Sammlung der Rechtsprechung

SCHLUSSANTRÄGE DES GENERALANWALTS
MANUEL CAMPOS SÁNCHEZ-BORDONA
vom 20. April 2023[1]

**Rechtssache C-548/21**

**C. G.**
**gegen**
**Bezirkshauptmannschaft Landeck**

(Vorabentscheidungsersuchen des Landesverwaltungsgerichts Tirol [Österreich])

„Vorlage zur Vorabentscheidung – Telekommunikation – Schutz personenbezogener Daten – Richtlinie (EU) 2016/680 – Strafverfahren – Versuchter Zugang der Behörden zu Daten, die auf einem Mobiltelefon gespeichert sind, ohne Genehmigung eines Gerichts oder einer unabhängigen Verwaltungsbehörde“

1. Das vorliegende Vorabentscheidungsersuchen betrifft im Wesentlichen die Bedingungen, die die Polizeibehörden beim Zugang zu Daten erfüllen müssen, die auf dem Mobiltelefon einer Person, gegen die ein strafrechtliches Ermittlungsverfahren geführt wird, gespeichert sind.

2. Wie ich erläutern werde, weist das Vorabentscheidungsersuchen in Bezug auf seine Zulässigkeit deutliche Mängel auf. Sollte der Gerichtshof dennoch beschließen, sich mit dem Vorabentscheidungsersuchen in der Sache zu befassen, wird er über den Anwendungsbereich der Richtlinie 2002/58/EG[2] und der Richtlinie (EU) 2016/680[3] zu entscheiden haben.

1 Originalsprache: Spanisch.

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).

3 Richtlinie des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. 2016, L 119, S. 89).

## I. Rechtlicher Rahmen

### *A. Unionsrecht*

#### *1. Verordnung (EU) 2016/679*[4]

3. Art. 2 („Sachlicher Anwendungsbereich“) Abs. 2 bestimmt:

„Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten

…

d) durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.“

#### *2. Richtlinie 2016/680*

4. Im zweiten Erwägungsgrund heißt es:

„Die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollten gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten … gewahrt bleiben. Diese Richtlinie soll zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts beitragen.“

5. Der 46. Erwägungsgrund lautet:

„Jede Einschränkung der Rechte der betroffenen Person muss mit der Charta und mit der EMRK in der Auslegung durch die Rechtsprechung des Gerichtshofs bzw. des Europäischen Gerichtshofs für Menschenrechte[5] vereinbar sein und insbesondere den Wesensgehalt dieser Rechte und Freiheiten achten.“

6. Im 49. Erwägungsgrund heißt es:

„Werden personenbezogene Daten im Zusammenhang mit strafrechtlichen Ermittlungen und Gerichtsverfahren in Strafsachen verarbeitet, so sollten die Mitgliedstaaten vorsehen können, dass die Ausübung des Rechts auf Unterrichtung, Auskunft, Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung nach Maßgabe des einzelstaatlichen Strafverfahrensrechts erfolgt.“

7. Art. 1 („Gegenstand und Ziele“) sieht vor:

„(1) Diese Richtlinie enthält Bestimmungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der

[4] Verordnung des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. 2016, L 119, S. 1).

[5] Im Folgenden: EGMR.

Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

(2) Gemäß dieser Richtlinie haben die Mitgliedstaaten

a) die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere deren Recht auf Schutz personenbezogener Daten, zu schützen und

…

(3) Diese Richtlinie hindert die Mitgliedstaaten nicht daran, zum Schutz der Rechte und Freiheiten der betroffenen Person bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden Garantien festzulegen, die strenger sind als die Garantien dieser Richtlinie."

8. Art. 2 („Anwendungsbereich") Abs. 1 bestimmt:

„Diese Richtlinie gilt für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zu den in Artikel 1 Absatz 1 genannten Zwecken."

9. Art. 3 („Begriffsbestimmungen") legt fest:

„Im Sinne dieser Richtlinie bezeichnet der Ausdruck:

…

2. ‚Verarbeitung' jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

…

7. ‚zuständige Behörde'

   a) eine staatliche Stelle, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zuständig ist, oder

…"

10. Art. 4 („Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten") Abs. 1 bestimmt:

„Die Mitgliedstaaten sehen vor, dass personenbezogene Daten

a) auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden,

b) für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden,

c) dem Verarbeitungszweck entsprechen, maßgeblich und in Bezug auf die Zwecke, für die sie verarbeitet werden, nicht übermäßig sind,

…

e) nicht länger, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht,

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen."

11. Art. 8 („Rechtmäßigkeit der Verarbeitung") lautet:

„(1) Die Mitgliedstaaten sehen vor, dass die Verarbeitung nur dann rechtmäßig ist, wenn und soweit diese Verarbeitung für die Erfüllung einer Aufgabe erforderlich ist, die von der zuständigen Behörde zu den in Artikel 1 Absatz 1 genannten Zwecken wahrgenommenen wird, und auf Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten erfolgt.

(2) Im Recht der Mitgliedstaaten, das die Verarbeitung innerhalb des Anwendungsbereichs dieser Richtlinie regelt, werden zumindest die Ziele der Verarbeitung, die personenbezogenen Daten, die verarbeitet werden sollen, und die Zwecke der Verarbeitung angegeben."

12. Art. 13 („Der betroffenen Person zur Verfügung zu stellende oder zu erteilende Informationen") schreibt vor:

„(1) Die Mitgliedstaaten sehen vor, dass der Verantwortliche der betroffenen Person zumindest die folgenden Informationen zur Verfügung stellt:

…

d) das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde sowie deren Kontaktdaten,

…

(3) Die Mitgliedstaaten können Gesetzgebungsmaßnahmen erlassen, nach denen die Unterrichtung der betroffenen Person gemäß Absatz 2 soweit und so lange aufgeschoben, eingeschränkt oder unterlassen werden kann, wie diese Maßnahme in einer demokratischen Gesellschaft erforderlich und verhältnismäßig ist und sofern den Grundrechten und den berechtigten Interessen der betroffenen natürlichen Person Rechnung getragen wird:

a) zur Gewährleistung, dass behördliche oder gerichtliche Untersuchungen, Ermittlungen oder Verfahren nicht behindert werden,

b) zur Gewährleistung, dass die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden,

c) zum Schutz der öffentlichen Sicherheit,

d) zum Schutz der nationalen Sicherheit,

e) zum Schutz der Rechte und Freiheiten anderer.

…“

13. In Art. 15 („Einschränkung des Auskunftsrechts“) Abs. 1 heißt es:

„Die Mitgliedstaaten können Gesetzgebungsmaßnahmen erlassen, die zu nachstehenden Zwecken das Recht der betroffenen Person auf Auskunft teilweise oder vollständig einschränken, soweit und so lange wie diese teilweise oder vollständige Einschränkung in einer demokratischen Gesellschaft erforderlich und verhältnismäßig ist und den Grundrechten und den berechtigten Interessen der betroffenen natürlichen Person Rechnung getragen wird:

a) Gewährleistung, dass behördliche oder gerichtliche Untersuchungen, Ermittlungen oder Verfahren nicht behindert werden,

b) Gewährleistung, dass die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden,

c) Schutz der öffentlichen Sicherheit,

d) Schutz der nationalen Sicherheit,

e) Schutz der Rechte und Freiheiten anderer.“

14. Art. 27 („Datenschutz-Folgenabschätzung“) lautet:

„(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so sehen die Mitgliedstaaten vor, dass der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchführt.

(2) Die Folgenabschätzung gemäß Absatz 1 trägt den Rechten und den berechtigten Interessen der von der Datenverarbeitung betroffenen Personen und sonstiger Betroffener Rechnung und enthält zumindest eine allgemeine Beschreibung der geplanten Verarbeitungsvorgänge und eine Bewertung der in Bezug auf die Rechte und Freiheiten der betroffenen Personen bestehenden Risiken sowie der geplanten Abhilfemaßnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Richtlinie eingehalten wird.“

15. Art. 28 („Vorherige Konsultation der Aufsichtsbehörde“) bestimmt:

„(1) Die Mitgliedstaaten sehen vor, dass der Verantwortliche oder der Auftragsverarbeiter vor der Verarbeitung personenbezogener Daten in neu anzulegenden Dateisystemen die Aufsichtsbehörde konsultiert, wenn

a) aus einer Datenschutz-Folgenabschätzung gemäß Artikel 27 hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft, oder

b) die Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, Mechanismen oder Verfahren, ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hat.

…“

16. Art. 54 („Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter“) legt fest:

„Die Mitgliedstaaten sehen vor, dass jede betroffene Person unbeschadet eines verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde gemäß Artikel 52 das Recht auf einen wirksamen gerichtlichen Rechtsbehelf hat, wenn sie der Ansicht ist, dass die Rechte, die ihr aufgrund von nach dieser Richtlinie erlassenen Vorschriften zustehen, infolge einer nicht mit diesen Vorschriften im Einklang stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden.“

### *B. Nationales Recht*

17. § 18 der Strafprozessordnung[6] weist der Kriminalpolizei Aufgaben im Dienste der Strafrechtspflege zu (Abs. 1). Die kriminalpolizeilichen Ermittlungen obliegen den Sicherheitsbehörden (Abs. 2). Die Organe des öffentlichen Sicherheitsdienstes versehen den kriminalpolizeilichen Exekutivdienst, der in der Aufklärung und Verfolgung von Straftaten besteht (Abs. 3).

18. Nach § 99 StPO ermittelt die Kriminalpolizei von Amts wegen oder aufgrund einer Anzeige; Anordnungen der Staatsanwaltschaft und des Gerichts hat sie zu befolgen (Abs. 1). Ist für eine Ermittlungsmaßnahme eine Anordnung der Staatsanwaltschaft erforderlich, so kann die Kriminalpolizei diese Befugnis bei Gefahr im Verzug ohne diese Anordnung ausüben. In diesem Fall hat die Kriminalpolizei unverzüglich um Genehmigung anzufragen (Abs. 2).

19. Sollen auf Datenträgern gespeicherte Informationen sichergestellt werden, so hat nach § 111 Abs. 2 StPO jedermann Zugang zu diesen Informationen zu gewähren und auf Verlangen einen elektronischen Datenträger in einem allgemein gebräuchlichen Dateiformat auszufolgen oder herstellen zu lassen. Überdies hat er die Herstellung einer Sicherungskopie der auf den Datenträgern gespeicherten Informationen zu dulden.

## II. Sachverhalt, Rechtsstreit und Vorlagefragen

20. C. G. ist deutscher Staatsbürger und arbeitet und wohnt in Österreich.

[6] Im Folgenden: StPO. BGBl. Nr. 631/1975, in der zum maßgeblichen Zeitpunkt anwendbaren Fassung (BGBl. I 24/2020).

21. Am 23. Februar 2021 beschlagnahmten Beamte des Zollamtes Innsbruck (Österreich) im Zuge einer Suchtmittelkontrolle ein an C. G. adressiertes Paket, in dem sich 85 g Cannabiskraut befanden.

22. Am 6. März 2021 befragten zwei Polizeibeamte C. G. zum Absender des Pakets und durchsuchten seinen Wohnbereich. Bei der Durchsuchung wurde sein Mobiltelefon (mit einer SIM- und einer SD-Karte) sichergestellt, und C. G. wurde ein Sicherstellungsprotokoll übergeben.

23. C. G. wurde aufgefordert, Einsicht in die Verbindungsdaten seines Mobiltelefons zu gewähren und den Zugangscode für das Telefon bekannt zu geben, lehnte beides jedoch ab.

24. Dem Bezirkspolizeikommando Landeck (Österreich) gelang es nicht, die Sperre des Mobiltelefons aufzuheben. Das Mobiltelefon wurde an das Bundeskriminalamt nach Wien (Österreich) übermittelt, und dort wurde abermals erfolglos versucht, das Telefon zu entsperren und die darauf gespeicherten Daten auszulesen.

25. Zu diesem Zeitpunkt lag für die gesetzten Maßnahmen weder eine Anordnung der Staatsanwaltschaft noch ein gerichtlicher Beschluss vor.

26. Am 31. März 2021 erhob C. G. beim Landesverwaltungsgericht Tirol (Österreich) Beschwerde gegen die erfolgte Zwangsmaßnahme, d. h. die Sicherstellung seines Mobiltelefons. Das Telefon wurde am 20. April 2021 an C. G. zurückgegeben.

27. C. G. wurde über die versuchte Auswertung des Inhalts des Mobiltelefons nicht informiert; er erfuhr hiervon erst dadurch, dass der Polizeibeamte, der die Sicherstellung durchgeführt und in weiterer Folge die digitale Auswertung eingeleitet hatte, als Zeuge unter Wahrheitspflicht vernommen wurde. Die versuchte Auswertung wurde auch nicht in der kriminalpolizeilichen Akte dokumentiert.

28. In diesem Zusammenhang hat das Landesverwaltungsgericht Tirol dem Gerichtshof die folgenden Fragen zur Vorabentscheidung vorgelegt:

1. Ist Art. 15 Abs. 1 (allenfalls in Verbindung mit Art. 5) der Richtlinie 2002/58 in der durch die Richtlinie 2009/136/EG geänderten Fassung im Licht der Art. 7 und 8 der Charta dahin auszulegen, dass der Zugang öffentlicher Stellen zu den auf Mobiltelefonen gespeicherten Daten einen Eingriff in deren in diesen Artikeln der Charta verankerte Grundrechte darstellt, der so schwer ist, dass dieser Zugang im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten auf die Bekämpfung der schweren Kriminalität beschränkt werden müsste?

2. Ist Art. 15 Abs. 1 der Richtlinie 2002/58 in der durch die Richtlinie 2009/136 geänderten Fassung im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta der Grundrechte dahin auszulegen, dass er einer nationalen Regelung wie § 18 in Verbindung mit § 99 Abs. 1 Strafprozessordnung entgegensteht, der zufolge Sicherheitsbehörden im Zuge eines strafrechtlichen Ermittlungsverfahrens ohne Genehmigung eines Gerichtes oder einer unabhängigen Verwaltungsstelle sich selbst einen umfassenden und unkontrollierten Zugang zu allen auf einem Mobiltelefon gespeicherten digitalen Daten verschaffen?

3. Ist Art. 47 der Charta allenfalls in Verbindung mit Art. 41 und Art. 52 der Charta der Grundrechte, unter dem Aspekt der Waffengleichheit und dem Aspekt eines wirksamen Rechtsbehelfs so zu verstehen, dass er einer mitgliedstaatlichen Regelung entgegensteht, die wie § 18 in Verbindung mit § 99 Abs. 1 StPO, es ermöglicht, dass ein Mobiltelefon digital ausgewertet wird, ohne dass der Betroffene vorher oder aber zumindest nach Setzung der Maßnahme davon in Kenntnis gesetzt wird?

## III. Verfahren vor dem Gerichtshof

29. Das Vorabentscheidungsersuchen ist am 6. September 2021 beim Gerichtshof eingegangen.

30. Am 20. Oktober 2021 ersuchte der Gerichtshof das vorlegende Gericht, mitzuteilen, ob es die Richtlinie 2016/680 im Ausgangsrechtsstreit für möglicherweise einschlägig hält.

31. Am 11. November 2021 antwortete das vorlegende Gericht, dass die Richtlinie 2016/680 im Ausgangsrechtsstreit anzuwenden sei.

32. Die dänische, die deutsche, die estnische, die französische, die irische, die niederländische, die norwegische, die österreichische, die polnische, die schwedische, die ungarische und die zyprische Regierung sowie die Europäische Kommission haben Erklärungen eingereicht.

33. Alle diese Regierungen mit Ausnahme der deutschen, der polnischen und der ungarischen Regierung sowie die finnische Regierung haben an der mündlichen Verhandlung vom 16. Januar 2023 teilgenommen. Die Teilnehmer am mündlichen Verfahren wurden vom Gerichtshof gebeten, ihre mündlichen Ausführungen auf die Richtlinie 2016/680 zu konzentrieren und in ihren mündlichen Ausführungen auf bestimmte Fragen zu der Richtlinie einzugehen.

## IV. Würdigung

### *A. Unzulässigkeit*

34. In der ursprünglichen Formulierung seiner Vorlagefragen hat das vorlegende Gericht den Gerichtshof lediglich um die Auslegung der Richtlinie 2002/58 ersucht. Nahezu alle Beteiligten stimmen allerdings überein, dass diese Richtlinie auf die vorliegende Rechtssache nicht anwendbar und ihre Auslegung somit für eine Entscheidung in dem Rechtsstreit nicht erforderlich ist.

35. Nach ihrem Art. 3 gilt die Richtlinie 2002/58 für „die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der [Union], einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen“.

36. Der Gerichtshof hat entschieden, dass „[w]enn die Mitgliedstaaten unmittelbar Maßnahmen umsetzen, mit denen von der Vertraulichkeit elektronischer Kommunikationen abgewichen wird, ohne den Betreibern elektronischer Kommunikationsdienste Verarbeitungspflichten aufzuerlegen, … der Schutz der Daten der Betroffenen … nicht unter die Richtlinie 2002/58

[fällt], sondern allein unter das nationale Recht, vorbehaltlich der Anwendung der [Richtlinie 2016/680]“ [7].

37. In der vorliegenden Rechtssache erfolgte der versuchte Zugang zu den Daten direkt durch die Polizeibehörden im Rahmen einer strafrechtlichen Ermittlung. Betreiber elektronischer Kommunikationsdienste waren nicht beteiligt und wurden auch nicht aufgefordert, personenbezogene Daten offenzulegen. Die Richtlinie 2002/58 kommt somit nicht zur Anwendung.

38. Die im vorliegenden Fall einschlägige Vorschrift des Unionsrechts ist die Richtlinie 2016/680, nach deren Art. 2 Abs. 1 sie für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum „Zwecke der … Ermittlung … von Straftaten“ gilt.

39. Die vorstehenden Erwägungen würden ausreichen, um das Vorabentscheidungsersuchen in der Fassung des vorlegenden Gerichts für unzulässig zu erklären, da die Vorschrift des Unionsrechts, um deren Auslegung ersucht wird, auf die Rechtssache nicht zur Anwendung kommt.

40. Nach Art. 267 AEUV kann der Gerichtshof jedoch die ihm zur Vorabentscheidung vorgelegten Fragen umformulieren oder auf die Existenz anderer eventuell einschlägiger Vorschriften des Unionsrechts hinweisen, um dem nationalen Gericht eine sachdienliche Antwort zu geben [8].

41. Der Gerichtshof hat das vorlegende Gericht aufgefordert, mitzuteilen, ob seiner Ansicht nach die Richtlinie 2016/680 zur Anwendung kommt. Er gab ihm also die Möglichkeit, seine Vorlagefragen selbst zu ergänzen bzw. umzuformulieren. Das vorlegende Gericht ist dem jedoch nicht nachgekommen, sondern hat sich darauf beschränkt, festzustellen, dass „[d]ie Vorgaben der Richtlinie (EU) 2016/680 … im hier vorliegenden Sachverhalt jedenfalls beachtlich [sind]“, ohne jedoch die Bestimmungen der Richtlinie zu nennen, auf die sich seine Zweifel beziehen, oder auf weitere materiell-rechtliche Erwägungen einzugehen [9].

42. Nach ständiger Rechtsprechung des Gerichtshofs ist es „nach Art. 94 Buchst. c der Verfahrensordnung unerlässlich, dass die Vorlageentscheidung eine Darstellung der Gründe enthält, aus denen das vorlegende Gericht Zweifel bezüglich der Auslegung oder der Gültigkeit bestimmter Vorschriften des Unionsrechts hat, und den Zusammenhang angibt, den es zwischen diesen Vorschriften und dem auf den Ausgangsrechtsstreit anwendbaren nationalen Recht herstellt“ [10].

43. Aus den vorstehenden Erwägungen ergibt sich, dass die Voraussetzungen von Art. 94 der Verfahrensordnung nicht erfüllt sind. Der Gerichtshof zeigt diesbezüglich zwar eine gewisse Flexibilität, jedoch hat die Zusammenarbeit mit dem vorlegenden Gericht auf Gegenseitigkeit zu beruhen: Mangelt es an einer Kooperation des vorlegenden Gerichts, was die Erläuterung seiner Zweifel hinsichtlich der Auslegung der von ihm für anwendbar gehaltenen

7 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, im Folgenden: Urteil La Quadrature du Net, Rn. 103).

8 Vgl. statt aller Urteil vom 28. April 2016, Oniors Bio (C-233/15, EU:C:2016:305, Rn. 30).

9 Der Gerichtshof sah sich gezwungen, die am mündlichen Verfahren Beteiligten aufzufordern, „die ihrer Ansicht nach einschlägigen Bestimmungen der Richtlinie 2016/680 anzugeben, in deren Licht der Gerichtshof die drei vom vorlegenden Gericht gestellten Fragen gegebenenfalls umformulieren sollte“ (vierte Frage zur Beantwortung in der mündlichen Verhandlung).

10 Urteil vom 6. Oktober 2021, Consorzio Italian Management und Catania Multiservizi (C-561/19, EU:C:2021:799, Rn. 69).

Unionsrechtsvorschriften (im vorliegenden Fall der Richtlinie 2016/680) angeht, ohne dass hierfür ein rechtfertigender Grund erkennbar wäre, erscheint es mir folgerichtig, dass das Vorabentscheidungsersuchen für unzulässig erklärt wird [11].

44. Hinzu kommt, dass das vorlegende Gericht

— weder die Art der von den Polizeibehörden versuchten Verarbeitung noch die Art der personenbezogenen Daten angibt, nach denen konkret gesucht wurde. Anfänglich scheint sich das Gericht auf Verbindungsdaten (d. h. Verkehrs- und Standortdaten) zu beschränken, schließt jedoch später nicht aus, dass die Entsperrung des Telefons Zugang zu „allen … gespeicherten digitalen Daten“ [12] und sogar zum Inhalt der über das Telefon geführten Kommunikation und der elektronischen Nachrichten [13] verschafft;

— sich sowohl auf die Sicherstellung des Telefons und den Zugang bzw. den versuchten Zugang zu den auf dem Telefon gespeicherten Daten als auch auf deren anschließende „Auswertung“, d. h. die Analyse und das Auslesen, bezieht. Diese Auswertung bedeute „den völlig unkontrollierten Zugang zur gesamten digitalen Kommunikation des Betroffenen“, was es ermögliche, „ein sehr detailliertes und tief gehendes Bild aus nahezu allen Bereichen des Privatlebens [zu] rekonstruieren“.

45. Unter diesen Umständen würde der Gerichtshof die Fragen des vorlegenden Gerichts nicht *umformulieren*, sondern vielmehr das Vorabentscheidungsersuchen vollkommen *neu aufsetzen*, das im Übrigen zum Teil auf hypothetischen Erwägungen und nicht auf feststehenden Tatsachen beruhen würde. Bei alldem ist, wie ich betonen möchte, zu berücksichtigen, dass der Gerichtshof dem vorlegenden Gericht zuvor die Möglichkeit gegeben hat, seine Fragen selbst zu ergänzen bzw. umzuformulieren.

46. Meiner Auffassung nach, die von mehreren der beteiligten Mitgliedstaaten vertreten wird, ist das Vorabentscheidungsersuchen daher für unzulässig zu erklären.

47. Die in der mündlichen Verhandlung hervorgehobene Tatsache, dass vor dem Gericht kein wirklicher Rechtsstreit mehr besteht, der die Auslegung von Vorschriften des Unionsrechts erfordert, führt ebenfalls zu dem Schluss, dass das Vorabentscheidungsersuchen für unzulässig zu erklären ist.

48. In der Tat räumt die österreichische Regierung (der die an den Ermittlungen beteiligten Polizeibehörden unterstehen) ein, dass das Vorgehen dieser Behörden rechtswidrig war und die Rechte des Betroffenen verletzt hat. Da sich nach der Vorlageentscheidung die Beschwerde des Beschwerdeführers vor dem Verwaltungsgericht gerade gegen die polizeilichen Maßnahmen richtete, die von der belangten Behörde als rechtswidrig angesehen werden, ist der Streitgegenstand, über den das vorlegende Gericht zu entscheiden hat, weggefallen.

49. Für den Fall, dass der Gerichtshof einen anderen Standpunkt vertritt, werde ich im Folgenden, hilfsweise, auf die materiell-rechtlichen Fragen eingehen, die den Vorlagefragen zugrunde liegen.

[11] Ich stimme insoweit mit der französischen Regierung überein (Rn. 36 bis 41 ihrer schriftlichen Erklärungen).

[12] So in der zweiten Vorlagefrage.

[13] Das vorlegende Gericht führt aus, dass „hinsichtlich der Verbindungsdaten … sich nahezu alle Kontakte nach Häufigkeit, Zeit und Dauer der Kommunikation, hinsichtlich mittels SMS und anderen Messengerdiensten geführter Kommunikation auch der Inhalt rekonstruieren [lassen]; auch durch die Auswertung von gespeicherten Lichtbildern und Browserverläufen erfolgt ein sehr intimer Einblick in das Privatleben des Betroffenen“.

50. Zunächst ist meiner Ansicht nach jedoch das Vorliegen eines weiteren Unzulässigkeitsgrundes auszuschließen, der von einigen Beteiligten im Verfahren vorgebracht wird [14]. Sie vertreten den Standpunkt, die Richtlinie 2016/680 gelte, da sie dem Schutz natürlicher Personen bei der *Verarbeitung* ihrer Daten diene, nicht für Fälle wie den vorliegenden, in denen keine Verarbeitung stattgefunden habe, sondern lediglich ein *versuchter Zugang* zu den Daten, der jedoch keinen Erfolg gehabt habe.

51. Nach Auffassung der Kommission ist hingegen im Hinblick auf die praktische Wirksamkeit der Richtlinie 2016/680 ihr Gegenstand dahin auszulegen, dass er sich nicht nur auf die Verarbeitung selbst beschränkt, sondern auch Angelegenheiten in direktem Zusammenhang mit einer solchen Verarbeitung umfasst. Hierzu zähle auch der versuchte Zugang zu den Daten, deren Verarbeitung beabsichtigt werde [15].

52. Meines Erachtens ist, ohne die Grenzen des Anwendungsbereichs der Richtlinie 2016/680 strapazieren zu müssen [16], ihre Anwendung auf den vorliegenden Fall nicht deshalb gerechtfertigt, weil das Mobiltelefon sichergestellt wurde [17], sondern weil die Polizeibehörden im Anschluss versuchten, bestimmte personenbezogene Daten des Betroffenen zu erlangen, wozu sie das Mobiltelefon zu entsperren und auf seinen Inhalt zuzugreifen versuchten.

53. Nach Art. 3 Abs. 2 der Richtlinie 2016/680 bezeichnet der Begriff „Verarbeitung“ jede „andere Form der Bereitstellung“ von personenbezogenen Daten, die im Rahmen einer strafrechtlichen Ermittlung erfolgt. Meines Erachtens führt eine Polizeibehörde, die ein Telefon sicherstellt, auf dem solche Daten gespeichert sind, und daran hantiert, um auf die Daten zuzugreifen, einen „Verarbeitungsvorgang“ durch, auch wenn dieser aus technischen Gründen infolge der Verschlüsselung erfolglos bleibt.

54. Der erfolglose Versuch, im Rahmen einer strafrechtlichen Ermittlung auf die auf einem Mobiltelefon gespeicherten personenbezogenen Daten zuzugreifen, richtet sich aus ähnlichen Gründen nach der Richtlinie 2016/680 wie denen, die den Gerichtshof zu der Entscheidung veranlasst haben, dass die Richtlinie 2002/58 auf den (ebenfalls erfolglosen) *Versuch* anwendbar ist, eine gerichtliche Erlaubnis zum Zugang zu bestimmten von einem Betreiber elektronischer Kommunikationsdienste gespeicherten Daten einer Person, gegen die ermittelt wird, zu erhalten [18].

55. Insoweit könnte die Würdigung durch das vorlegende Gericht, sofern es über die Rechtswidrigkeit der polizeilichen Maßnahme zu entscheiden hätte (die von der österreichischen Regierung jedoch, wie oben dargestellt, anerkannt wird), von der Rechtmäßigkeit des mit der Maßnahme verfolgten Zwecks abhängen, und zwar sowohl, wenn die Maßnahme erfolgreich war, als auch, wenn sie nur erfolglos versucht wurde.

[14] Ich beziehe mich konkret auf die französische, die niederländische, die norwegische und die österreichische Regierung.

[15] Nach Meinung der Kommission ist es „unerheblich, ob die Zugriffsversuche letztlich erfolgreich waren oder nicht. Das Auftreten technischer Schwierigkeiten, die den erfolgreichen Abschluss der Zugriffsversuche verhindern, ist ein Umstand, der nicht im Voraus bekannt sein kann und die Risiken für den Schutz personenbezogener Daten nicht berührt.“

[16] Insbesondere der Rückgriff auf die Art. 27 und 28 der Richtlinie 2016/680, wie die Kommission ihn in ihren schriftlichen Erklärungen vorschlägt, ist meiner Meinung nach unnötig. Die in Art. 27 vorgesehene „Datenschutz-Folgenabschätzung“ bezieht sich allgemein auf „eine Form der Verarbeitung“ und nicht auf konkrete oder spezielle Verarbeitungsvorgänge. Dies ergibt sich aus dem 58. Erwägungsgrund der Richtlinie 2016/680: „Datenschutz-Folgenabschätzungen sollten auf maßgebliche Systeme und Verfahren im Rahmen von Verarbeitungsvorgängen abstellen, *nicht jedoch auf Einzelfälle*“ (Hervorhebung nur hier). In der mündlichen Verhandlung hat die Kommission ihre Bezugnahme auf die beiden Bestimmungen relativiert und erklärt, sie habe diese nur angeführt, um zu zeigen, dass die Richtlinie 2016/680 auch Situationen abdecke, die der eigentlichen Datenverarbeitung vorausgingen.

[17] Die Richtlinie 2016/680 regelt nicht die Sicherstellung eines Telefons als Beweismittel im Rahmen einer strafrechtlichen Ermittlung.

[18] Urteil vom 2. Oktober 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788).

## *B. Zur Beantwortung der Fragen*

### *1. Erste Vorlagefrage*

56. Das vorlegende Gericht möchte wissen, ob nach Art. 15 Abs. 1 (eventuell in Verbindung mit Art. 5) der Richtlinie 2002/58 und im Licht der Art. 7 und 8 der Charta „der Zugang öffentlicher Stellen zu den auf Mobiltelefonen gespeicherten Daten einen Eingriff in deren in diesen Artikeln der Charta verankerte Grundrechte darstellt, der so schwer ist, dass dieser Zugang im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten auf die Bekämpfung der schweren Kriminalität beschränkt werden müsste“.

57. Sollte das Vorabentscheidungsersuchen zulässig sein, müsste die erste Vorlagefrage aufgrund der Unanwendbarkeit der Richtlinie 2002/58 so umformuliert werden, dass der Gerichtshof in seiner Antwort die Richtlinie 2016/680 auslegt.

58. In der Antwort des Gerichtshofs sollte nacheinander geklärt werden, ob in einem Fall wie dem vorliegenden von einem Eingriff gesprochen werden kann, und, falls ein Eingriff vorliegt, ob die Richtlinie 2016/680 vorschreibt, dass der Zugang zu den Daten auf Fälle der Bekämpfung schwerer Straftaten zu beschränken ist.

59. Die Verarbeitung personenbezogener Daten kann definitionsgemäß in das Recht auf Achtung des Privatlebens (Art. 7 der Charta) und das Recht auf den Schutz personenbezogener Daten (Art. 8 der Charta) eingreifen. Die Behörden müssen daher die in Art. 52 Abs. 1 der Charta festgeschriebenen Bedingungen erfüllen, um ein Eingreifen in die Ausübung dieser Grundrechte rechtfertigen zu können.

60. Der Eingriff in die durch die Art. 7 und 8 der Charta geschützten Rechte ist umso schwerwiegender, wenn mit ihm a) der Zugang zu sensiblen Daten beabsichtigt wird, wie sie gewöhnlich auf Mobiltelefonen gespeichert werden und die Bereiche des Lebens ihrer Besitzer offenbaren können, die vor der Offenlegung gegenüber Dritten zu schützen sind, und b) der Zugang zum Inhalt der Mitteilungen ermöglicht wird.

61. Allgemein betrachtet und unter Berücksichtigung ihres Inhalts kann die Richtlinie 2016/680 jedoch nicht dahin ausgelegt werden, dass die Datenverarbeitung, auf die sie sich bezieht, allein auf Fälle der Bekämpfung schwerer Straftaten zu beschränken sei.

62. Die Richtlinie 2016/680 bezieht sich vielmehr auf jeglichen Vorgang der Verarbeitung[19] personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung *aller Arten* von Straftaten.

63. Den in der Richtlinie 2016/680 festgelegten Grundsätzen für die Verarbeitung personenbezogener Daten zu diesen Zwecken (Art. 4) und den Voraussetzungen für die Rechtmäßigkeit der Verarbeitung (Art. 8) lässt sich nicht entnehmen, dass die Verarbeitung von Daten regelmäßig nur in Fällen schwerer Straftaten zulässig wäre.

[19] Die Art der „Vorgänge“ ist in Art. 3 Abs. 2 der Richtlinie 2016/680 sehr weit gefasst. Vgl. den Wortlaut von Art. 3 Abs. 2 in Nr. 9 der vorliegenden Schlussanträge.

64. Eine Beschränkung auf Fälle der Bekämpfung schwerer Straftaten lässt sich auch nicht damit begründen, dass die Rechtsprechung des Gerichtshofs zur Richtlinie 2002/58 [20] ohne Weiteres auf Fälle wie den vorliegenden zu übertragen sei.

65. Eine Übertragung ist meines Erachtens deshalb nicht möglich, weil sich diese Rechtsprechung, unbeschadet dessen, was ich im Folgenden ausführen werde, auf eine allgemeine und unterschiedslose Speicherung personenbezogener Daten einer allgemeinen und unbestimmten Gruppe bezieht, die von den Betreibern elektronischer Kommunikationsdienste systematisch durchgeführt wird. Die Schwere des Eingriffs, den diese Art der Speicherung für die Gesellschaft als Ganzes darstellt, erklärt, warum der Gerichtshof hinsichtlich ihres Verbots und der Festlegung der Ausnahmen von diesem Verbot besonders streng ist.

66. Anders liegt der Fall, wenn der beabsichtigte Zugang nicht die gesamte Bevölkerung bzw. einen großen Teil von ihr (d. h. die personenbezogenen Daten einer allgemeinen und unbestimmten Gruppe) betrifft, sondern die auf einem einzelnen Mobiltelefon gespeicherten Informationen im Rahmen eines einzelnen strafrechtlichen Ermittlungsverfahrens, auf das speziell die Richtlinie 2016/680 zur Anwendung kommt.

67. Gegenstand der Richtlinie 2016/680 ist gerade die Verarbeitung von Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, und zwar aller Arten von Straftaten und nicht nur von schweren Straftaten.

68. Wie einige Beteiligte des Vorabentscheidungsverfahrens hervorgehoben haben, wäre zudem mangels Angaben zur Schwere von Straftaten in der Richtlinie 2016/680 eine einheitliche Anwendung der Richtlinie in den Mitgliedstaaten unmöglich, da die Schwere von strafbaren Handlungen im nationalen Recht der einzelnen Mitgliedstaaten sehr unterschiedlich bewertet wird [21].

69. Im Ergebnis setzt die Richtlinie 2016/680 für die Rechtmäßigkeit der von ihr geregelten Verarbeitung personenbezogener Daten nicht voraus, dass sie zum Zweck der Bekämpfung schwerer Straftaten erfolgt.

70. Dies gilt unbeschadet der Tatsache, dass in Anwendung des Grundsatzes der Verhältnismäßigkeit und im Einzelfall die von den zuständigen Behörden gemäß der Richtlinie 2016/680 beabsichtigte Datenverarbeitung in einem angemessenen Verhältnis zu erfolgen hat zu: a) der Art der verfolgten Straftaten und b) der Art der verarbeiteten personenbezogenen Daten.

71. Insoweit stimme ich dem Standpunkt der deutschen Regierung über die Beschränkung des Zugangs zu Daten von sichergestellten Mobiltelefonen zu, wenn mit ihnen anhand sämtlicher digitaler Inhalte ein umfassendes Persönlichkeitsprofil der Betroffenen erstellt werden kann. Nach Auffassung der deutschen Regierung ist der Zugang auf Daten zu beschränken, die im

[20] Urteile La Quadrature du Net sowie vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970, im Folgenden: Urteil Tele2 Sverige und Watson), vom 2. Oktober 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788), vom 6. Oktober 2020, Privacy International (C-623/17, EU:C:2020:790), und 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).

[21] Die französische Regierung führt als Beispiel die Straftatbestände des Betäubungsmittelbesitzes und des Betäubungsmittelhandels an, deren Schwere im österreichischen Recht anders beurteilt wird als im französischen Recht. Einen ähnlichen Standpunkt vertritt die schwedische Regierung.

konkreten Einzelfall als Beweismittel erforderlich sind, und kann bei Vorliegen von Faktoren wie „die Geringfügigkeit der zu ermittelnden Straftat oder eine geringe Beweisbedeutung der zu beschlagnahmenden Daten“ unzulässig sein [22].

72. *Abstrakt* ist nach der Richtlinie 2016/680 der Zugang zu auf einem Mobiltelefon gespeicherten personenbezogenen Daten zu dem Zweck, bezüglich Handlungen zu ermitteln, die zu den allgemeinen oder häufigeren Straftaten zählen, somit nicht von vornherein rechtswidrig. Ob ein solcher Zugang *konkret* zulässig ist, hat die zuständige Behörde im Einzelfall und unter Berücksichtigung der Erforderlichkeit und des Kriteriums der Verhältnismäßigkeit, auf das ich vorstehend verwiesen habe, zu beurteilen.

73. Dies geht meines Erachtens aus den Bestimmungen der Richtlinie 2016/680 über die Bedingungen für die Zulässigkeit der Verarbeitung personenbezogener Daten im Rahmen der Bekämpfung von Straftaten hervor, und zwar konkret aus:

— Art. 4 Abs. 1 Buchst. a, wonach die Daten „auf rechtmäßige Weise … verarbeitet werden“ müssen, und

— Art. 8 Abs. 1, in dem hervorgehoben wird, dass die Verarbeitung *erforderlich* sein und auf Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten erfolgen muss.

*2. Zweite Vorlagefrage*

74. Mit der zweiten Vorlagefrage möchte das vorlegende Gericht klären, ob Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8, 11 sowie von Art. 52 Abs. 1 der Charta „einer nationalen Regelung wie § 18 in Verbindung mit § 99 Abs. 1 [StPO] entgegensteht, der zufolge Sicherheitsbehörden im Zuge eines strafrechtlichen Ermittlungsverfahrens ohne Genehmigung eines Gerichts oder einer unabhängigen Verwaltungsstelle sich selbst einen umfassenden und unkontrollierten Zugang zu allen auf einem Mobiltelefon gespeicherten digitalen Daten verschaffen“.

75. Der Wortlaut der Frage ist nicht ganz eindeutig. Das vorlegende Gericht

— erkennt an, dass nach § 110 Abs. 2 StPO für die Sicherstellung von Gegenständen grundsätzlich eine Anordnung der Staatsanwaltschaft erforderlich ist. Ohne eine solche Anordnung kann die Polizeibehörde eine Sicherstellung nur unter den in § 110 Abs. 3 vorgesehenen außergewöhnlichen Umständen durchführen (die im vorliegenden Fall nicht vorzuliegen scheinen);

— fügt allerdings hinzu, dass die Auswertung von auf Mobiltelefonen gespeicherten Informationen in der StPO „nicht abschließend geregelt“ sei und von den Sicherheitsbehörden auf eigene Initiative und ohne vorherige Anordnung durchgeführt werden könne.

76. Die österreichische Regierung stellt die nationale Regelung anders dar als das vorlegende Gericht. Insbesondere weist sie darauf hin, dass nach den nationalen Rechtsvorschriften sowohl die Sicherstellung des Telefons (mit der Ausnahme von Eilfällen) als auch die Auswertung der

[22] Schriftliche Erklärungen der deutschen Regierung, Rn. 20.

darauf gespeicherten Daten nur mit Anordnung der Staatsanwaltschaft zulässig sei [23]. Ohne die Anordnung der Staatsanwaltschaft sei die Auswertung der auf dem Telefon gespeicherten Daten durch die Polizei unzulässig.

77. Die Auslegung der nationalen Rechtsvorschriften ist Sache des vorlegenden Gerichts. Im Rahmen des Verfahrens nach Art. 267 AEUV ist der Gerichtshof nicht zur Auslegung des nationalen Rechts befugt, und allein das nationale Gericht ist dafür zuständig, die genaue Bedeutung der nationalen Rechts- oder Verwaltungsvorschriften zu bestimmen [24].

78. Ohne auf die Frage der korrekten Auslegung der österreichischen Rechtsvorschriften eingehen zu wollen, kann ich allein aus den vom vorlegenden Gericht genannten Vorschriften (§ 18 StPO in Verbindung mit § 99 Abs. 1 StPO) nur schwer die von ihm dargestellte Folge ableiten. Jedoch kann hierüber, wie ich wiederholen möchte, nur das vorlegende Gericht entscheiden.

79. Auf jeden Fall ist das vorlegende Gericht der Auffassung, dass die Rechtsprechung aus dem Urteil Prokuratuur [25] über die vorherige Kontrolle des Zugangs zu den gespeicherten Daten durch ein Gericht oder eine unabhängige Verwaltungsstelle auf einen Fall wie den vorliegenden übertragen werden könne.

80. Nach Ansicht der niederländischen Regierung hingegen betrifft dieses Urteil eine nationale Regelung, die den *allgemeinen* Zugang der zuständigen Behörden zu *allen* gespeicherten Verkehrs- und Standortdaten regelt. Dies erkläre das Erfordernis einer vorherigen gerichtlichen Anordnung, das jedoch im Fall des Zugangs zu den Daten eines einzelnen Mobiltelefons nicht gerechtfertigt sei.

81. Ebenso macht die norwegische Regierung geltend, dass die Richtlinie 2016/680 zwar eine ganze Reihe Garantien vorsehe [26], jedoch nicht ausdrücklich zu einer vorherigen Genehmigung durch ein Gericht oder eine unabhängige Verwaltungsstelle verpflichte.

82. Ausgehend von der Prämisse, dass die Bestimmungen der Richtlinie 2016/680 im Licht der Charta auszulegen seien, stellt die Kommission fest, die Mitgliedstaaten hätten infolge der ihnen durch Art. 8 Abs. 1 der Richtlinie auferlegten Verpflichtung (Bedingungen für die Rechtmäßigkeit der Verarbeitung) die durch die Art. 7 und 8 der Charta garantierten Grundrechte zu achten.

83. Ich stimme mit der Kommission darin überein, dass der nationale Gesetzgeber unter Beachtung dieser Bestimmungen der Charta verpflichtet ist, die erforderlichen Regeln festzulegen, um sicherzustellen, dass jeglicher Zugang zu den Daten gerechtfertigt ist und auf das Erforderliche und Verhältnismäßige beschränkt bleibt.

[23] Rn. 19 der schriftlichen Erklärungen der österreichischen Regierung. Sie verweist auf die Entscheidung des Obersten Gerichtshofs (Österreich) vom 13. Oktober 2020 (Rechtssache 11 Os 56/20z), wonach die Auswertung von Daten, die sich auf einem Mobiltelefon befinden, durch die Kriminalpolizei ohne entsprechende Anordnung durch die Staatsanwaltschaft einen Verstoß gegen die subjektiven Rechte der betroffenen Person darstelle und damit rechtswidrig sei.

[24] Vgl. statt aller Urteil vom 28. April 2022, SeGEC u. a. (C-277/21, EU:C:2022:318, Rn. 21).

[25] Urteil Prokuratuur (Rn. 51): „[E]s [ist] unabdingbar, dass der Zugang der zuständigen nationalen Behörden zu den gespeicherten Daten einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird und dass dessen oder deren Entscheidung auf einen mit Gründen versehenen, von den zuständigen nationalen Behörden insbesondere im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten gestellten Antrag ergeht“.

[26] Neben den Garantien aus Art. 4 und 8 die in den Kapiteln III („Rechte der betroffenen Person“), IV („Verantwortlicher und Auftragsverarbeiter“), VI („Unabhängige Aufsichtsbehörden“) und VIII („Rechtsbehelfe, Haftung und Sanktionen“) enthaltenen Garantien.

84. Diese nationalen Vorschriften müssen sich jedoch nicht speziell auf den Zugang zu personenbezogenen Daten beziehen, die, wie im vorliegenden Fall, auf einem Mobiltelefon gespeichert sind, sondern es kann sich auch um nationale Vorschriften handeln, die allgemein die Beweisaufnahme regeln.

85. Insoweit habe ich bereits Rn. 103 des Urteils La Quadrature du Net bezüglich der Maßnahmen der Mitgliedstaaten wiedergegeben, mit denen von der Vertraulichkeit elektronischer Kommunikationen abgewichen wird, ohne den Betreibern elektronischer Kommunikationsdienste Verarbeitungspflichten aufzuerlegen [27].

86. Es sind somit aus der Richtlinie 2016/680 keine *spezifischen* Verfahrensregeln, die die Rechtmäßigkeit des Zugangs zu den auf einem Mobiltelefon gespeicherten Daten gewährleisten, abzuleiten [28], sondern es gelten die nationalen Rechtsvorschriften zur Regelung von Durchsuchungen und Sicherstellungen im Rahmen strafrechtlicher Ermittlungen [29].

87. Der Verweis auf die nationalen Rechtsvorschriften, um die Rechtmäßigkeit des Zugangs gemäß der Richtlinie 2016/680 zu gewährleisten, steht im Übrigen im Einklang mit der Rechtsprechung des EGMR. In einem Fall, der die Republik Österreich im Zusammenhang mit Art. 8 EMRK (Recht auf Achtung des Privat- und Familienlebens, der Wohnung und der Korrespondenz) betrifft, hat der EGMR festgestellt, dass die österreichischen Rechtsvorschriften über die Sicherstellung von Gegenständen, insbesondere von Dokumenten, auf die Durchsuchung und Sicherstellung von auf Datenträgern gespeicherten Daten anwendbar sind [30].

88. Wenn, wie die österreichische Regierung unter Verweis auf die Rechtsprechung des Obersten Gerichtshofs feststellt, die Polizeibehörden ohne Anordnung durch die Staatsanwaltschaft nicht berechtigt sind, auf die auf einem bestimmten Mobiltelefon gespeicherten Daten zuzugreifen, verliert die zweite Vorlagefrage weitgehend an Bedeutung.

89. Auf jeden Fall kann bei der Antwort auf diese Frage nicht ausgeschlossen werden, dass sich infolge des Zugangs zu den auf dem sichergestellten Telefon gespeicherten personenbezogenen Daten „ein sehr detailliertes und tief gehendes Bild aus nahezu allen Bereichen des Privatlebens [des Betroffenen] rekonstruieren“ lässt [31]. Sollte dies der Fall sein, müssen die Polizeibehörden über die im Urteil Prokuratuur angeführte vorherige Genehmigung verfügen.

90. Auf den ersten Blick scheint diese Aussage im Widerspruch dazu zu stehen, dass im vorliegenden Fall, wie ich vorstehend dargestellt habe, die Richtlinie 2002/58 (die im Urteil Prokuratuur ausgelegt wird) nicht zur Anwendung kommt. Ich bin jedoch der Überzeugung, dass der Sinn und Zweck jenes Urteils zu der gleichen Lösung führt.

[27] Siehe Nr. 36 der vorliegenden Schlussanträge.

[28] Ein gutes Beispiel für die Schwierigkeiten eines solchen Ansatzes sind die Bemühungen der Kommission in den Rn. 34 bis 39 ihrer schriftlichen Erklärungen, klare und genaue Regeln für die Festlegung von Grenzen und angemessenen Garantien beim Zugang zu auf Mobiltelefonen gespeicherten Daten herauszuarbeiten.

[29] Diese Vorschriften fallen, wie u. a. die dänische und die irische Regierung hervorheben, nicht in den Anwendungsbereich des Unionsrechts, können jedoch dazu dienen, die sich aus dem Unionsrecht ergebenden Erfordernisse zu erfüllen.

[30] EGMR, Urteil vom 16. Oktober 2007, Wieser und Bicos Beteiligungen/Österreich (CE:ECHR:2007:1016JUD007433601, § 54): „Die StPO enthält zwar keine besonderen Vorschriften für die Durchsuchung und Sicherstellung elektronischer Daten, regelt jedoch detailliert die Beschlagnahme von Gegenständen und von Papieren. Nach der gefestigten Rechtsprechung der österreichischen Gerichte sind diese Vorschriften auch auf elektronische Daten anzuwenden.“

[31] Vgl. die Feststellungen des vorlegenden Gerichts, die in Nr. 44 der vorliegenden Schlussanträge wiedergegeben werden.

91. In dem Rechtsstreit, in dem das Urteil Prokuratuur ergangen ist, erfolgte der Zugang zwar durch die Beschaffung von Daten (Metadaten) bei den Betreibern elektronischer Kommunikationsdienste, jedoch ging es wie im vorliegenden Fall um eine einzelne strafrechtliche Ermittlung, die sich gegen eine bestimmte Person richtete. Ziel war es, Daten in Bezug auf „mehrere Telefonnummern und verschiedene Internationale Mobilfunk-Teilnehmerkennungen" zu erheben [32].

92. Im Urteil Prokuratuur lassen sich meines Erachtens zwei Ebenen unterscheiden: a) die Frage, ob eine allgemeine Regelung eines Mitgliedstaats über die allgemeine und unterschiedslose Vorratsspeicherung von im Besitz der Betreiber elektronischer Kommunikationsdienste befindlichen Daten und den anschließenden Zugang zu diesen Daten den Unionsvorschriften entgegensteht, und b) die Frage der vorherigen Kontrolle des Zugangs zu solchen Metadaten im Einzelfall, wenn sie die Erstellung eines genauen Profils des Privatlebens einer Person ermöglichen.

93. Der Umstand, dass sich in der vorliegenden Rechtssache die die Schlüsse auf das Privatleben zulassenden Daten nicht im Besitz der Betreiber elektronischer Kommunikationsdienste befinden und von einem einzigen sichergestellten Telefon erlangt werden bzw. erlangt werden sollen, scheint mir gegenüber dem Sinn und Zweck des im Urteil Prokuratuur angemahnten Erfordernisses einer vorherigen Kontrolle von untergeordneter Bedeutung zu sein.

94. Grundlage der vorherigen Kontrolle ist letztlich der in den Art. 7 und 8 der Charta verankerte Schutz. Die Behörde, die diese Kontrolle durchführt, muss „in der Lage [sein], für einen gerechten Ausgleich zwischen den Interessen, die sich aus den Erfordernissen der Ermittlungen im Rahmen der Kriminalitätsbekämpfung ergeben, und den Grundrechten auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten der Personen, auf deren Daten zugegriffen wird, zu sorgen" [33].

### *3. Dritte Vorlagefrage*

95. Mit der dritten Vorlagefrage möchte das vorlegende Gericht wissen, ob Art. 47 (allenfalls in Verbindung mit den Art. 41 und 52) der Charta einer Regelung wie der österreichischen [34] entgegensteht, die „es ermöglicht, dass ein Mobiltelefon digital ausgewertet wird, ohne dass der Betroffene vorher oder aber zumindest nach Setzung der Maßnahme davon in Kenntnis gesetzt wird".

96. Die so formulierte Frage ist meiner Ansicht nach für die Entscheidung über den Rechtsstreit möglicherweise nicht erforderlich, weil der Betroffene das in Art. 47 der Charta verankerte Recht ausüben konnte, indem er beim vorlegenden Gericht die Erklärung der Nichtigkeit der am sichergestellten Telefon erfolgten polizeilichen Maßnahme beantragt hat, zu der auch die anschließende (und erfolglose) Auswertung der darauf gespeicherten Daten gehörte.

[32] Urteil Prokuratuur (Rn. 17).

[33] Urteil Prokuratuur (Rn. 52).

[34] Auch hier bezieht sich das vorlegende Gericht auf § 18 StPO in Verbindung mit § 99 StPO.

97. In Bezug auf die beiden Zeitpunkte des polizeilichen Handelns ist zu unterscheiden:

— Was die Sicherstellung des Telefons selbst betrifft, so wusste der Betroffene nach den hier vorliegenden Informationen davon und weigerte sich, als das Telefon sichergestellt wurde, den Polizeibehörden den Zugangscode bekannt zu geben.

— Was die versuchte Auswertung der Daten betrifft, scheint der für die Verarbeitung Verantwortliche den Betroffenen nicht über diese Maßnahme informiert zu haben, obwohl die österreichische Regierung angibt, der Betroffene hätte Einsicht in einen Bericht über die am Telefon erfolgten Maßnahmen der Kriminalpolizei gehabt [35].

98. Hinsichtlich der Auswertung der Daten und der Kenntnis des Betroffenen hiervon verbleiben somit gewisse Unklarheiten, die das vorlegende Gericht, wie ich bereits festgestellt habe, in der Vorlageentscheidung hätte klären müssen und die eine sachdienliche Antwort auf die dritte Vorlagefrage unmöglich machen.

99. Für den Fall, dass der Gerichtshof diese Frage für zulässig hält, werde ich mich dazu äußern. In diesem Fall, und da die Richtlinie 2002/58 nicht zur Anwendung kommt, müsste die Vorlagefrage jedoch im Licht der Richtlinie 2016/680 umformuliert werden, da ihre Art. 13, 15 und 54 Anhaltspunkte für die Beantwortung der Frage liefern.

100. Gemäß der Richtlinie 2016/680 sind dem Betroffenen die Informationen über die Verarbeitung seiner Daten zur Verfügung zu stellen, die u. a. erforderlich sind, um a) eine Beschwerde bei der Aufsichtsbehörde einzureichen (Art. 13 Abs. 1 Buchst. d) und b) unbeschadet eines verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs effektiven gerichtlichen Rechtsschutz gegen eine Verletzung der durch die Richtlinie 2016/680 garantierten Rechte zu erhalten (Art. 54).

101. Nicht zu vergessen ist jedoch, dass sowohl Art. 13 Abs. 3 als auch Art. 15 Abs. 1 der Richtlinie 2016/680 die Mitgliedstaaten ermächtigen, Gesetzgebungsmaßnahmen zu erlassen, nach denen:

— die Unterrichtung der betroffenen Person gemäß Art. 13 Abs. 2 aufgeschoben, eingeschränkt oder unterlassen werden kann;

— das Recht der betroffenen Person auf Auskunft über die verarbeiteten Daten teilweise oder vollständig eingeschränkt wird, sofern diese Einschränkung erforderlich und verhältnismäßig ist, um u. a. zu gewährleisten, dass behördliche oder gerichtliche Untersuchungen oder Verfahren nicht behindert und strafrechtliche Ermittlungen nicht beeinträchtigt werden [36].

102. Auf jeden Fall hängt die Rechtmäßigkeit der Datenverarbeitung nicht davon ab, ob die zuständigen Behörden die ihnen durch Art. 13 der Richtlinie 2016/680 auferlegten (nachfolgenden) Pflichten erfüllt haben, sondern von der Rechtmäßigkeit des Zwecks, zu dem sie durchgeführt wurde, d. h. davon, ob diese Verwaltungsbehörden zur Verarbeitung der personenbezogenen Daten berechtigt waren.

[35] Rn. 37 ihrer schriftlichen Erklärungen.

[36] In diesem Sinne vgl. Urteil Tele2 Sverige und Watson (Rn. 121). Die Rechtsprechung in Bezug auf die Richtlinie 2002/58 kann im Zusammenhang mit der Garantie des gerichtlichen Schutzes der Rechte der von der Datenverarbeitung betroffenen Personen auf die Richtlinie 2016/680 übertragen werden.

103. Vor diesem Hintergrund hat die Frage, ob die betroffene Person über den versuchten Zugang zu den auf dem sichergestellten Telefon gespeicherten Daten informiert wurde, an sich nichts mit der materiellen Rechtmäßigkeit der polizeilichen Maßnahme zu tun. Dass das Verhalten des für die Verarbeitung Verantwortlichen möglicherweise gegen die ihm durch Art. 13 der Richtlinie 2016/680 auferlegten Pflichten verstößt, kann sonstige Folgen haben, hat aber, wie ich wiederholen möchte, keine Auswirkungen auf die Rechtmäßigkeit oder Rechtswidrigkeit der Verarbeitung selbst.

104. Es ist Sache des vorlegenden Gerichts, zu prüfen, ob die nationale Regelung die wirksame Ausübung dieser Rechte durch den Betroffenen ermöglicht.

## V. Ergebnis

105. Nach alledem schlage ich dem Gerichtshof vor, das Vorabentscheidungsersuchen des Landesverwaltungsgerichts Tirol (Österreich) für unzulässig zu erklären.

Hilfsweise schlage ich vor, auf die Vorlagefragen wie folgt zu antworten:

1. Art. 4 Abs. 1 Buchst. a und Art. 8 Abs. 1 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates in Verbindung mit den Art. 7, 8 und 52 der Charta der Grundrechte der Europäischen Union

   sind dahin auszulegen, dass

   im Rahmen einer strafrechtlichen Ermittlung der Zugang der Behörden zu auf einem Mobiltelefon gespeicherten personenbezogenen Daten mit dem Ziel ihrer Verarbeitung nicht auf Fälle der Bekämpfung schwerer Straftaten beschränkt ist.

   Ein solcher Zugang muss abhängig von der Art der verfolgten Straftaten und der personenbezogenen Daten, auf die zugegriffen werden soll, in jedem einzelnen Fall gerechtfertigt und auf das unbedingt erforderliche und verhältnismäßige Maß beschränkt sein.

   Im Rahmen einer strafrechtlichen Ermittlung dürfen die Polizeibehörden nicht in Eigeninitiative und ohne vorherige gerichtliche Anordnung umfassenden und unkontrollierten Zugang zu allen auf einem Mobiltelefon gespeicherten Daten erhalten, wenn sich daraus ein genaues Bild des Privatlebens der betroffenen Person gewinnen lässt.

2. Die Art. 13, 15 und 54 der Richtlinie 2016/680 in Verbindung mit den Art. 47 und 52 der Charta

   sind dahin auszulegen, dass

   der Inhaber eines Mobiltelefons unbeschadet der nach Art. 15 Abs. 1 der Richtlinie 2016/680 zulässigen Beschränkungen oder anderer verfügbarer verwaltungsrechtlicher oder außergerichtlicher Rechtsbehelfe zu dem Zeitpunkt und unter den Bedingungen, die erforderlich sind, um die wirksame Ausübung seines Rechts auf gerichtlichen Schutz gegen

eine etwaige Verletzung der in der Richtlinie 2016/680 verankerten Rechte zu garantieren, über die von den zuständigen Behörden vorgenommene Verarbeitung der auf dem Telefon gespeicherten personenbezogenen Daten zu informieren ist.