sind staatliche Tätigkeiten in bestimmten Bereichen wie der öffentlichen Sicherheit, der Landesverteidigung und der Sicherheit des Staates sowie im strafrechtlichen Bereich ausdrücklich vom Anwendungsbereich der Richtlinie 2002/58 ausgenommen. Die Tätigkeiten, auf die Art. 15 Abs. 1 der Richtlinie 2002/58 Bezug nimmt, überschneiden sich im Wesentlichen mit denen, die in Art. 1 Abs. 3 dieser Richtlinie beschrieben sind, und umfassen staatliche Tätigkeiten im Bereich des Strafrechts, die ausdrücklich vom Geltungsbereich dieser Richtlinie ausgeschlossen sind [27]. Es besteht somit ein eindeutiger Zusammenhang zwischen den staatlichen Tätigkeiten, die gemäß Art. 1 Abs. 3 der Richtlinie 2002/58 von deren Geltungsbereich ausgeschlossen sind, und den Rechtsvorschriften, die die Mitgliedstaaten nach Art. 15 Abs. 1 dieser Richtlinie erlassen dürfen [28].

22. Ungeachtet dieses eindeutigen Zusammenhangs hat der Gerichtshof in ständiger Rechtsprechung entschieden, dass die in Art. 15 Abs. 1 der Richtlinie 2002/58 beschriebenen nationalen Rechtsvorschriften in den Geltungsbereich der Richtlinie fallen, da diese Bestimmung die Mitgliedstaaten ausdrücklich zum Erlass solcher Vorschriften ermächtigt. Aus dieser Rechtsprechung folgt, dass sich der Begriff „Tätigkeiten", einschließlich der „Tätigkeiten des Staates im strafrechtlichen Bereich" im Sinne von Art. 1 Abs. 3 der Richtlinie 2002/58, nicht auf die in Art. 15 Abs. 1 dieser Richtlinie genannten Rechtsvorschriften erstreckt [29].

[23] Urteil Prokuratuur, Rn. 34 und 35. Vgl. entsprechend Urteil vom 2. Oktober 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, Rn. 59 bis 62). Es ist Sache des nationalen Gerichts, zu beurteilen, ob der Zugang zu den fraglichen Daten einen „schwerwiegenden" Eingriff in die Grundrechte der Personen darstellt, deren Daten betroffen sind. In den vorliegenden Schlussanträgen gehe ich davon aus, dass der Zugang zu den oben in Nr. 10 beschriebenen Daten mit einem solchen schwerwiegenden Eingriff verbunden ist.

[24] Die Aufzählung der Ziele in Art. 15 Abs. 1 der Richtlinie 2002/58 ist abschließend. Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970, Rn. 90).

[25] Vgl. in diesem Sinne Schlussanträge von Generalanwalt Saugmandsgaard Øe in der Rechtssache Ministerio Fiscal (C-207/16, EU:C:2018:300, Nrn. 79 bis 82 und die dort angeführte Rechtsprechung). Im Zusammenhang mit dem Ziel, die Kriminalität zu bekämpfen, darf ein Zugang grundsätzlich nur zu den Daten von Personen gewährt werden, die im Verdacht stehen, eine schwere Straftat zu planen, zu begehen oder begangen zu haben oder auf irgendeine Weise in eine solche Straftat verwickelt zu sein. Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a. (C-140/20, EU:C:2022:258, Rn. 105).

[26] Vgl. in diesem Sinne Art. 3 der Richtlinie 2002/58, wonach die Richtlinie für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste gilt. Vgl. auch Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970, Rn. 70 und 74), sowie entsprechend Schlussanträge von Generalanwalt Szpunar in der Rechtssache La Quadrature du Net u. a. (Personenbezogene Daten und Maßnahmen zur Bekämpfung von Urheberrechtsverletzungen) (C-470/21, EU:C:2022:838, Nr. 38).

[27] Urteil vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 97).

[28] Zum Schutz der nationalen Sicherheit, der Landesverteidigung und der öffentlichen Sicherheit sowie zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen.

[29] Urteile vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 98), und vom 6. Oktober 2020, Privacy International (C-623/17, EU:C:2020:790, Rn. 38 und die dort angeführte Rechtsprechung).

23. Weder in Art. 2 der Richtlinie 2002/58, der eine Reihe von Begriffsbestimmungen für die Zwecke der Anwendung dieser Richtlinie enthält, noch in einer anderen Bestimmung der Richtlinie 2002/58, auch nicht in Art. 15 Abs. 1, wird der Begriff „Straftaten" definiert. Die Richtlinie 2002/58 enthält auch keine Aufzählung von „Straftaten" [30]. Ebenso wenig findet sich in der Rechtsprechung zur Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 eine Definition dieses Begriffs [31].

24. Obwohl es an derartigen Begriffsbestimmungen fehlt, sieht die Richtlinie 2002/58 nicht vor, dass jeder Mitgliedstaat „Straftaten" nach Maßgabe seines nationalen Rechts definiert [32]. Nach ständiger Rechtsprechung des Gerichtshofs folgt aus den Anforderungen sowohl der einheitlichen Anwendung des Unionsrechts als auch des Gleichheitsgrundsatzes, dass eine Bestimmung des Unionsrechts, die für die Ermittlung ihres Sinnes und ihrer Bedeutung nicht ausdrücklich auf das Recht der Mitgliedstaaten verweist, in der Regel in der gesamten Union eine autonome und einheitliche Auslegung erhalten muss. Im Rahmen der Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 kann der Begriff „Straftaten" zumindest grundsätzlich als autonomer Begriff des Unionsrechts angesehen werden, der im Hoheitsgebiet sämtlicher Mitgliedstaaten einheitlich auszulegen ist [33].

25. Die zehn Mitgliedstaaten, die Erklärungen beim Gerichtshof eingereicht haben, und die Kommission sind jedoch übereinstimmend der Ansicht, es sei Sache jedes Mitgliedstaats, den Begriff „Straftaten", einschließlich schwerer Straftaten, auf den Art. 15 Abs. 1 der Richtlinie 2002/58 verweise, in seinem nationalen Recht zu definieren.

26. Diesem Vorbringen schließe ich mich aus den folgenden Gründen an.

27. Erstens hat der Gerichtshof bereits entschieden, dass es im Zusammenhang mit Art. 15 Abs. 1 der Richtlinie 2002/58 Sache der Mitgliedstaaten ist, ihre wesentlichen Sicherheitsinteressen festzulegen und die geeigneten Maßnahmen zu ergreifen, um ihre innere und äußere Sicherheit zu gewährleisten [34]. Der Gerichtshof scheint also, auch wenn er dies nicht ausdrücklich festgestellt hat, der Auffassung zu sein, dass der Begriff „nationale Sicherheit" in Art. 15 Abs. 1 der Richtlinie 2002/58, obwohl er nicht definiert ist und es auch an einem ausdrücklichen Verweis auf das Recht

30 Vgl. demgegenüber Art. 2 Abs. 2 des Rahmenbeschlusses 2002/584/JI des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten (ABl. 2002, L 190, S. 1) in der Fassung des Rahmenbeschlusses 2009/299/JI des Rates vom 26. Februar 2009 (ABl. 2009, L 81, S. 24), in dem die Straftaten aufgeführt sind, bei denen eine Übergabe aufgrund eines Europäischen Haftbefehls erfolgt, sowie Anhang II der Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (ABl. 2016, L 119, S. 132), in dem die in Art. 3 Nr. 9 dieser Richtlinie definierten Straftaten „schwerer Kriminalität" aufgeführt sind.

31 Die Richtlinie 2002/58 spricht weder von „Straftaten im Allgemeinen" noch von „schweren Straftaten" oder von „Kriminalität". Der Gerichtshof verwendet in seiner Rechtsprechung diese Begriffe, ohne sie zu definieren oder Kriterien dafür zu nennen, wie der nationale Gesetzgeber dies tun könnte. Vgl. u. a. Urteile vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970, Rn. 115 und 125), und vom 2. Oktober 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, Rn. 54, 56 und 63). Vgl. hierzu auch Rn. 45 des Urteils Prokuratuur.

32 Vgl. demgegenüber Art. 1 Abs. 1 der 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 (ABl. 2006, L 105, S. 54), in dem es hieß: „Mit dieser Richtlinie sollen die Vorschriften der Mitgliedstaaten über die Pflichten von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes im Zusammenhang mit der Vorratsspeicherung bestimmter Daten, die von ihnen erzeugt oder verarbeitet werden, harmonisiert werden, um sicherzustellen, dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, *wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden*, zur Verfügung stehen." (Hervorhebung nur hier). Mit Urteil vom 8. April 2014, Digital Rights Ireland u. a. (C-293/12 und C-594/12, EU:C:2014:238), hat der Gerichtshof die Richtlinie 2006/24 für ungültig erklärt.

33 Vgl. entsprechend Urteil vom 7. September 2022, Staatssecretaris van Justitie en Veiligheid (Natur des Aufenthaltsrechts aus Art. 20 AEUV) (C-624/20, EU:C:2022:639, Rn. 19 und 20).

34 Urteil vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 99 und 136).

der Mitgliedstaaten fehlt, kein autonomer Begriff des Unionsrechts ist [35]. Ich sehe keinen Grund, warum dies nicht auch für die Befugnis der Mitgliedstaaten gelten sollte, „Straftaten" oder „schwere Straftaten" im Sinne von Art. 15 Abs. 1 der Richtlinie 2002/58 zu definieren. Die Begriffe „Straftaten", „öffentliche Sicherheit" und „nationale Sicherheit" in dieser Bestimmung können als ein zusammengehöriges Ganzes (*noscitur a sociis*) angesehen werden, denn es war offenbar der Wille des Unionsgesetzgebers, dass sie alle in gleicher Weise behandelt werden sollten, auch in Bezug auf die Methode ihrer Definition [36].

28. Zweitens verpflichtet Art. 4 Abs. 2 EUV die Union zur Achtung der nationalen Identität der Mitgliedstaaten, die in deren grundlegenden politischen und verfassungsmäßigen Strukturen zum Ausdruck kommt. Auch in der Präambel der Charta wird bekräftigt, dass die Union zwar zur Erhaltung und zur Entwicklung gemeinsamer Werte beiträgt, dabei aber u. a. die Vielfalt der Kulturen und Traditionen der Völker Europas achtet. Die Definition von Straftaten und Strafen [37] spiegelt nationale Befindlichkeiten und Traditionen wider, die sich nicht nur von Mitgliedstaat zu Mitgliedstaat, sondern auch im Laufe der Zeit und im Zuge des gesellschaftlichen Wandels erheblich voneinander unterscheiden [38].

29. In diesem Zusammenhang ist darauf hinzuweisen, dass die Mitgliedstaaten bei der Festlegung von Straftatbeständen und Strafen eine Vielzahl verschiedener Faktoren in unterschiedlichem Maße berücksichtigen. Die Bewertung der „Schwere" einer bestimmten Straftat durch einen Mitgliedstaat schlägt sich häufig, wenn nicht ausnahmslos, in der Schwere der Strafe nieder, mit der er die Begehung dieser Straftat bedroht. In der Dauer einer Freiheitsstrafe kann eine Analyse mehrerer Faktoren zum Ausdruck kommen, wie etwa die vermutete immanente „Schwere" einer Straftat sowie ihre relative „Schwere" im Vergleich zu anderen Straftaten. Es wurden keine Gründe dafür angeführt, warum die Mitgliedstaaten von dieser Befugnis keinen Gebrauch machen sollten oder warum überhaupt für die Definition von „Straftaten", „schweren Straftaten" oder „Straftaten im Allgemeinen" im vorliegenden speziellen Kontext etwas anderes gelten sollte.

30. Die Zuständigkeit der Mitgliedstaaten im Bereich des Strafrechts lässt die Zuständigkeit der Union unberührt, in gewissen Fällen z. B. Mindestvorschriften zur Festlegung von Straftaten und Strafen im Hinblick auf besonders schwere Kriminalität zu erlassen, die aufgrund der Art oder der Auswirkungen dieser Straftaten oder aufgrund einer besonderen Notwendigkeit, sie auf einer

[35] Darüber hinaus fällt nach Art. 4 Abs. 2 EUV die nationale Sicherheit weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten. Die Tatsache, dass eine nationale Maßnahme zum Schutz der nationalen Sicherheit getroffen wird, führt nicht zur Unanwendbarkeit des Unionsrechts und entbindet die Mitgliedstaaten nicht von der erforderlichen Beachtung dieses Rechts. Urteil vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 99 und 135).

[36] Auch wenn das Ziel des Schutzes der nationalen Sicherheit bedeutsamer ist als das Ziel der Bekämpfung schwerer Kriminalität und daher gravierendere Grundrechtseingriffe rechtfertigen kann, berührt dieses Ziel nicht das Recht der Mitgliedstaaten, „Straftaten" oder „schwere Straftaten" zu definieren. Urteil vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 136).

[37] Sowie von strafmildernden und -erschwerenden Umständen.

[38] Nach Ansicht von Generalanwalt Saugmandsgaard Øe fallen die Strafgesetzgebung und das Strafverfahren in die Zuständigkeit der Mitgliedstaaten, auch wenn das nationale Recht von in diesem Bereich u. a. gemäß Art. 83 Abs. 2 AEUV erlassenen Bestimmungen des Unionsrechts berührt werden könne. Es gebe also keine allgemeine Bestimmung, die eine Definition des Begriffs der „schweren Straftat" enthalte. Schlussanträge in der Rechtssache Ministerio Fiscal (C-207/16, EU:C:2018:300, Nr. 95). Generalanwalt Pitruzzella zufolge muss die Definition dessen, was als „schwere Straftat" eingestuft werden könne, den Mitgliedstaaten überlassen bleiben. Nach den nationalen Rechtsordnungen könne dieselbe Straftat nämlich mehr oder weniger scharf verurteilt werden. Auch die Definition der straferschwerenden Umstände könne von Mitgliedstaat zu Mitgliedstaat variieren. Schlussanträge in der Rechtssache Prokuratuur (Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation) (C-746/18, EU:C:2020:18, Nrn. 91 und 92). Nach Ansicht von Generalanwalt Szpunar ist hingegen „[d]er Begriff ‚schwere Kriminalität' … autonom auszulegen. Er darf nicht von den Auffassungen der einzelnen Mitgliedstaaten abhängen, weil es andernfalls möglich wäre, die Anforderungen von Art. 15 Abs. 1 der Richtlinie 2002/58 zu umgehen, je nachdem, ob die Mitgliedstaaten ein weites Verständnis der Bekämpfung schwerer Kriminalität vertreten oder nicht." Schlussanträge in der Rechtssache La Quadrature du Net u. a. (Personenbezogene Daten und Maßnahmen zur Bekämpfung von Urheberrechtsverletzungen) (C-470/21, EU:C:2022:838, Nr. 74).

gemeinsamen Grundlage zu bekämpfen, eine grenzüberschreitende Dimension haben [39]. Der Unionsgesetzgeber hat jedoch keine Vorschriften zur Definition von Straftaten im Sinne von Art. 15 Abs. 1 der Richtlinie 2002/58 erlassen [40]. Wie bereits dargelegt [41], ergibt sich nämlich aus Art. 1 Abs. 3 dieser Richtlinie, dass der Unionsgesetzgeber mit deren Erlass keine Zuständigkeit im strafrechtlichen Bereich wahrnehmen wollte.

31. Diese beiden Gründe erklären hinreichend, warum die Mitgliedstaaten, obwohl die nach Art. 15 Abs. 1 der Richtlinie 2002/58 erlassenen nationalen Rechtsvorschriften zur Ermittlung und Verfolgung von Straftaten in den Anwendungsbereich dieser Richtlinie fallen, weiterhin für die Definition von „Straftaten", einschließlich „schwerer Straftaten", und die Festlegung von Strafen für die Begehung solcher Taten zuständig sind [42].

3. Prüfungsmaßstab in Bezug auf die Ausübung der in Art. 15 Abs. 1 der Richtlinie 2002/58 vorgesehenen Möglichkeit, vom Grundsatz der Vertraulichkeit abzuweichen

32. Der Gerichtshof hat betont, dass die Möglichkeit, u. a. von dem in Art. 5 Abs. 1 der Richtlinie 2002/58 vorgesehenen Grundsatz der Vertraulichkeit abzuweichen [43], eng auszulegen ist, damit sie nicht zur allgemeinen Regel und der Grundsatz nicht dadurch ausgehöhlt wird [44]. Bei der Wahrnehmung dieser Möglichkeit müssen daher unter anderem die Grundsätze der Äquivalenz [45] und der Effektivität beachtet werden [46]. Dabei ist auch den allgemeinen Grundsätzen des Unionsrechts, einschließlich des Grundsatzes der Verhältnismäßigkeit [47], sowie den Art. 7, 8 und 11 [48] nebst Art. 52 Abs. 1 der Charta zu genügen [49]. Das Ziel der Bekämpfung schwerer Straftaten muss stets mit der Wahrung der hiervon betroffenen Grundrechte in Einklang gebracht werden. Die in den Art. 7, 8 und 11 der Charta verankerten Rechte können

[39] Art. 83 Abs. 1 Unterabs. 1 AEUV. Vgl. auch Urteil vom 21. Oktober 2021, Okrazhna prokuratura – Varna (C-845/19 und C-863/19, EU:C:2021:864, Rn. 32).

[40] Vgl. entsprechend Urteil Prokuratuur (Rn. 41 und 42). Der Gerichtshof hat entschieden, dass es mangels einschlägiger unionsrechtlicher Vorschriften nach dem Grundsatz der Verfahrensautonomie „grundsätzlich allein Sache des nationalen Rechts ist, die Vorschriften für die Zulässigkeit und die Würdigung der durch eine unionsrechtswidrige allgemeine und unterschiedslose Speicherung dieser Daten erlangten Informationen und Beweise im Rahmen eines Strafverfahrens gegen Personen festzulegen, die im Verdacht stehen, Straftaten begangen zu haben". Rechtsgrundlage der Richtlinie 2002/58 ist Art. 114 AEUV (vormals Art. 95 EGV) und nicht z. B. Art. 83 Abs. 1 Unterabs. 1 AEUV. Im Gegensatz dazu beruht die Richtlinie 2016/681 auf Art. 82 Abs. 1 Unterabs. 2 Buchst. d AEUV (justizielle Zusammenarbeit in Strafsachen) und auf Art. 87 Abs. 2 Buchst. a AEUV (polizeiliche Zusammenarbeit).

[41] Siehe Nr. 21 der vorliegenden Schlussanträge.

[42] Vgl. entsprechend Urteil vom 23. Oktober 2007, Kommission/Rat (C-440/05, EU:C:2007:625, Rn. 66, 70 und 71 und die dort angeführte Rechtsprechung). Vgl. auch Urteil vom 28. April 2011, El Dridi (C-61/11 PPU, EU:C:2011:268, Rn. 53).

[43] In Art. 15 Abs. 1 der Richtlinie 2002/58 heißt es, dass die Mitgliedstaaten Rechtsvorschriften „erlassen können", die bestimmte in dieser Richtlinie vorgesehene Rechte und Pflichten beschränken.

[44] Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970, Rn. 89). Generalanwalt Saugmandsgaard Øe hat hierzu erklärt: „Auch wenn … jeder Mitgliedstaat in der Beurteilung, was ein für eine schwere Straftat angemessenes Strafmaß ist, frei ist, ist er gleichwohl verpflichtet, dieses nicht auf ein im Verhältnis zu den in diesem Staat üblichen Strafen derart niedriges Maß festzulegen, dass die in diesem Art. 15 Abs. 1 vorgesehenen Ausnahmen vom Verbot der Speicherung und Nutzung zur Regel gemacht werden …" Schlussanträge in der Rechtssache Ministerio Fiscal (C-207/16, EU:C:2018:300, Nr. 114).

[45] Es deutet nichts darauf hin, dass das fragliche italienische Gesetz diesem Grundsatz nicht entsprechen würde.

[46] Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a. (C-140/20, EU:C:2022:258, Rn. 127).

[47] Vgl. auch elfter Erwägungsgrund der Richtlinie 2002/58.

[48] Vgl. auch zweiter Erwägungsgrund der Richtlinie 2002/58.

[49] Urteile vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970, Rn. 89), und vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 111 bis 113). Vgl. auch Schlussanträge von Generalanwalt Saugmandsgaard Øe in der Rechtssache Ministerio Fiscal (C-207/16, EU:C:2018:300, Nrn. 116 bis 120). Im Urteil vom 8. März 2022, Bezirkshauptmannschaft Hartberg-Fürstenfeld (Unmittelbare Wirkung) (C-205/20, EU:C:2022:168, Rn. 31), hat der Gerichtshof darauf hingewiesen, dass die Mitgliedstaaten bei der Durchführung des Unionsrechts den Grundsatz der Verhältnismäßigkeit beachten müssen. Die Mitgliedstaaten haben, wenn sie in diesem Zusammenhang strafrechtliche Sanktionen festlegen, Art. 49 Abs. 3 der Charta zu beachten, auch wenn es keine Rechtsvorschriften der Union zur Harmonisierung dieser Sanktionen gibt.

keine uneingeschränkte Geltung beanspruchen; ihre Ausübung muss im Hinblick auf ihre gesellschaftliche Funktion gesehen werden [50]. Art. 52 Abs. 1 der Charta lässt daher Einschränkungen der Ausübung dieser Rechte zu, sofern sie gesetzlich vorgesehen sind, den Wesensgehalt der Rechte achten, unter Wahrung des Verhältnismäßigkeitsgrundsatzes erforderlich sind und den von der Europäischen Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen. Nationale Rechtsvorschriften, die aufgrund von Art. 15 Abs. 1 der Richtlinie 2002/58 erlassen werden, müssen also tatsächlich strikt einem der in dieser Bestimmung genannten Zweck dienen. Sie müssen sich auf objektive Kriterien stützen, rechtsverbindlich sein sowie klare und präzise Regeln aufstellen, aus denen hervorgeht, unter welchen materiell- und verfahrensrechtlichen Voraussetzungen die Betreiber elektronischer Kommunikationsdienste den zuständigen nationalen Behörden Zugang zu den Daten zu gewähren haben [51].

33. Damit in der Praxis die vollständige Einhaltung dieser Voraussetzungen gewährleistet ist, muss der Zugang der zuständigen nationalen Behörden zu gespeicherten Daten grundsätzlich [52] einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen werden [53], nachdem diese Behörden einen mit Gründen versehenen Antrag gestellt und die betroffenen Personen davon in Kenntnis gesetzt haben [54]. Nach ständiger Rechtsprechung muss das Gericht oder die unabhängige Verwaltungsstelle bei der Durchführung dieser vorherigen Kontrolle die verschiedenen einander gegenüberstehenden Interessen und Rechte miteinander in Einklang bringen, um für einen gerechten Ausgleich zwischen den Erfordernissen der Ermittlungen und der gebotenen Wahrung der Grundrechte auf Achtung der Privatsphäre und auf Schutz der personenbezogenen Daten der Betroffenen zu sorgen [55].

34. Im vorliegenden Fall regelt Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003 die Voraussetzungen, unter denen ein nationales Gericht den Betreibern elektronischer Kommunikationsdienste aufgeben muss, der Staatsanwaltschaft auf deren Antrag Zugang zu Daten zu gewähren. Es steht fest [56], dass dieser Art. 132 Abs. 3 in klaren und präzisen Worten festlegt, unter welchen Umständen und Voraussetzungen ein nationales Gericht die Betreiber elektronischer Kommunikationsdienste anweisen kann, einen solchen Zugang zu gewähren. Das vorlegende Gericht ist jedoch der Ansicht, die Sanktion einer „Freiheitsstrafe im Höchstmaß von mindestens drei Jahren“ sei zu weit gefasst, da sie auch wenig sozialschädliche Straftaten wie einfachen Diebstahl erfasse.

[50] Art. 52 Abs. 1 der Charta. Urteil vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 120).

[51] Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970, Rn. 117 bis 119). Vgl. auch Urteil vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 110 und 129 bis 133).

[52] Zum Beispiel enthält Art. 132 Abs. 3-bis des gesetzesvertretenden Dekrets Nr. 196/2003 Sonderbestimmungen für den Zugang zu Daten in dringenden Fällen. In seinen Schlussanträgen in der Rechtssache La Quadrature du Net u. a. (Personenbezogene Daten und Maßnahmen zur Bekämpfung von Urheberrechtsverletzungen) (C-470/21, EU:C:2022:838, Nrn. 99 bis 105) hat Generalanwalt Szpunar ausgeführt, eine vorherige Kontrolle sei nur geboten, wenn ein schwerwiegender Eingriff in das Privatleben der Nutzer elektronischer Kommunikationsdienste vorliege. Da der Eingriff im vorliegenden Verfahren wegen der Art der Daten, zu denen die Staatsanwaltschaft Zugang begehrt, schwerwiegend ist, bedarf es einer vorherigen Prüfung.

[53] Das Erfordernis der vorherigen Kontrolle geht auf die Rechtsprechung des Gerichtshofs und nicht auf die Richtlinie 2002/58 zurück: Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970, Rn. 120 und 121 und die dort angeführte Rechtsprechung).

[54] Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970, Rn. 120 und 121).

[55] Urteil Prokuratuur (Rn. 52).

[56] Vorbehaltlich einer Überprüfung durch das vorlegende Gericht.

35. Obwohl Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003 potenziell ein breites Spektrum von Straftaten abdeckt, liegen dem Gerichtshof im vorliegenden Verfahren keine Anhaltspunkte vor, dass wegen der großen Zahl der erfassten Straftaten der Zugang zu Daten hiernach eher die Regel als die Ausnahme wäre [57]. Der in dieser Bestimmung vorgesehene Strafrahmen einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren erscheint nicht als zu niedrig [58]. Zum Vergleich: Art. 3 Nr. 9 der Richtlinie 2016/681 [59] definiert „schwere Kriminalität" als „die in Anhang II aufgeführten strafbaren Handlungen, die nach dem nationalen Recht eines Mitgliedstaats mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht sind" [60]. Der Gerichtshof hat allerdings entschieden, dass – da sich Art. 3 Abs. 9 der Richtlinie 2016/681 nicht auf die jeweilige Mindeststrafe, sondern auf die jeweilige Höchststrafe bezieht – nicht auszuschließen ist, dass die betreffenden „Daten Gegenstand einer Verarbeitung zur Bekämpfung strafbarer Handlungen sein können, die, obwohl sie das in dieser Bestimmung vorgesehene Kriterium in Bezug auf den Schweregrad erfüllen, angesichts der Besonderheiten des nationalen Strafrechtssystems nicht zur schweren Kriminalität gehören, sondern zur gewöhnlichen Kriminalität" [61].

36. Die in Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003 vorgesehene Strafe von drei Jahren bezieht sich auf die jeweilige Höchststrafe und könnte somit auch für Straftaten wie einfachen Diebstahl gelten [62]. Es ist daher zu untersuchen, wie diese Bestimmung in der Praxis angewandt wird. Vorbehaltlich einer Überprüfung durch das vorlegende Gericht scheint Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003 je nach Art der untersuchten Straftaten zwei unterschiedliche Prüfungsmaßstäbe für die vorherige Kontrolle durch ein nationales Gericht vorzugeben.

37. Im Rahmen des ersten dieser Prüfungsmaßstäbe sind die nationalen Gerichte verpflichtet [63], der Staatsanwaltschaft den Zugriff auf die von den Betreibern elektronischer Kommunikationsdienste gespeicherten Daten zu gestatten, wenn diese Daten für die Zwecke der Aufklärung des Sachverhalts relevant sind und ausreichende Anhaltspunkte für die Begehung einer Straftat der Bedrohung und Belästigung oder Störung von Personen per Telefon vorliegen, sofern die Bedrohung oder die Störung schwerwiegend ist. Das nationale Gericht muss daher im Einzelfall die Schwere der fraglichen Straftat beurteilen und prüfen, ob deren Untersuchung und Verfolgung eine Einschränkung der in den Art. 7, 8 und 11 der Charta verankerten allgemeinen Rechte sowie der in den Art. 5, 6 und 9 der Richtlinie 2002/58 vorgesehenen besonderen Rechte

[57] Vgl. die Analyse in den Schlussanträgen von Generalanwalt Saugmandsgaard Øe in der Rechtssache Ministerio Fiscal (C-207/16, EU:C:2018:300, Nrn. 116 bis 120). Es ist letztlich Sache des vorlegenden Gerichts, dies zu beurteilen.

[58] Der Umstand, dass es in einem Mitgliedstaat eine andere Definition von Straftaten und eine andere Sanktionsregelung gibt als in einem anderen, kann für sich allein keinen Einfluss auf die Verhältnismäßigkeit der Rechtsvorschriften haben. Vgl. entsprechend Urteil vom 8. Juli 2010, Sjöberg und Gerdin (C-447/08 und C-448/08, EU:C:2010:415, Rn. 38).

[59] Die Richtlinie 2016/681 betrifft die Übermittlung und Verarbeitung von Fluggastdaten zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität.

[60] Der Gerichtshof hat entschieden, dass die aus dieser Bestimmung resultierenden Anforderungen, die sich auf Art und Schwere der verwirkten Strafe beziehen, grundsätzlich geeignet sind, die Anwendung des durch die Richtlinie 2016/681 geschaffenen Systems auf strafbare Handlungen mit hinreichendem Schweregrad zu beschränken, die einen Eingriff in die in den Art. 7 und 8 der Charta verankerten Grundrechte rechtfertigen können. Urteil vom 21. Juni 2022, Ligue des droits humains (C-817/19, EU:C:2022:491, Rn. 150).

[61] Der Gerichtshof hat somit festgestellt, dass die Mitgliedstaaten dafür sorgen müssen, dass das mit der Richtlinie 2016/681 geschaffene System auf die Bekämpfung schwerer Kriminalität beschränkt bleibt und nicht auf gewöhnliche Kriminalität erstreckt wird. Urteil vom 21. Juni 2022, Ligue des droits humains (C-817/19, EU:C:2022:491, Rn. 151 und 152). Die Richtlinie 2016/681, die u. a. den Austausch von PNR-Daten zwischen den Mitgliedstaaten vorsieht, überschneidet sich in ihrem Gegenstand und Anwendungsbereich nicht mit der Richtlinie 2002/58. Folglich sind die Bestimmungen dieser Richtlinien gesondert und nach ihren eigenen Merkmalen zu beurteilen. Insoweit ist der Begriff der „schweren Kriminalität" in der Richtlinie 2016/681 – anders als bei Art. 15 Abs. 1 der Richtlinie 2002/58 – ein autonomer Begriff des Unionsrechts. Vgl. hierzu auch zwölfter Erwägungsgrund sowie Art. 3 Nr. 9 und Anhang II der Richtlinie 2016/681.

[62] Vgl. entsprechend Urteil vom 21. Juni 2022, Ligue des droits humains (C-817/19, EU:C:2022:491, Rn. 151).

[63] In der Originalsprache heißt es „i dati sono acquisiti".

rechtfertigt. Anhand dieses Maßstabs kann im Einzelfall konkret beurteilt werden, ob der Eingriff in diese Rechte gemessen an dem im öffentlichen Interesse liegenden Ziel der Verbrechensbekämpfung verhältnismäßig ist.

38. Demgegenüber sind die nationalen Gerichte im Rahmen des – für unser Verfahren einschlägigen – zweiten dieser Prüfungsmaßstäbe verpflichtet[64], der Staatsanwaltschaft den Zugriff auf die von den Betreibern elektronischer Kommunikationsdienste gespeicherten Daten zu gestatten, wenn diese Daten für die Zwecke der Aufklärung des Sachverhalts relevant sind und ausreichende Anhaltspunkte für die Begehung einer Straftat vorliegen, die u. a. mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren bedroht ist. In diesem Fall beschränkt sich die Aufgabe des nationalen Gerichts auf die Prüfung, ob diese objektiven Voraussetzungen erfüllt sind, ohne dass es irgendeine Möglichkeit hätte, im Einzelfall die jeweiligen Interessen konkret einer Verhältnismäßigkeitsprüfung zu unterziehen[65]. Die Kontrolle, die das nationale Gericht gemäß Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003 ausübt, hat somit keinen realen Bezug zu den spezifischen Umständen des Einzelfalls, mit dem es befasst ist.

39. Wenngleich die nationalen Gerichte nicht befugt sein mögen, die gesetzliche Begriffsbestimmung von Straftaten oder deren Einstufung hinsichtlich des Schweregrades zu kontrollieren[66], müssen sie doch im Einzelfall prüfen dürfen, ob es verhältnismäßig ist, wenn aufgrund von Rechtsvorschriften gemäß Art. 15 Abs. 1 der Richtlinie 2002/58 Zugang zu sensiblen Daten gewährt wird, die genaue Schlüsse auf das Privatleben eines Nutzers zulassen, was einen gravierenden Eingriff in die in den Art. 7, 8 und 11 sowie in Art. 52 Abs. 1 der Charta verankerten Grundrechte darstellt.

40. Folglich dürfen die gemäß Art. 15 Abs. 1 der Richtlinie 2002/58 erlassenen Vorschriften nur dann Zugang zu sensiblen Daten gestatten, wenn i) die betreffende Straftat den vom nationalen Gesetzgeber im Voraus festgelegten Schweregrad erreicht und ii) ein Gericht oder eine unabhängige Verwaltungsbehörde im Anschluss an eine Einzelfallprüfung oder -kontrolle feststellt, dass der mit der Gewährung des Zugangs verbundene Eingriff in die Grundrechte jeweils in einem angemessenen Verhältnis zu dem im öffentlichen Interesse liegenden Ziel der Verbrechensbekämpfung steht. In manchen Fällen darf der Zugang zu solchen Daten aber auch dann nicht gewährt werden, wenn die Straftat den im nationalen Recht vorgesehenen Grad an Schwere erreicht.

41. Die Straftat des schweren Diebstahls, um die es sich im vorliegenden Fall handelt, gilt nach nationalem Recht als „schwer“, weil sie u. a. mit einer Freiheitsstrafe von zwei bis sechs Jahren bedroht ist und somit dem Schweregrad gemäß Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003 entspricht[67]. Bei der Anwendung von Vorschriften, die nach Art. 15 Abs. 1 der Richtlinie 2002/58 erlassen wurden, sind die italienischen Gerichte offenbar nicht befugt, die

[64] Vorbehaltlich einer Überprüfung durch das vorlegende Gericht bedeutet die Verwendung des Indikativs in Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003 („i dati sono acquisiti“), dass der Zugang zu den betreffenden Daten vom nationalen Gericht gewährt wird, sofern die in dieser Bestimmung aufgestellten objektiven Voraussetzungen erfüllt sind.

[65] In der mündlichen Verhandlung haben die Staatsanwaltschaft (Bozen) und die italienische Regierung unterschiedliche Ansichten zur Rolle des nationalen Gerichts und zum Umfang der vorherigen Kontrolle nach Art. 132 Abs. 3 des gesetzesvertretenden Dekrets Nr. 196/2003 geäußert. Während die Staatsanwaltschaft (Bozen) meinte, das nationale Gericht müsse vor der Gewährung des Zugangs zu diesen Daten konkret eine Verhältnismäßigkeitsprüfung durchführen, betonte die italienische Regierung, dass das vorlegende Gericht gemäß Art. 101 der Costituzione della Repubblica Italiana (Verfassung der Italienischen Republik) und Art. 1 des Strafgesetzbuchs an das Legalitätsprinzip gebunden sei und daher keine – von ihr als kreativ bezeichnete – Auslegung des Gesetzes vornehmen dürfe. Die Auslegung der einschlägigen Bestimmungen des nationalen Rechts ist Sache des vorlegenden Gerichts.

[66] Außer wenn das nationale Recht dies zulässt und vorbehaltlich der Beachtung u. a. von Art. 49 der Charta.

[67] Eine Freiheitsstrafe im Höchstmaß von mindestens drei Jahren.

Einstufung des schweren Diebstahls als „schwere Straftat“ im Sinne des nationalen Rechts in Frage zu stellen. Wird der im nationalen Recht festgelegte Strafrahmen nicht erreicht, darf das vorlegende Gericht daher keinen Zugang zu den gewünschten Daten gewähren [68].

42. Wird der vom nationalen Gesetzgeber festgelegte Strafrahmen erreicht, muss das vorlegende Gericht nach Art. 15 Abs. 1 der Richtlinie 2002/58 unter Berücksichtigung aller Umstände des konkreten Falles prüfen, ob der mit der Erleichterung des Zugangs zu sensiblen Daten verbundene Eingriff in die Grundrechte in einem angemessenen Verhältnis zu dem im öffentlichen Interesse liegenden Ziel der Bekämpfung dieser Straftat steht. Das vorlegende Gericht muss insoweit alle relevanten Rechte und Interessen berücksichtigen und abwägen, wozu u. a. die Beeinträchtigung der durch Art. 17 der Charta geschützten Eigentumsrechte der Opfer sowie der Umstand gehören, dass Mobiltelefone hochsensible Informationen über das private und berufliche Leben sowie die finanziellen Verhältnisse ihrer Besitzer enthalten können [69]. Der Zugang zu den betreffenden Daten kann das einzige wirksame Mittel sein, um die fraglichen Straftaten zu ermitteln und zu verfolgen und um sicherzustellen, dass die noch unbekannten Täter nicht straffrei ausgehen. Auch die Rechte Dritter [70] sind zu berücksichtigen.

43. Was die Rechte Dritter anbelangt, so ergibt sich [71] aus den Akten des vorlegenden Gerichts, dass die Staatsanwaltschaft (Bozen) Zugang zu den Kommunikationsdaten der gestohlenen Mobiltelefone ab dem 29. Oktober 2021 für den ersten, am 27. Oktober 2021 begangenen Diebstahl [72] und ab dem 20. November 2021 für den zweiten, an diesem Tag begangenen Diebstahl [73] beantragt hat. Diese Zeitangaben zeigen, dass die Anträge auf Datenzugang nur in sehr geringem Maß die namentlich durch die Art. 7, 8 und 11 der Charta garantierten Rechte der Opfer beeinträchtigen [74]. Die italienische Regierung hat in ihren schriftlichen Erklärungen zudem darauf hingewiesen, dass das nationale Verfahren ausschließlich zur Identifizierung des/der Täter(s) der fraglichen Diebstähle geeignete Daten betreffe. Für den Fall, dass Anrufe an Dritte oder von Dritten, die nichts mit dem Diebstahl zu tun hätten, identifiziert würden, erfolge die Vernichtung dieser Daten gemäß Art. 269 der Strafprozessordnung [75]. Schließlich sieht Art. 132 Abs. 3-quater des gesetzesvertretenden Dekrets Nr. 196/2003 vor, dass unter Verstoß gegen Abs. 3 oder Abs. 3-bis erlangte Daten nicht verwendet werden dürfen [76].

[68] Nach Art. 52 Abs. 1 der Charta muss jede Einschränkung der Ausübung eines Rechts gesetzlich vorgesehen sein. Dies bedeutet, dass die nationalen Gerichte grundsätzlich an nationale Regelungen gebunden sind, die solche Einschränkungen enthalten.

[69] Mobiltelefone können Fotos, Gesundheitsdaten, Kontoauszüge, Passwörter usw. enthalten. Der Diebstahl eines Mobiltelefons kann daher die digitale Identität seines Besitzers gefährden, und seine Konsequenzen können den Verlust des Geldwerts erheblich übersteigen. Das vorlegende Gericht sollte daher auch eine mögliche Verletzung der Rechte des Opfers u. a. aus den Art. 7, 8 und 17 der Charta in Betracht ziehen und abwägen.

[70] Wie etwa der Opfer der mutmaßlichen Straftat.

[71] Vorbehaltlich einer Überprüfung durch das vorlegende Gericht.

[72] Aktenzeichen RGNR 9228/2021.

[73] Aktenzeichen RGNR 9794/2021.

[74] Die Daten können sich zwar auf Nachrichten an das Opfer nach dem Zeitpunkt des Diebstahls beziehen, keineswegs aber auf Nachrichten des Opfers oder auf dessen Standortdaten.

[75] Wie die italienische Regierung ausführt, sieht die anwendbare Fassung von Art. 269 Abs. 2 der Strafprozessordnung vor, dass „… die Aufzeichnungen so lange aufbewahrt [werden], bis … das Urteil rechtskräftig geworden ist. … jedoch … können die betroffenen Personen zum Schutz der Vertraulichkeit die Vernichtung der nicht zu den Akten genommenen Aufzeichnungen bei dem Richter, der ihre Aufbewahrung genehmigt oder bestätigt hat, beantragen“ (da sie unerheblich sind). Während der Zugang zu den Daten unschuldiger Dritter unbeschränkt ist, scheint die Verwendung dieser Daten, vorbehaltlich einer Überprüfung durch das vorlegende Gericht, durch das nationale Recht eingeschränkt zu sein.

[76] Im Vorabentscheidungsersuchen wird weder die genaue Bedeutung dieser Bestimmung noch ihre Anwendung in der Praxis erläutert.

VI. Ergebnis

44. Nach alledem schlage ich dem Gerichtshof vor, die Frage des Tribunale di Bolzano (Landesgericht Bozen, Italien) wie folgt zu beantworten:

Art. 15 Abs. 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 geänderten Fassung und die Art. 7, 8, und 11 sowie Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union

sind dahin auszulegen, dass sie einer nationalen Regelung nicht entgegenstehen, wonach ein Gericht verpflichtet ist, der Staatsanwaltschaft Zugang zu den von den Betreibern elektronischer Kommunikationsdienste rechtmäßig gespeicherten Daten zu gestatten, aus denen genaue Schlüsse auf das Privatleben eines Nutzers gezogen werden können, sofern diese Daten für die Zwecke der Aufklärung des Sachverhalts relevant sind und hinreichende Anhaltspunkte für die Begehung einer schweren Straftat im Sinne des nationalen Rechts vorliegen, die mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren bedroht ist. Vor der Gewährung des Zugangs muss das nationale Gericht im Einzelfall konkret prüfen, ob der mit der Gewährung dieses Zugangs verbundene Eingriff in die Grundrechte in Anbetracht u. a. der Schwere der spezifischen Straftat und des jeweiligen Sachverhalts verhältnismäßig ist.