Сборник съдебна практика

ЗАКЛЮЧЕНИЕ НА ГЕНЕРАЛНИЯ АДВОКАТ
M. CAMPOS SÁNCHEZ-BORDONA
представено на 20 април 2023 година [1]

Дело C-548/21

C. G.
срещу
Bezirkshauptmannschaft Landeck

(Преюдициално запитване, отправено от Landesverwaltungsgericht Tirol (Областен административен съд Тирол, Австрия)

„Преюдициално запитване — Телекомуникации — Защита на личните данни — Директива (ЕС) 2016/680 — Наказателно производство — Опит за достъп на публични органи до запазени на мобилен телефон данни без разрешение от съд или независим административен орган“

1. Настоящото преюдициално запитване се отнася накратко до условията, към които полицейските органи трябва да се придържат, за да получат достъп до данните, запазени на мобилния телефон на лицето, срещу което се води наказателно разследване.

2. Както ще се опитам да обясня, в преюдициалното запитване са налице значителни недостатъци по отношение на неговата допустимост. Ако Съдът въпреки всичко реши да го разгледа по същество, следва да се произнесе по съответното приложно поле на Директива 2002/58/ЕО [2] и Директива (ЕС) 2016/680 [3].

[1] Език на оригиналния текст: испански.

[2] Директива на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации) (ОВ L 201, 2002 г., стр. 37; Специално издание на български език, 2007 г., глава 13, том 36, стр. 63).

[3] Директива на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета (ОВ L 119, 2016 г., стр. 89).

I. Правна уредба

A. Правото на Съюза

1. Регламент (ЕС) 2016/679[4]

3. Член 2 („Материален обхват“), параграф 2 предвижда:

„Настоящият регламент не се прилага за обработването на лични данни:

[…]

г) от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазването от и предотвратяването на заплахи за обществената сигурност“.

2. Директива 2016/680

4. В съображение 2 се посочва, че:

„Принципите и правилата относно защитата на физическите лица във връзка с обработването на личните им данни следва […] да са съобразени с техните основни права и свободи и по-конкретно с правото на защита на личните им данни. Целта на настоящата директива е да допринесе за изграждането на пространство на свобода, сигурност и правосъдие“.

5. Съображение 46 гласи:

„Всяко ограничаване на правата на субекта на данни трябва да бъде в съответствие с Хартата и с ЕКПЧ, както се тълкуват съответно в практиката на Съда и от Европейския съд по правата на човека[5], и по-специално като се зачита същността на тези права и свободи“.

6. Съображение 49 гласи:

„Когато личните данни се обработват в хода на наказателно разследване и съдебно производство по наказателно дело, държавите членки следва да могат да гарантират, че правото на информация, достъп до и коригиране или изтриване на лични данни и ограничаване на обработването се упражнява в съответствие с националните правила относно съдебните производства“.

[4] Регламент на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 2016 г., стр. 1). Наричан по-нататък „ОРЗД“.

[5] Наричан по-нататък „ЕСПЧ“.

7. Член 1 („Предмет и цели“) предвижда:

„1. С настоящата директива се установяват правилата във връзка със защитата на физическите лица по отношение на обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществената сигурност и тяхното предотвратяване.

2. В съответствие с настоящата директива държавите членки:

а) защитават основните права и свободи на физическите лица и по-специално правото им на защита на личните данни; и

[…]

3. Настоящата директива не възпрепятства държавите членки да предвиждат по-строги предпазни мерки от установените в настоящата директива за защитата на правата и свободите на субекта на данните по отношение на обработването на лични данни от компетентните органи“.

8. Член 2 („Обхват“), параграф 1 гласи:

„Настоящата директива се прилага за обработването на лични данни от компетентните органи за целите, посочени в член 1, параграф 1“.

9. Член 3 („Определения“) предвижда:

„За целите на настоящата директива:

[…]

2) „обработване“ означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друга форма на осигуряване на достъп до данните, подреждане или комбиниране, ограничаване, изтриване или унищожаване;

[…]

7) „компетентен орган“ означава:

а) всеки публичен орган, който е компетентен за предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществената сигурност и тяхното предотвратяване; или

[…]“.

10. Член 4 („Принципи, свързани с обработването на лични данни“), параграф 1 предвижда:

„Държавите членки гарантират, че личните данни са:

а) обработвани законосъобразно и добросъвестно;

б) събирани за конкретни, изрично указани и легитимни цели и не се обработват по начин, който е несъвместим с тези цели;

в) подходящи, относими и не надхвърлят необходимото във връзка с целите, за които данните се обработват;

[…]

д) съхранявани във вид, който позволява идентифицирането на субектите на данните за период не по-дълъг от необходимия за целите, за които те се обработват;

е) обработвани по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки“.

11. Член 8 („Законосъобразност на обработването“) гласи:

„1. Държавите членки предвиждат обработването да бъде законосъобразно само ако и доколкото то е необходимо за изпълнението на задача, осъществявана от компетентен орган за целите, определени в член 1, параграф 1, и е въз основа на правото на Съюза или правото на държава членка.

2. В правото на държавата членка, регламентиращо обработването, попадащо в обхвата на настоящата директива, се посочват най-малко общите цели на обработването, личните данни, които се обработват, и конкретните цели на обработването“.

12. Член 13 („Информация, до която се осигурява достъп или която се предоставя на субекта на данните“) предвижда:

„1. Държавите членки предвиждат администраторът да предоставя на субектите на данни най-малко следната информация:

[…]

г) правото да бъде подадена жалба до надзорен орган и да бъдат предоставени неговите координати за връзка;

[…]

3. Държавите членки могат да приемат законодателни мерки, които забавят, ограничават или водят до пропускане на предоставянето на информация на субекта на данните съгласно параграф 2, до такава степен и за толкова време, за колкото тази мярка е необходима и пропорционална в едно демократично общество, като надлежно се вземат под внимание основните права и легитимните интереси на засегнатото физическо лице, за да:

а) се избегне възпрепятстването на официални или съдебни проучвания, разследвания или процедури;

б) не се допусне неблагоприятно влияние върху предотвратяването, разкриването, разследването или наказателното преследване на престъпления или изпълнението на наказания;

в) се защити обществената сигурност;

г) се защити националната сигурност;

д) се защитят правата и свободите на други лица.

[…]“.

13. Съгласно член 15 („Ограничения на правото на достъп“), параграф 1:

„Държавите членки могат да приемат законодателни мерки, които ограничават изцяло или частично правото на достъп на субекта на данните, до степен и срок, при които такова частично или пълно ограничаване представлява необходима и пропорционална мярка в едно демократично общество, като надлежно се вземат под внимание основните права и легитимните интереси на засегнатото физическо лице, за да

а) се избегне възпрепятстването на официални или съдебни проучвания, разследвания или процедури;

б) не се допусне неблагоприятно влияние върху предотвратяването, разкриването, разследването или наказателното преследване на престъпления или изпълнението на наказания;

в) се защити обществената сигурност;

г) се защити националната сигурност;

д) се защитят правата и свободите на други лица“.

14. Съгласно член 27 („Оценка на въздействието върху защитата на данните“):

„1. Когато съществува вероятност определен вид обработване, по-специално при което се използват нови технологии, и предвид естеството, обхвата, контекста и целите на обработването, да породи висок риск за правата и свободите на физическите лица, държавите членки предвиждат, преди да бъде извършено обработването, администраторът да извършва оценка на въздействието на предвидените операции по обработването върху защитата на личните данни.

2. Оценката, посочена в параграф 1, съдържа най-малко общо описание на предвидените операции по обработване, оценка на рисковете за правата и свободите на субектите на данните, мерките, предвидени за справяне с тези рискове, гаранции, мерки за сигурност и механизми за гарантиране на защитата на личните данни и за доказване на съответствие с настоящата директива, като се вземат предвид правата и легитимните интереси на субектите на данните и другите засегнати лица“.

15. Член 28 („Предварителна консултация с надзорния орган“) гласи:

„1. Държавите членки предвиждат администраторът или обработващият лични данни да се консултира с надзорния орган преди обработването на лични данни, което ще бъде част от нов регистър с лични данни, който предстои да бъде създаден, когато:

а) оценката на въздействието върху защитата на данните съгласно член 27 покаже, че обработването ще породи висок риск, ако администраторът не предприеме мерки за ограничаване на риска; или

б) видът обработване, по-специално когато се използват нови технологии, механизми или процедури, включва висока степен на риск за правата и свободите на субектите на данните.

[…]“.

16. Член 54 („Право на ефективна съдебна защита срещу администратор или обработващ лични данни“) предвижда:

„Без да се засягат наличните средства за административна или извънсъдебна защита, включително правото да се подаде жалба до надзорен орган съгласно член 52, държавите членки предвиждат правото на субектите на данни на ефективна съдебна защита, ако считат, че правата им, установени в разпоредби, приети съгласно настоящата директива, са нарушени вследствие на обработването на личните им данни при неспазване на посочените разпоредби“.

Б. Националното право

17. Член 18 от Strafprozessordnung[6] възлага на криминалната полиция изпълнението на функции в служба на наказателното правораздаване (параграф 1). Разследванията на криминалната полиция се извършват от органите в сферата на сигурността (параграф 2). Органите за обществена сигурност изпълняват изпълнителните функции на криминалната полиция, които се състоят в разследване и преследване на престъпления (параграф 3).

18. Съгласно член 99 от StPO криминалната полиция провежда разследвания служебно или по жалба при спазване на прокурорските разпореждания и съдебните определения (параграф 1). Когато за мярка по разследване се изисква прокурорско разпореждане, криминалната полиция може да упражни съответното правомощие и без такова разпореждане в случай на непосредствена опасност. В такъв случай тя трябва незабавно да поиска разрешение (параграф 2).

[6] Наказателнопроцесуален кодекс. Наричан по-нататък „StPO“. BGBl № 631/1975, в приложимата редакция към момента на настъпване на фактите (BGBl I № 24/2020).

19. Съгласно член 111, параграф 2 от StPO, когато информация, запазена на носители на данни, трябва да бъде предмет на събиране на данни, всяко лице е длъжно да разреши достъпа до нея и при поискване да предаде или разреши създаването на електронен носител на данни в обичайно използван файлов формат. Освен това то трябва да позволи създаването на резервно копие на информацията, запазена на носители на данни.

II. Фактите, спорът и преюдициалните въпроси

20. C. G. е германски гражданин, който работи и живее в Австрия.

21. На 23 февруари 2021 г. при проверка за наркотични вещества служители на митническата служба в Инсбрук (Австрия) изземват адресиран до C. G. пакет, съдържащ 85 грама канабис.

22. На 6 март 2021 г. двама полицаи разпитват C. G. относно подателя на пакета и претърсват жилището му. В хода на това претърсване е иззет мобилният му телефон (съдържащ SIM и SD карта) и му е връчен протокол за изземването.

23. След като му е поискано да предостави достъп до данните за телефонните му контакти от мобилния му телефон, C. G. отказва това, както и да разкрие кода за достъп до телефона.

24. Районното полицейско управление Ландек (Австрия) не успява да отключи мобилния телефон. Той е изпратен на Bundeskriminalamt (Федерална криминална полиция) във Виена (Австрия), където отново е направен неуспешен опит за отключване на телефона и анализ на запазените данни.

25. В момента, в който тези мерки са наложени от полицията, не е имало прокурорско разпореждане, нито съдебно определение за тях.

26. На 31 март 2021 г. C. G. подава до Landesverwaltungsgericht Tirol (Областен административен съд, Тирол, Австрия) жалба срещу наложената му принудителна мярка, като обжалва изземването на мобилния му телефон. Той му е върнат на 20 април 2021 г.

27. C. G. не е уведомен относно опитите за анализ на данни от мобилния телефон; те му стават известни едва когато, като свидетел, обвързан от задължението да говори истината, е разпитан полицейският служител, който е извършил изземването и впоследствие е започнал анализа на цифровите данни. Тези опити за анализ на данни не са документирани и в акта на криминалната полиция.

28. В този контекст Landesverwaltungsgericht Tirol (Областен административен съд Тирол, Австрия) отправя до Съда следните преюдициални въпроси:

„1) Трябва ли член 15, параграф 1 (евентуално във връзка с член 5) от Директива 2002/58, изменена с Директива 2009/136/ЕО, в светлината на членове 7 и 8 от Хартата […] да се тълкува в смисъл, че достъпът на публични органи до запазените на мобилни телефони данни представлява намеса в закрепените в тези членове от Хартата основни права, тежестта на която е такава, че в областта на превенцията, разследването, разкриването и преследването на престъпления посоченият достъп трябва да бъде ограничен до борбата с тежката престъпност?

2) Трябва ли член 15, параграф 1 от Директива 2002/58, изменена с Директива 2009/136, в светлината на членове 7, 8 и 11, както и на член 52, параграф 1 от Хартата да се тълкува в смисъл, че не допуска национална правна уредба като тази на член 18 във връзка с член 99, параграф 1 от [StPO], която позволява органите в сферата на сигурността да имат в хода на наказателното разследване широк и неконтролиран достъп до всички запазени на мобилен телефон цифрови данни, без да разполагат с разрешение за това от съд или независим административен орган?

3) Трябва ли член 47 от Хартата, евентуално във връзка с членове 41 и 52 от нея, разглеждани с оглед на принципа за равните процесуални възможности и правото на ефективни правни средства за защита, да се тълкува в смисъл, че не допуска национална правна уредба, която като член 18 във връзка с член 99, параграф 1 от [StPO] позволява да бъдат анализирани цифрови данни от мобилен телефон, без засегнатото лице да бъде уведомено за това преди или най-малкото след налагането на съответната мярка?“.

III. Производството пред Съда

29. Преюдициалното запитване постъпва в Съда на 6 септември 2021 г.

30. На 20 октомври 2021 г. Съдът приканва запитващата юрисдикция да изрази становище по въпроса дали Директива 2016/680 е приложима в случая.

31. На 11 ноември 2021 г. запитващата юрисдикция отговаря, че Директива 2016/680 трябва да бъде приложена в главното производство.

32. Писмени становища представят германското, австрийското, кипърското, датското, естонското, френското, унгарското, ирландското, нидерландското, норвежкото, полското и шведското правителство, както и Европейската комисия.

33. Те се явяват в съдебното заседание, проведено на 16 януари 2023 г., с изключение на германското, унгарското и полското правителство, които представят, както и финландското правителство, писмени становища. Всички са приканени от Съда да съсредоточат становищата си върху Директива 2016/680 и да отговорят устно на определени свързани с нея въпроси.

IV. Анализ

A. Недопустимост

34. При първоначалната формулировка на въпросите си запитващата юрисдикция иска тълкуване само на Директива 2002/58. Почти всички участници в производството обаче споделят мнението, че тази директива не е приложима в настоящия случай и следователно нейното тълкуване не е необходимо за разрешаването на спора.

35. Съгласно член 3 Директива 2002/58 урежда „[…] обработката на лични данни във връзка с предоставянето на обществено достъпни електронни съобщителни услуги в обществени съобщителни мрежи в [Съюза], включително обществени съобщителни мрежи, поддържащи събиране на данни и устройства за идентификация“.

36. Съдът е приел, че „когато държавите членки прилагат пряко мерки, които въвеждат изключение от поверителността на електронните съобщения, без да налагат на доставчиците на услуги задължения за обработване на такива съобщения, защитата на данните на засегнатите лица се урежда не от Директива 2002/58, а единствено от националното право, без да се накърнява прилагането на [Директива 2016/680]“ [7].

37. В разглеждания случай опитът за достъп до данните е извършен директно от полицейските органи в хода на наказателно разследване. Няма намеса на доставчици на електронни съобщителни услуги, от които не е поискано предаването на лични данни. Следователно Директива 2002/58 не е приложима.

38. Нормата от правото на Съюза, уреждаща това положение, е Директива 2016/680, съгласно член 2, параграф 1 от която тя се прилага за обработването на лични данни от компетентните органи за „целите на […] разследването […] на престъпления“.

39. Гореизложеното е достатъчно, за да се приеме, че формулираното по този начин от националния съд преюдициално запитване е недопустимо, тъй като нормата от правото на Съюза, чието тълкуване иска, не е приложима в настоящия случай.

40. Вярно е обаче, че член 267 ДФЕС допуска Съдът да преформулира преюдициалните въпроси, които са му зададени, или да посочи, че съществуват други евентуално приложими норми от правото на Съюза, за да даде на националния съд полезен отговор [8].

41. Съдът е поискал от запитващата юрисдикция да се произнесе относно евентуалното значение на Директива 2016/680. Следователно ѝ е предоставил възможност да допълни или преформулира въпросите си. Вместо това запитващата юрисдикция отбелязва само, че „по настоящото дело следва при всички случаи да се спазят разпоредбите на Директива 2016/680“, без да посочи разпоредбите ѝ, по отношение на които изпитва съмнения, и да изложи други съображения по същество [9].

42. Съдът последователно приема, че „съгласно член 94, буква в) от Процедурния правилник е необходимо преюдициалното запитване да съдържа изложение на причините, поради които запитващата юрисдикция има въпроси относно тълкуването или валидността на някои разпоредби на правото на Съюза, както и установената от нея връзка между тези разпоредби и националното законодателство, приложимо в главното производство“ [10].

43. В настоящото преюдициално запитване обаче неизпълнението на изискванията на член 94 от Процедурния правилник е очевидно предвид изложеното по-горе. Дори когато Съдът прояви определена гъвкавост в това отношение, сътрудничеството със запитващата

[7] Решение от 6 октомври 2020 г., La Quadrature du Net и др. (C-511/18, C-512/18 и C-520/18, EU:C:2020:791, наричано по-нататък „решение La Quadrature du Net“, т. 103).

[8] По-специално решение от 28 април 2016 г., Oniors Bio (C-233/15, EU:C:2016:305, т. 30).

[9] Наложило се е Съдът да прикани страните да посочат „кои според тях са приложимите разпоредби на Директива 2016/680, с оглед на които Съдът би следвало евентуално да преформулира трите преюдициални въпроса, отправени от запитващата юрисдикция“ (четвъртият от поставените въпроси за устен отговор в съдебното заседание).

[10] Решение от 6 октомври 2021 г., Consorzio Italian Management и Catania Multiservizi (C-561/19, EU:C:2021:799, т. 69).

юрисдикция трябва да е взаимно: при неоснователна липса на сътрудничество от нейна страна да изложи съмненията си относно тълкуването на правото на Съюза, което счита за приложимо (в случая Директива 2016/680), според мен е логично да се приеме преюдициалното запитване за недопустимо [11].

44. Към гореизложеното се добавя и обстоятелството, че посоченият съд:

— не е уточнил естеството на направения от полицейските органи опит за обработка или на конкретно търсените лични данни. Първоначално тя, изглежда, посочва, че става въпрос само за данните за осъществени телефонни разговори (т.е. за трафик и местонахождение), но след това не изключва възможността отключването на телефона да осигури достъп до „всички запазени цифрови данни“ [12] и дори до съдържанието на проведената комуникация и разменените чрез него електронни съобщения [13],

— посочва както изземването на телефона и достъпа или опита за достъп до съдържащите се в него данни, така и последващото им „обработване“ (Auswertung), т.е. до техния анализ и разчитане. Той добавя, че последното „е равнозначн[но] на получаване на напълно неконтролиран достъп до цялата цифрова комуникация на засегнатото лице“, с което „може да бъде реконструирана много подробна и всеобхватна картина на почти всички области от личния живот“.

45. При това положение освен *преформулиране* на въпросите на запитващата юрисдикция Съдът би извършил същинска *преработка* на преюдициалното запитване, основана освен това отчасти на хипотетични съображения, а не на установени факти. Съдът трябва да направи всичко това, повтарям, след като е предоставил на запитващата юрисдикция възможността сама да допълни или преформулира въпросите си.

46. Ето защо предлагам преюдициалното запитване да се приеме за недопустимо, както са поискали повечето от встъпилите държави.

47. До този извод за недопустимост би трябвало да води и обстоятелството, изтъкнато в съдебното заседание, че пред запитващата юрисдикция вече не съществува същински спор, който да налага тълкуване на норми от правото на Съюза.

48. Всъщност австрийското правителство (към което принадлежат участвалите в разследването полицейски органи) признава, че действията на тези органи са били незаконосъобразни и нарушават правата на засегнатото лице. Предвид обстоятелството, че според акта за преюдициално запитване исканията на жалбоподателя до административния съд са насочени именно срещу полицейските мерки, които администрацията ответник счита за незаконосъобразни, спорът, с който е сезирана запитващата юрисдикция, вече не съществува.

[11] Споделям преценката по този въпрос на френското правителство (т. 36—41 от писменото му становище).

[12] Така във втория преюдициален въпрос.

[13] Запитващата юрисдикция посочва, че „от данните за осъществени телефонни разговори е възможно да се възстановят почти всички контакти, като честота, време и продължителност на комуникацията, а от съобщения и други месинджър услуги — дори съдържанието на проведената комуникация; анализът на запазени снимки и историята на браузъра също позволяват поглед върху изключително интимни области от личния живот на засегнатото лице“.

49. При всички случаи, ако Съдът не споделя виждането ми, ще разгледам по-нататък при условията на евентуалност проблемите по същество, които са в основата на преюдициалните въпроси.

50. Преди това обаче считам, че е необходимо да изключа наличието на друго основание за недопустимост, изтъкнато от някои от встъпилите страни в производството [14]. Според тях, тъй като Директива 2016/680 се отнася до защитата на физическите лица във връзка с *обработването* на личните им данни, тя не урежда случаи като настоящия, в които не е имало обработване, а само *опит за достъп* до данни, които в крайна сметка не е можело да бъдат получени.

51. Обратно, според Комисията полезното действие на Директива 2016/680 трябва да води до предпочитане на тълкуване в смисъл, че нейната цел не се свежда до обработването на данни в тесния смисъл на думата, а включва и пряко свързани с него въпроси. Сред тях е опитът за достъп до данните, чието обработване се иска [15].

52. Според мен, без да е необходимо да се разширява обхватът на Директива 2016/680 [16], приложимостта ѝ в настоящия случай е обоснована не поради изземването на мобилния телефон [17], а поради последващите действия на полицейските органи да извлекат от него определени лични данни на засегнатото лице, за която цел са се опитали да го отключат и осигурят достъп до съдържанието му.

53. Една от операциите, определени като „обработване“ в член 3, точка 2 от Директива 2016/680, е „друга форма на осигуряване на достъп до“ личните данни, осъществена в хода на наказателно разследване. Според мен, когато полицейският орган изземва телефон, на който са запазени тези данни, и го използва, за да ги извлече от него, започва „операция“ по обработване макар и неуспешна поради технически причини, свързани с криптографската сигурност.

54. Неуспешният опит за достъп до запазени на мобилен телефон лични данни в хода на наказателно преследване се урежда от Директива 2016/680 по причини, аналогични на тези, поради които Съдът приема, че Директива 2002/58 е приложима към *опита* (също неуспешен) за получаване на разрешение от съда за достъп до определени данни на заподозряно лице, притежавани от телефонен оператор [18].

[14] Имам предвид по-конкретно австрийското, френското, нидерландското и норвежкото правителство.

[15] Според Комисията „няма значение дали опитите са успешни“. Възникването на технически затруднения, възпрепятстващи успешния опит за обработване, е обстоятелство, което не може да се знае предварително и не засяга рисковете за защитата на личните данни“.

[16] По-специално считам за ненужно прибягването до членове 27 и 28 от Директива 2016/680, предложено от Комисията в писменото ѝ становище. „Оценката на въздействието върху защитата на данните“, предвидена в член 27 се отнася като цяло до „определен вид обработване“, а не до отделно или специфично обработване. Това следва от съображение 58 от Директива 2016/680: „[о]ценките на въздействието следва да обхващат съответните системи и процеси на операциите по обработване, а не *отделни случаи*“ (курсивът е мой). Комисията пояснява в съдебното заседание посочването ѝ на двете разпоредби, които е цитирала само за да подчертае, че Директива 2016/680 предвижда и положения, предшестващи същинското обработване на данни.

[17] Директива 2016/680 не урежда изземването на телефона като доказателство в хода на наказателно разследване.

[18] Решение от 2 октомври 2018 г., Ministerio Fiscal (C-207/16, EU:C:2018: 788).

55. В този контекст, ако запитващата юрисдикция трябваше да се произнесе по незаконосъобразността на полицейските действия (призната от австрийското правителство, както посочих по-горе), нейната преценка би могла да зависи от законосъобразността на целта на тези действия, независимо дали мярката е осъществена или е предприета неуспешно.

Б. По съществото на спора

1. По първия преюдициален въпрос

56. Запитващата юрисдикция иска да се установи дали съгласно член 15, параграф 1 от Директива 2002/58 (евентуално във връзка с член 5 от нея) и в светлината на членове 7 и 8 от Хартата „достъпът на публични органи до запазените на мобилни телефони данни представлява намеса в закрепените в тези членове от Хартата основни права, тежестта на която е такава, че в областта на превенцията, разследването, разкриването и преследването на престъпления посоченият достъп трябва да бъде ограничен до борбата с тежката престъпност“.

57. В случай на допустимост на преюдициалното запитване неприложимостта на Директива 2002/58 налага да се преформулира първият въпрос така, че отговорът на Съда да предостави тълкуване на Директива 2016/680.

58. Този отговор би трябвало да изясни на свой ред дали може да се говори за намеса в случаи като настоящия, и ако такава е налице, дали Директива 2016/680 изисква достъпът до данните да е ограничен до случаите на борба с тежката престъпност.

59. Операциите по обработване на данни могат да нарушават по дефиниция правата на зачитане на личния живот (член 7 от Хартата) и на защита на личните данни (член 8 от Хартата). Следователно публичните органи трябва да спазват условията, предвидени в член 52, параграф 1 от Хартата, за да обосноват намесата си в упражняването на тези основни права.

60. Намесата в правата, защитени от членове 7 и 8 от Хартата, ще бъде още по-голяма, когато с нея: а) се цели достъп до чувствителни данни, които обикновено се запазват на мобилните телефони и чието узнаване може да разкрие аспекти от живота на притежателите им, които не трябва да стават достояние на трети лица, и б) става възможен достъпът до съдържанието на проведената комуникация.

61. В общия случай и предвид нейното съдържание обаче Директива 2016/680 не може да се тълкува в смисъл, че обработването на данни, за което се отнася, се свежда до случаите на борба с тежката престъпност.

62. Директива 2016/680 урежда всяка операция по обработване[19] на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на *всякакъв вид* престъпления.

[19] Типологията на „операциите“, съдържащи се в член 3, точка 2 от Директива 2016/680, е много обширна. Вж. възпроизвеждането ѝ в точка 9 от настоящото заключение.

63. От установените с Директива 2016/680 принципи, свързани с обработването на лични данни с посочената цел (член 4), или от условията за законосъобразност на това обработване (член 8) не следва, че по правило обработването на данните е възможно само в случаите на тежка престъпност.

64. Ограничаването до случаите на борба с тежката престъпност не би могло и да се обоснове автоматично с прилагането на практиката на Съда, свързана с Директива 2002/58[20], към случаи като настоящия.

65. Това е така, защото според мен, без да се засяга изложеното по-нататък, тази съдебна практика се отнася до общото и неизбирателно запазване на лични данни на общ и неопределен кръг лица, осъществявано системно от доставчици на електронни съобщителни услуги. Тежестта на намесата, която този вид запазване представлява за обществото като цяло, обяснява причините, поради които Съдът е проявил особена строгост при забраната ѝ и предвиждането на изключения от нея.

66. Това не е така, когато исканият достъп не засяга всички или големи групи от населението (т.е. личните данни на общ и неопределен кръг лица), а само запазената на отделен мобилен телефон информация в хода на наказателно разследване, което също е отделно и уредено изрично в Директива 2016/680.

67. Директива 2016/680 урежда именно обработването на данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления — на всички видове престъпления, а не само на тежките.

68. Освен това, както подчертават някои от участниците в преюдициалното производство, при липсата на каквото и да е указание относно тежестта на престъпленията в Директива 2016/680 тя може да не се прилага еднакво в държавите членки, тъй като преценката на по-голямата или по-малката тежест на дадено наказуемо деяние се различава значително във всяко национално право[21].

69. В обобщение Директива 2016/680 не предвижда като условие за законосъобразност, че уреденото с нея обработване на лични данни е възможно само за борбата с тежката престъпност.

70. Гореизложеното не променя факта, че при прилагане на принципа на пропорционалност и според всеки конкретен случай обработването на данни, което компетентните органи искат да извършат на основание Директива 2016/680, трябва да бъде ограничено в зависимост от: а) естеството на преследваното престъпление и б) качеството на личните данни, към които е насочено това обработване.

71. Споделям в това отношение някои виждания на германското правителство относно ограничаването на достъпа до данните на иззетите телефони, когато с тях може да се направи пълен личностен профил на притежателите им с оглед на цифровото им

[20] Решения La Quadrature du Net и от 21 декември 2016 г., Tele2 Sverige и Watson и др. (C-203/15 и C-698/15, EU:C:2016:970, наричано по-нататък „решение Tele2 Sverige и Watson“), от 2 октомври 2018 г., Ministerio Fiscal (C-207/16, EU:C:2018:788), от 6 октомври 2020 г., Privacy International (C-623/17, EU:C:2020:790), и от 2 март 2021 г., Prokuratuur (Условия за достъп до данните за електронните съобщения) (C-746/18, EU:C:2021:152, наричано по-нататък „решение Prokuratuur“).

[21] Френското правителство посочва като пример престъпленията в областта на притежанието и разпространението на наркотици, по отношение на чиято тежест се различават наказателноправните норми на Австрия и Франция. В подобен смисъл е и становището на шведското правителство.

съдържание. Според германското правителство този достъп трябва да е ограничен до данните, които са необходими като доказателство в конкретен случай, и може да не е уместен при наличие на фактори като „незначителност на разследваното престъпление или ниската доказателствена стойност на данните, чието получаване се иска“ [22].

72. Поради това, *абстрактно*, Директива 2016/680 не предвижда, че достъпът до запазените на мобилен телефон лични данни с цел улесняване на разследването на престъпления, които могат да бъдат причислени към общата или обичайната престъпност, е автоматично незаконосъобразен. Дали *конкретно* е налице такъв достъп, е въпрос, който съответният орган трябва да преценява във всеки конкретен случай с оглед на необходимостта от него и критерия за пропорционалност, който току-що посочих.

73. Според мен това следва от разпоредбите на Директива 2016/680, определящи условията за законосъобразност на обработването на лични данни в рамките на борбата с престъпността:

— член 4, параграф 1, буква а), въз основа на който данните трябва да бъдат „обработвани законосъобразно и добросъвестно“,

— член 8, параграф 1, в който се подчертава, че обработването трябва да е *необходимо* и да е въз основа на правото на Съюза или правото на държава членка.

2. По втория преюдициален въпрос

74. С втория си преюдициален въпрос запитващата юрисдикция иска да се установи дали член 15, параграф 1 от Директива 2002/58 в светлината на членове 7, 8, 11 и 52, параграф 1 от Хартата „не допуска национална правна уредба като тази на член 18 във връзка с член 99, параграф 1 от Strafprozessordnung, която позволява органите в сферата на сигурността да имат в хода на наказателното разследване широк и неконтролиран достъп до всички запазени на мобилен телефон цифрови данни, без да разполагат с разрешение за това от съд или независим административен орган“.

75. Текстът на въпроса е двусмислен в известна степен. Запитващата юрисдикция:

— признава, че член 110, параграф 2 от StPO предвижда, че по принцип за изземване на вещи се изисква разрешение от прокурор. Полицейският орган може да извършва тези изземвания без такова разрешение само в предвидените в параграф 3 от същия член извънредни случаи (които, изглежда, не са налице в настоящия случай),

— въпреки това добавя, че анализът на запазената на мобилните телефони информация „не е регламентиран [в StPO] еднозначно“ и органите в сферата на сигурността могат да го осъществяват по собствена инициатива без предварително разрешение.

76. Австрийското правителство предлага тълкуване на националната правна уредба, което не съответства на изложеното в акта за преюдициално запитване. По-конкретно то посочва, че съгласно националното право както изземването на телефона (освен в

[22] Писмено становище на германското правителство, точка 20.

неотложни случаи), така и анализът на запазените на него данни е възможен само с разрешение от прокурор [23]. Без прокурорско разпореждане използването от полицейските органи на запазените на този телефон данни е незаконосъобразно.

77. Запитващата юрисдикция трябва да провери условията на вътрешната правна уредба. В рамките на производството по член 267 ДФЕС Съдът не е компетентен да тълкува националното право и единствено запитващата юрисдикция може да определи точния обхват на националните законови, подзаконови или административни разпоредби [24].

78. Без да имам намерение да се намесвам в спора относно тълкуването на австрийското право, ми изглежда трудно само от посочените от запитващата юрисдикция разпоредби (член 18 от StPO във връзка с член 99, параграф 1 от същия закон) да се направи изводът, до който тя стига. Това обаче, повтарям, е въпрос, който само посоченият съд може да разреши.

79. При всички положения запитващата юрисдикция счита, че към настоящия случай е приложима практиката, установена с решение Prokuratuur [25], относно предварителния контрол от юрисдикция или от независима структура на достъпа до запазените данни.

80. Обратно, според нидерландското правителство тази съдебна практика трябва да се разглежда в контекста на национална правна уредба, която допуска *общия* достъп на компетентните органи до *всички* запазени данни за трафик и данни за местонахождение. С това се обяснява изискването за предварително разрешение от съд, което обаче може да не е обосновано в случай на достъп до запазените само на един мобилен телефон данни.

81. В същия смисъл норвежкото правителство посочва, че сред множеството предвидени в Директива 2016/680 гаранции [26] не фигурира изрично необходимостта от предварително разрешение от съд или независима административна структура.

82. Като изхожда от това, че разпоредбите на Директива 2016/680 трябва да се тълкуват във връзка с Хартата, Комисията посочва, че задължението, наложено на държавите членки с член 8, параграф 1 от тази директива (условия за законосъобразност на обработването), включва необходимостта от зачитане на основните права, гарантирани от членове 8 и 7 от Хартата.

83. Споделям становището на Комисията, че при спазване на тези разпоредби на Хартата националните законодатели са длъжни да установят необходимите правила, за да се гарантира, че достъпът до данните е обоснован във всеки конкретен случай, ограничен до строго необходимото и пропорционален.

[23] Точка 19 от писменото становище на австрийското правителство. То цитира решение на Oberster Gerichtshof (Върховен съд, Австрия) от 13 октомври 2020 г. (дело 11 Os 56/20z), съгласно което анализът от страна на криминална полиция на данните на мобилен телефон без разрешение от прокурор е незаконосъобразен, тъй като нарушава субективните права на засегнатото лице.

[24] По-специално решение от 28 април 2022 г., SeGEC и др. (C-277/21, EU:C:2022:318, т. 21).

[25] Решение Prokuratuur, точка 51: „от съществено значение е достъпът на компетентните национални органи до запазените данни да се предоставя след предварителен контрол, осъществяван или от юрисдикция, или от независима административна структура, и решението на тази юрисдикция или на тази структура да се постановява след мотивирана молба на тези органи, подадена по-специално в рамките на наказателни производства за предотвратяване, разкриване или наказателно преследване на престъпления“.

[26] Освен гаранциите по членове 4 и 8, съдържащите се гаранции в глава III („Права на субекта на данни“), глава IV („Администратор и обработващ лични данни“), глава VI („Независими надзорни органи“) и глава VIII („Средства за правна защита, отговорност за причинени вреди и наказания“).

84. Не е задължително обаче такива национални правила да са специални за достъпа до съдържащите се в мобилен телефон лични данни, както в настоящия случай, а могат да са предвидените като цяло във вътрешното право в областта на събирането на доказателства.

85. В това отношение цитирах по-горе точка 103 от решение La Quadrature du Net по отношение на мерките на държавите членки, засягащи поверителността на електронните съобщения, без да налагат на доставчиците на услуги задължения за обработване на такива съобщения [27].

86. Следователно, без да е необходимо да се извеждат от Директива 2016/680 *специални* процесуални правила като гаранция за законосъобразността на достъпа до запазените на мобилен телефон данни [28], се прилагат националните правила, уреждащи упражняването на правомощията за претърсване и изземване в хода на наказателните разследвания [29].

87. Освен това препращането към разпоредбите от вътрешното право, за да се гарантира законосъобразността на достъпа по смисъла на Директива 2016/680, е в съответствие с практиката на ЕСПЧ. Именно по дело, свързано с Република Австрия, във връзка с член 8 от ЕКПЧ (право на зачитане на личния и семейния живот, на жилището и на тайната на кореспонденцията) ЕСПЧ приема, че австрийското законодателство относно изземването на вещи, и по-специално на документи, се прилага към претърсването и изземването на запазени на информационни носители данни [30].

88. Ако, както твърди австрийското правителство, цитирайки практиката на Oberster Gerichtshof (Върховен съд, Австрия), полицейските органи нямат право на достъп до запазените данни на определен мобилен телефон без разрешение от прокурор, вторият преюдициален въпрос губи до голяма степен смисъла си.

89. При всички случаи отговорът на този въпрос не може да изключва възможността достъпът до личните данни в иззетия телефон да води до „реконструиран[е] [на] много подробна и всеобхватна картина на почти всички области от личния живот“ на засегнатото лице [31]. Ако това е така, полицейските органи трябва да имат предварителното разрешение, посочено в решение Prokuratuur.

90. На пръв поглед това твърдение, изглежда, не съответства на неприлагането в настоящия случай на Директива 2002/58 (тълкувана в Prokuratuur), както посочих по-горе. Считам обаче, че смисълът на това решение е в подкрепа на същото разрешение.

[27] Вж. точка 36 от настоящото заключение.

[28] Начинание, за чиято трудност свидетелстват усилията на Комисията в точки 34—39 от писменото ѝ становище да допринесе за определянето на ясни и точни правила за установяване на подходящите граници и гаранции във връзка с достъпа до данните на мобилен телефон.

[29] Правила, които, както припомнят например датското и ирландското правителство, са извън приложното поле на правото на Съюза, но могат да послужат за изпълнението на произтичащо от него изискване.

[30] Решение на ЕСПЧ от 16 октомври 2007 г., Wieser и Bicos Beteiligungen с/у Австрия (CE:ECHR:2007:1016JUD007433601), § 54: „the Austrian Code of Criminal Procedure does not contain specific provisions for the search and seizure of electronic data. However, it contains detailed provisions for the seizure of objects and, in addition, specific rules for the seizure of documents. It is established in the domestic courts' case-law that these provisions also apply to the search and seizure of electronic data“.

[31] Вж. твърденията на запитващата юрисдикция, възпроизведени в точка 44 от настоящото заключение.

91. В делото, по което е постановено решение Prokuratuur, въпреки че с достъпа са получени данни (метаданни) от доставчици на електронни съобщителни услуги, е налице, както в настоящия случай, отделно наказателно разследване, водено срещу определено лице. Става въпрос за събиране на „данни[…] относно няколко телефонни номера […] и различни международни идентификационни номера на нейния мобилен апарат“ [32].

92. Според мен в решение Prokuratuur могат да се разграничат два аспекта: а) поставянето под съмнение на общата правна уредба на държава членка относно общото и недиференцирано запазване и последващия достъп до данните, с които доставчиците на услугата разполагат, и б) предварителния контрол в отделен случай на достъпа до тези метаданни, когато с тях може да се направи точен профил на личния живот на дадено лице.

93. Според мен обстоятелството, че в разглеждания случай данните, разкриващи личния живот, не се съхраняват от доставчиците на услуга и са получени (или е направен опит за получаването им) от един-единствен телефон, е от второстепенно значение спрямо смисъла и целта на застъпеното в решение Prokuratuur изискване за предварителен контрол.

94. Този предварителен контрол в крайна сметка намира своето основание в защитата, гарантирана от членове 7 и 8 от Хартата. Органът, който го извършва, трябва да е „в състояние да осигури справедливо равновесие между, от една страна, интересите, свързани с нуждите на разследването в рамките на борбата с престъпността, и от друга страна, основните права на зачитане на личния живот и на защита на личните данни на лицата, чиито данни са засегнати от достъпа“ [33].

3. По третия преюдициален въпрос

95. С третия преюдициален въпрос запитващата юрисдикция иска да се установи дали член 47 от Хартата (евентуално във връзка с членове 41 и 52) допуска правна уредба като австрийската [34], която „позволява да бъдат анализирани цифрови данни от мобилен телефон, без засегнатото лице да бъде уведомено за това преди или най-малкото след налагането на съответната мярка“.

96. Считам, че въпросът, формулиран по този начин, може да не е необходим за разрешаването на спора, тъй като засегнатото лице е могло да упражни правото, предвидено в член 47 от Хартата, като поиска запитващата юрисдикция да обяви за недействително полицейското действие, свързано с изземания телефон, включващо последващото (и неуспешно) обработване на запазените на него данни.

97. Между тези два момента на полицейските действия следва да се направи разграничение:

— що се отнася до самото изземване на телефона, от материалите по делото следва, че засегнатото лице е знаело за него и е отказало да предостави на полицейските органи кода за отключване при изземването му;

[32] Решение Prokuratuur, точка 17.

[33] Решение Prokuratuur, точка 52.

[34] Отново става въпрос за член 18 от StPO във връзка с член 99 от него.

— що се отнася до опита за анализ на данните, по всичко личи, че администраторът не е уведомил засегнатото лице за тази операция, въпреки че австрийското правителство твърди, че то е било запознато с доклад, в който са посочени свързаните с телефона действия на криминалната полиция [35].

98. Следователно около обработването на данните и знанието на засегнатото лице за него има известни неясноти, които, както посочих по-горе, е трябвало да бъдат изяснени от запитващата юрисдикция в акта за преюдициално запитване и които пречат да се даде полезен отговор на третия преюдициален въпрос.

99. При всички случаи, ако Съдът не счете този въпрос за недопустим, ще изразя становището си по него. При тази хипотеза и предвид неприложимостта на Директива 2002/58, той следва да се преформулира с оглед на Директива 2016/680, членове 13, 15 и 54 от която дават насоките за отговора на този въпрос.

100. Съгласно Директива 2016/680 информацията за обработването на личните му данни, която трябва да се предостави на субекта на данни, е необходимата информация по-специално за: а) подаване на жалба до надзорен орган (член 13, параграф 1, буква г) и б) получаване на ефективна съдебна защита при нарушение на правата, гарантирани от Директива 2016/680, без да се засягат наличните средства за административна или извънсъдебна защита (член 54).

101. Не трябва да се забравя обаче, че както член 13, параграф 3, така и член 15, параграф 1 от Директива 2016/680 дава право на държавите членки да приемат законодателни мерки, които:

— забавят, ограничават или водят до пропускане на предоставянето на информация на субекта на данните съгласно член 13, параграф 2;

— ограничават изцяло или частично правото на достъп на субекта на обработваните данни, до степен и срок, при които това ограничаване представлява необходима и пропорционална мярка, по-специално за да се избегне възпрепятстването на официални или съдебни разследвания или процедури и да не се допусне неблагоприятно влияние върху разследването на престъпления [36].

102. При всички случаи законосъобразността на обработването на данните не зависи от изпълнението от компетентните органи на наложените им с член 13 от Директива 2016/680 задължения (последващи), а от законосъобразността на целта, за която то се извършва, т.е. от това дали тези административни органи са оправомощени да обработват личните данни.

103. От тази гледна точка обстоятелството, че засегнатото лице е било уведомено за опитите за достъп до запазените на иззетия му телефон данни, само по себе си не е свързано със законосъобразността на полицейските действия поради наличието на основателни причини. Поведението на администратора, което евентуално противоречи на

[35] Точка 37 от писменото му становище.

[36] В този смисъл вж. решение Tele2 Sverige и Watson, точка 121. Установената с него практика във връзка с Директива 2002/58 може да бъде приложена и по отношение на Директива 2016/680 в контекста на гаранцията за съдебна защита на правата на субектите на обработваните данни.

наложените му с член 13 от Директива 2016/680 задължения, може да има други последици, но повтарям, само по себе си не засяга законосъобразността или незаконосъобразността на обработването.

104. Запитващата юрисдикция следва да установи дали националната правна уредба позволява ефективното упражняване на посочените права от засегнатото лице.

V. Заключение

105. По изложените съображения предлагам на Съда да приеме за недопустимо преюдициалното запитване, отправено от Landesverwaltungsgericht Tirol (Областен административен съд Тирол, Австрия).

При условията на евентуалност, предлагам да се отговори на настоящото запитване по следния начин:

„1) Член 4, параграф 1, буква а) и член 8, параграф 1 от Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета във връзка с членове 7, 8 и 52 от Хартата на основните права на Европейския съюз

следва да се тълкуват в смисъл, че

в хода на наказателно разследване достъпът на публичните органи до запазените на мобилен телефон лични данни с оглед на тяхното обработване не е ограничен до случаите на борба с тежката престъпност.

Този достъп трябва да е обоснован във всеки конкретен случай, ограничен до строго необходимото и пропорционален в зависимост от естеството на преследваните престъпления и личните данни, до които се иска достъп.

Полицейските органи не могат да имат в хода на наказателно разследване широк и неконтролиран достъп до всички запазени на мобилен телефон данни, без да разполагат с разрешение за това от съд, когато с тях може да бъде получена точна картина на личния живот на дадено лице.

2) Членове 13, 15 и 54 от Директива 2016/680 във връзка с членове 47 и 52 от Хартата

следва да се тълкуват в смисъл, че

без да се засягат ограниченията, разрешени от член 15, параграф 1 от Директива 2016/680, или наличните средства за административна или извънсъдебна защита, притежателят на мобилен телефон трябва да бъде информиран за обработването на запазените на него лични данни, извършено от съответните органи, в момента и при условията, които са необходими, за да се гарантира ефективното упражняване на правото му на съдебна защита при евентуално нарушение на правата, предвидени в Директива 2016/680“.