Zbierka súdnych rozhodnutí

NÁVRHY GENERÁLNEHO ADVOKÁTA
MANUEL CAMPOS SÁNCHEZ-BORDONA
prednesené 20. apríla 2023 [1]

Vec C-548/21

C. G.
proti
Bezirkshauptmannschaft Landeck

[návrh na začatie prejudiciálneho konania, ktorý podal Landesverwaltungsgericht Tirol (Krajinský správny súd spolkovej krajiny Tirolsko, Rakúsko)]

„Prejudiciálne konanie – Telekomunikácie – Ochrana osobných údajov – Smernica (EÚ) 2016/680 – Trestné konanie – Pokus orgánov verejnej moci o prístup k údajom uloženým v mobilnom telefóne bez povolenia súdu alebo nezávislého správneho orgánu“

1. Prejednávaný návrh na začatie prejudiciálneho konania sa v podstate týka podmienok, ktoré musia dodržiavať policajné orgány pri získavaní prístupu k údajom uloženým v mobilnom telefóne osoby, proti ktorej sa vedie trestné vyšetrovanie.

2. Ako sa pokúsim vysvetliť, tento návrh na začatie prejudiciálneho konania má značné nedostatky, pokiaľ ide o jeho prípustnosť. Ak by sa Súdny dvor napriek tomu rozhodol, že sa bude zaoberať jeho vecnou stránkou, bude musieť rozhodnúť o pôsobnosti smernice 2002/58/ES [2] a smernice (EÚ) 2016/680 [3].

[1] Jazyk prednesu: španielčina.

[2] Smernica Európskeho parlamentu a Rady z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 2002, s. 37; Mim. vyd. 13/029, s. 514).

[3] Smernica Európskeho parlamentu a Rady z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV (Ú. v. EÚ L 119, 2016, s. 89).

I. Právny rámec

A. Právo Únie

1. Nariadenie (EÚ) 2016/679[4]

3. Článok 2 s názvom „Vecná pôsobnosť“ v odseku 2 stanovuje:

„Toto nariadenie sa nevzťahuje na spracúvanie osobných údajov:

…

d) príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania, alebo výkonu trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a jeho predchádzania“.

2. Smernica 2016/680

4. V odôvodnení 2 sa konštatuje:

„Zásady a pravidlá ochrany fyzických osôb pri spracúvaní ich osobných údajov by… mali rešpektovať základné práva a slobody, najmä ich právo na ochranu osobných údajov. Táto smernica má prispieť k dobudovaniu priestoru slobody, bezpečnosti a spravodlivosti.“

5. Odôvodnenie 46 znie:

„Akékoľvek obmedzenie práv dotknutej osoby musí byť v súlade s chartou a EDĽP, ako sa vykladajú v judikatúre Súdneho dvora a Európskym súdom pre ľudské práva[5], a predovšetkým musí rešpektovať podstatu uvedených práv a slobôd.“

6. V odôvodnení 49 sa uvádza:

„Ak sa osobné údaje spracúvajú počas vyšetrovania trestného činu a súdneho konania v trestných veciach, členské štáty by mali mať možnosť stanoviť, že uplatňovanie práva na informácie, prístup a opravu alebo vymazanie osobných údajov a obmedzenie spracúvania sa vykonáva v súlade s vnútroštátnymi pravidlami súdneho konania.“

7. V článku 1, nazvanom „Predmet úpravy a ciele“, sa stanovuje:

„1. Touto smernicou sa stanovujú pravidlá ochrany fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií, vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu.

[4] Nariadenie Európskeho parlamentu a Rady z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 2016, s. 1; ďalej len „GDPR“).

[5] Ďalej len „ESĽP“.

2. Členské štáty v súlade s touto smernicou:

a) chránia základné práva a slobody fyzických osôb, najmä ich právo na ochranu osobných údajov, a

….

3. Táto smernica členským štátom nebráni, aby stanovili prísnejšie záruky, ako sú záruky stanovené v tejto smernici na ochranu práv a slobôd dotknutých osôb, pokiaľ ide o spracúvanie osobných údajov príslušnými orgánmi.“

8. Článok 2 („Rozsah pôsobnosti“) v odseku 1 stanovuje:

„Táto smernica sa vzťahuje na spracúvanie osobných údajov príslušnými orgánmi na účely stanovené v článku 1 ods. 1“

9. V článku 3 s názvom „Vymedzenie pojmov“ sa uvádza:

„Na účely tejto smernice:

…

2. ‚spracúvanie‘ je operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami;

…

7. ‚príslušný orgán‘ je:

   a) akýkoľvek orgán verejnej moci príslušný v oblasti predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania, alebo na účely výkonu trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu, alebo

…“

10. Článok 4, nazvaný „Zásady týkajúce sa spracúvania osobných údajov“, v odseku 1 stanovuje:

„Členské štáty stanovia, že osobné údaje sú:

a) spracúvané zákonným spôsobom a spravodlivo;

b) získané na konkrétne určené, výslovne uvedené a legitímne účely a nesmú byť spracúvané spôsobom, ktorý je nezlučiteľný s týmito účelmi;

c) primerané, relevantné a nie neúmerné vo vzťahu k účelom, na ktoré sa spracúvajú;

…

e) uchovávané vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac dovtedy, kým je to potrebné na účely, na ktoré sa spracúvajú;

f) spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, likvidáciou alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení.“

11. V článku 8, nazvanom „Zákonnosť spracúvania“, sa uvádza:

„1. Členské štáty stanovia, že spracúvanie je zákonné iba vtedy a do takej miery, pokiaľ je nevyhnutné na splnenie úlohy realizovanej príslušným orgánom na účely stanovené v článku 1 ods. 1, a ak je založené na práve Únie alebo na práve členského štátu.

2. Právo členského štátu upravujúce spracúvanie v rámci rozsahu pôsobnosti tejto smernice stanoví aspoň ciele spracúvania, osobné údaje, ktoré sa majú spracúvať, a účely spracúvania.“

12. Článok 13 s názvom „Informácie, ktoré sa majú sprístupniť alebo poskytnúť dotknutej osobe“ stanovuje:

„1. Členské štáty stanovia, že prevádzkovateľ sprístupní dotknutej osobe aspoň tieto informácie:

…

d) právo podať sťažnosť dozornému orgánu a kontaktné údaje dozorného orgánu;

…

3. Členské štáty môžu prijať legislatívne opatrenia, ktorými sa poskytovanie informácií dotknutej osobe podľa odseku 2 odloží, obmedzí alebo sa od neho upustí v takom rozsahu a na tak dlho, ako toto opatrenie s náležitým zreteľom na základné práva a oprávnené záujmy danej fyzickej osoby predstavuje nevyhnutné a primerané opatrenie v demokratickej spoločnosti s cieľom:

a) zabrániť mareniu úradného alebo súdneho zisťovania, vyšetrovania alebo konania;

b) zabrániť ohrozeniu predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo výkonu trestných sankcií;

c) chrániť verejnú bezpečnosť;

d) chrániť národnú bezpečnosť;

e) chrániť práva a slobody iných.

…“

13. Článok 15 s názvom „Obmedzenia práva na prístup“ v odseku 1 stanovuje:

„Členské štáty môžu prijať legislatívne opatrenia, ktorými sa úplne alebo čiastočne obmedzuje právo dotknutej osoby na prístup v takom rozsahu a na tak dlho, ako toto čiastočné či úplné obmedzenie s náležitým ohľadom na základné práva a oprávnené záujmy danej fyzickej osoby predstavuje nevyhnutné a primerané opatrenie v demokratickej spoločnosti s cieľom:

a) zabrániť mareniu úradného alebo súdneho zisťovania, vyšetrovania alebo konania;

b) zabrániť ohrozeniu predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo výkonu trestných sankcií;

c) chrániť verejnú bezpečnosť;

d) chrániť národnú bezpečnosť;

e) chrániť práva a slobody iných.“

14. Podľa článku 27, nazvanom „Posúdenie vplyvu na ochranu údajov“:

„1. Ak typ spracúvania, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účely spracúvania pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, členské štáty stanovia, že prevádzkovateľ pred spracúvaním vykoná posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov.

2. Posúdenie uvedené v odseku 1 obsahuje aspoň všeobecný opis plánovaných spracovateľských operácií, hodnotenie rizík pre práva a slobody dotknutých osôb, opatrenia na riešenie daných rizík, záruky, bezpečnostné opatrenia a mechanizmy na zabezpečenie ochrany osobných údajov a na preukázanie súladu s touto smernicou, s ohľadom na práva a oprávnené záujmy dotknutých osôb a prípadných ďalších osôb.“

15. V článku 28, nazvanom „Predchádzajúca konzultácia s dozorným orgánom“, sa uvádza:

„1. Členské štáty stanovia, že prevádzkovateľ alebo sprostredkovateľ uskutoční konzultácie s dozorným orgánom pred spracúvaním, ktoré bude tvoriť súčasť nového informačného systému, ktorý sa má vytvoriť, ak:

a) je z posúdenia vplyvu na ochranu údajov uvedeného v článku 27 zrejmé, že toto spracúvanie by viedlo k vysokému riziku, ak by prevádzkovateľ neprijal opatrenia na zmiernenie tohto rizika; alebo

b) sa s typom spracúvania, najmä s využitím nových technológií, mechanizmov alebo postupov, spája vysoké riziko pre práva a slobody dotknutých osôb.

…“

16. Článok 54 s názvom „Právo na účinný súdny prostriedok nápravy voči prevádzkovateľovi alebo sprostredkovateľovi“ stanovuje:

„Bez toho, aby bol dotknutý akýkoľvek dostupný správny alebo mimosúdny prostriedok nápravy vrátane práva na podanie sťažnosti dozornému orgánu podľa článku 52, členské štáty stanovia právo dotknutej osoby na účinný súdny prostriedok nápravy, ak sa domnieva, že v dôsledku spracúvania jej osobných údajov v rozpore s ustanoveniami prijatými podľa tejto smernice došlo k porušeniu jej práv stanovených v ustanoveniach prijatých podľa tejto smernice.“

B. Vnútroštátne právo

17. Ustanovenie § 18 Strafprozessordnung[6] stanovuje, že kriminálna polícia plní úlohy v záujme výkonu trestného súdnictva (odsek 1). Za vyšetrovanie, ktoré vedie kriminálna polícia, sú zodpovedné bezpečnostné orgány (odsek 2). Orgány, ktoré plnia úlohy týkajúce sa verejnej bezpečnosti, poskytujú kriminálnej polícii služby výkonných orgánov, ktoré spočívajú vo vyšetrovaní a stíhaní trestných činov (odsek 3).

18. Podľa § 99 StPO kriminálna polícia vedie vyšetrovanie z úradnej moci alebo na základe trestného oznámenia, pričom sa musí riadiť príkazmi prokuratúry a súdov (odsek 1). Ak je na vykonanie vyšetrovacieho opatrenia potrebný príkaz prokuratúry, kriminálna polícia môže vykonať príslušnú právomoc aj bez takého príkazu, pokiaľ hrozí nebezpečenstvo z omeškania. V takom prípade musí bezodkladne požiadať o povolenie (odsek 2).

19. V súlade s § 111 ods. 2 StPO, ak sa majú zaistiť informácie uložené na dátových nosičoch, každý je povinný poskytnúť prístup k týmto informáciám a na základe žiadosti odovzdať elektronický dátový nosič alebo umožniť jeho zhotovenie v bežne používanom súborovom formáte. Okrem toho musí umožniť zhotovenie záložnej kópie informácií uložených na dátových nosičoch.

II. Skutkový stav, spor vo veci samej a prejudiciálne otázky

20. C. G. je nemecký občan, ktorý pracuje a býva v Rakúsku.

21. Dňa 23. februára 2021 úradníci Zollamt Innsbruck (Colný úrad Innsbruck, Rakúsko) počas kontroly týkajúcej sa omamných látok zadržali balík adresovaný C. G., ktorý obsahoval 85 gramov marihuany.

22. Dňa 6. marca 2021 dvaja príslušníci polície vypočuli C. G. v súvislosti s odosielateľom balíka a prehľadali jeho obydlie. Počas tejto prehliadky zaistili jeho mobilný telefón (ktorého súčasťou bola SIM karta a SD karta) a odovzdali mu záznam o zaistení.

23. C. G. bol vyzvaný, aby umožnil prístup k údajom o pripojení svojho mobilného telefónu, čo odmietol, pričom tiež odmietol oznámiť kód na prístup do tohto telefónu.

[6] Trestný poriadok (ďalej len „StPO“). BGBl č. 631/1975, v znení uplatniteľnom v čase skutkových okolností (BGBl I č. 24/2020).

24. Bezirkspolizeikommando Landeck (Okresné policajné komando Landeck, Rakúsko) nebolo schopné odblokovať mobilný telefón. Tento telefón bol zaslaný na Bundeskriminalamt (Spolkový kriminálny úrad) vo Viedni (Rakúsko), kde bol bez úspechu zopakovaný pokus odblokovať ho a načítať uložené údaje.

25. Na uvedené opatrenia sa v čase, keď ich prijala polícia, nevzťahoval príkaz prokuratúry ani súdne rozhodnutie.

26. Dňa 31. marca 2021 podal C. G. sťažnosť proti donucovaciemu opatreniu, ktoré mu bolo uložené, na Landesverwaltungsgericht Tirol (Krajinský správny súd spolkovej krajiny Tirolsko, Rakúsko), pričom napadol zaistenie svojho mobilného telefónu. Tento telefón mu bol vrátený 20. apríla 2021.

27. C. G. nebol informovaný o pokusoch o analýzu obsahu mobilného telefónu a dozvedel sa o nich na základe toho, že príslušník polície, ktorý vykonal zaistenie a neskôr začal digitálnu analýzu, bol vypočutý ako svedok, ktorý je povinný vypovedať pravdu. Tieto pokusy tiež neboli zdokumentované v spise kriminálnej polície.

28. Za týchto okolností Landesverwaltungsgericht Tirol (Krajinský správny súd spolkovej krajiny Tirolsko) položil Súdnemu dvoru nasledujúce prejudiciálne otázky:

„1. Má sa článok 15 ods. 1 (prípadne v spojení s článkom 5) smernice 2002/58, zmenenej smernicou 2009/136/ES, vzhľadom na články 7 a 8 Charty… vykladať v tom zmysle, že prístup orgánov verejnej moci k údajom uloženým v mobilných telefónoch predstavuje zásah do základných práv, ktoré sú zakotvené v týchto článkoch Charty, ktorý je taký závažný, že tento prístup pri zabránení, vyšetrovaní, odhaľovaní a stíhaní trestných činov musí byť obmedzený na boj proti závažnej trestnej činnosti?

2. Má sa článok 15 ods. 1 smernice 2002/58, zmenenej smernicou 2009/136, vzhľadom na články 7, 8 a 11, ako aj článok 52 ods. 1 Charty… vykladať v tom zmysle, že bráni vnútroštátnej právnej úprave, akou je § 18 v spojení s § 99 ods. 1 [StPO], podľa ktorej si bezpečnostné orgány v rámci trestného vyšetrovania bez povolenia súdu alebo nezávislého správneho orgánu samy zaobstarajú úplný a nekontrolovaný prístup ku všetkým digitálnym údajom uloženým v mobilnom telefóne?

3. Má sa článok 47 Charty…, prípadne v spojení s článkami 41 a 52 Charty…, z hľadiska rovnosti zbraní a z hľadiska účinného prostriedku nápravy chápať tak, že bráni právnej úprave členského štátu, ktorá – tak ako § 18 v spojení s § 99 ods. 1 [StPO] – umožňuje digitálnu analýzu mobilného telefónu bez toho, aby sa dotknutá osoba o nej dozvedela predtým alebo aspoň po prijatí tohto opatrenia?“

III. Konanie na Súdnom dvore

29. Návrh na začatie prejudiciálneho konania bol doručený do kancelárie Súdneho dvora 6. septembra 2021.

30. Dňa 20. októbra 2021 Súdny dvor požiadal vnútroštátny súd, aby sa vyjadril, či by pre prejednávanú vec mohla byť relevantná smernica 2016/680.

31. Dňa 11. novembra 2021 vnútroštátny súd odpovedal, že v spore vo veci samej sa má uplatniť smernica 2016/680.

32. Písomné pripomienky predložili nemecká, rakúska, cyperská, dánska, estónska, francúzska, maďarská, írska, holandská, nórska, poľská a švédska vláda, ako aj Európska komisia.

33. Na pojednávaní, ktoré sa konalo 16. januára 2023, sa – s výnimkou nemeckej, maďarskej a poľskej vlády – zúčastnili účastníci prejudiciálneho konania, ktorí predložili písomné pripomienky, ako aj fínska vláda. Súdny dvor všetkých týchto účastníkov prejudiciálneho konania vyzval, aby sa vo svojich vyjadreniach zamerali na smernicu 2016/680 a aby ústne odpovedali na určité otázky súvisiace s ňou.

IV. Analýza

A. Neprípustnosť

34. Vnútroštátny súd pôvodne sformuloval svoje otázky tak, že požiadal len o výklad smernice 2002/58. Takmer všetci účastníci prejudiciálneho konania sa však zhodujú na tom, že táto smernica sa neuplatní na prejednávanú vec a v dôsledku toho jej výklad tiež nie je nevyhnutný na rozhodnutie sporu.

35. Smernica 2002/58 podľa jej článku 3 upravuje „… spracúvanie osobných údajov v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb vo verejných komunikačných sieťach v [Únii] vrátane verejných komunikačných sietí, ktoré podporujú zariadenia na zber údajov a identifikáciu“.

36. Súdny dvor rozhodol, že „ak členské štáty priamo vykonajú opatrenia, ktoré predstavujú výnimku zo zásady dôvernosti elektronických komunikácií, bez toho, aby ukladali povinnosť spracovávania poskytovateľom takýchto komunikačných služieb, na ochranu údajov dotknutých osôb sa nevzťahuje smernica 2002/58, ale len vnútroštátne právo, s výhradou uplatnenia [smernice 2016/680]“ [7].

37. V prejednávanej veci pokus o prístup k údajom vykonali priamo policajné orgány v rámci trestného vyšetrovania. Nedošlo k zásahu poskytovateľov elektronických komunikačných služieb, ktorí neboli požiadaní o poskytnutie osobných údajov. Smernica 2002/58 sa teda neuplatní.

38. Právnym predpisom Únie, ktorý upravuje túto situáciu, je smernica 2016/680, ktorá v článku 2 ods. 1 stanovuje, že sa vzťahuje na spracúvanie osobných údajov príslušnými orgánmi na „účely… vyšetrovania“ trestných činov.

39. Vyššie uvedené by postačovalo na priklonenie sa k záveru, že návrh na začatie prejudiciálneho konania v podobe, v akej ho podal vnútroštátny súd, je neprípustný, keďže právny predpis Únie, o výklad ktorého tento súd požiadal, sa nevzťahoval na danú vec.

[7] Rozsudok zo 6. októbra 2020, La Quadrature du Net a i. (C-511/18, C-512/18 a C-520/18, EU:C:2020:791; ďalej len „rozsudok La Quadrature du Net“, bod 103).

40. Je však pravda, že článok 267 ZFEÚ dovoľuje, aby Súdny dvor preformuloval otázky, ktoré sú mu položené, alebo poukázal na existenciu iných prípadne relevantných ustanovení práva Únie, aby poskytol vnútroštátnemu súdu užitočnú odpoveď. [8]

41. Súdny dvor požiadal vnútroštátny súd, aby sa vyjadril k prípadnému vplyvu smernice 2016/680. Poskytol teda vnútroštátnemu súdu možnosť, aby sám doplnil alebo preformuloval svoje otázky. Vnútroštátny súd namiesto toho, aby to urobil, len oznámil, že „v prejednávanej veci je v každom prípade potrebné dodržať ustanovenia smernice 2016/680“, pričom však neuviedol ustanovenia tejto smernice, o ktorých má pochybnosti, ani neuviedol iné podrobnejšie vecné úvahy. [9]

42. Súdny dvor opakovane rozhodol, že „je… nevyhnutné, ako stanovuje článok 94 písm. c) rokovacieho poriadku, aby návrh na začatie prejudiciálneho konania obsahoval uvedenie dôvodov, pre ktoré sa vnútroštátny súd rozhodol položiť otázku o výklade alebo platnosti určitých ustanovení práva Únie, ako aj súvislosť, ktorú vnútroštátny súd vidí medzi týmito ustanoveniami a svojou právnou úpravou uplatniteľnou v spore vo veci samej“ [10].

43. Vzhľadom na vyššie uvedené je pritom jednoznačné, že v tomto prejudiciálnom konaní nie sú splnené požiadavky článku 94 rokovacieho poriadku. Aj keď je Súdny dvor v tomto smere do určitej miery flexibilný, spolupráca s vnútroštátnym súdom musí byť vzájomná: ak vnútroštátny súd bezdôvodne nespolupracuje a neopíše svoje pochybnosti týkajúce sa výkladu právneho predpisu Únie, ktorý sa podľa jeho názoru uplatní (v tomto prípade smernice 2016/680), považujem za logické určiť, že návrh na začatie prejudiciálneho konania je neprípustný. [11]

44. Uvedený súd navyše:

– nespresnil povahu spracúvania, ktoré sa pokúsili vykonať policajné orgány, alebo konkrétne hľadaných osobných údajov. Najprv podľa všetkého uvádza, že toto spracovanie bolo obmedzené na údaje o pripojení (teda údaje o prenose dát a polohe), ale neskôr nevylučuje, že odblokovanie telefónu umožní prístup ku „všetkým [uloženým] digitálnym údajom“ [12] a dokonca aj k obsahu komunikácie a elektronických správ zasielaných a prijímaných prostredníctvom neho, [13]

– hovorí tak o zaistení telefónu a o prístupe alebo pokuse o prístup k údajom, ktoré sú v ňom uložené, ako aj o ich následnom „využití“ (*Auswertung*), teda o ich analýze a prehliadaní. Ďalej uvádza, že toto prehliadanie „znamená úplný a nekontrolovaný prístup k celej digitálnej komunikácii dotknutej osoby“, čo umožňuje „rekonštrukciu veľmi podrobného a hĺbkového obrazu takmer všetkých oblastí súkromného života“.

8 Pozri napríklad rozsudok z 28. apríla 2016, Oniors Bio (C-233/15, EU:C:2016:305, bod 30).

9 Súdny dvor bol nútený vyzvať účastníkov konania, aby uviedli, „ktoré sú podľa ich názoru relevantné ustanovenia smernice 2016/680, vzhľadom na ktoré by Súdny dvor prípadne mal preformulovať tri prejudiciálne otázky položené vnútroštátnym súdom“ (štvrtá zo zaslaných otázok, ktoré mali byť ústne zodpovedané na pojednávaní).

10 Rozsudok zo 6. októbra 2021, Consorzio Italian Management a Catania Multiservizi (C-561/19, EU:C:2021:799, bod 69).

11 Pokiaľ ide o toto konštatovanie, súhlasím s francúzskou vládou (body 36 až 41 jej písomných pripomienok).

12 Tak je to uvedené v druhej prejudiciálnej otázke.

13 Vnútroštátny súd uvádza, že „v súvislosti s údajmi o pripojení sa dajú rekonštruovať takmer všetky kontakty podľa frekvencie, času a trvania komunikácie; v súvislosti s komunikáciou vedenou prostredníctvom SMS a iných služieb posielania správ aj obsah; analýzou uložených fotografií a histórie prehliadania sa tiež získa veľmi intímny pohľad do súkromného života dotknutej osoby“.

45. Za týchto podmienok by Súdny dvor namiesto *preformulovania* otázok vnútroštátneho súdu vykonal skutočnú *rekonštrukciu* návrhu na začatie prejudiciálneho konania, ktorá by bola navyše sčasti založená skôr na hypotetických úvahách než na preukázaných skutkových okolnostiach. Zdôrazňujem, že Súdny dvor by to urobil po tom, čo vnútroštátnemu súdu poskytol možnosť, aby sám doplnil alebo preformuloval svoje otázky.

46. Odporúčam teda určiť, že návrh na začatie prejudiciálneho konania je neprípustný, ako to navrhli viaceré štáty, ktoré vstúpili do konania.

47. K tomu istému určeniu neprípustnosti by mala viesť okolnosť, na ktorú sa poukázalo na pojednávaní, že vnútroštátny súd už neprejednáva skutočný spor, ktorý by si vyžadoval výklad ustanovení práva Únie.

48. Rakúska vláda (pod ktorú spadajú policajné orgány, ktoré konali v rámci vyšetrovania) totiž uznáva, že postup týchto orgánov bol nezákonný a boli ním porušené práva dotknutej osoby. Keďže podľa rozhodnutia vnútroštátneho súdu návrh sťažovateľa v konaní na správnom súde smeroval práve proti policajným opatreniam, ktoré správny orgán, ktorý je odporcom v tomto konaní, považuje za nezákonné, spor, o ktorom mal vnútroštátny súd rozhodnúť, zanikol.

49. Pre prípad, že Súdny dvor by sa nestotožnil s mojím názorom, tak či tak ďalej v týchto návrhoch subsidiárne preskúmam vecné problémy, na ktorých sú založené prejudiciálne otázky.

50. Domnievam sa však, že najprv je potrebné vylúčiť existenciu iného dôvodu neprípustnosti, ktorý uviedli niektorí z účastníkov prejudiciálneho konania.[14] Podľa ich názoru vzhľadom na to, že smernica 2016/680 sa týka ochrany fyzických osôb pri *spracúvaní* ich údajov, neupravuje prípady, ako je prejednávaný prípad, v ktorých nedošlo k spracúvaniu, ale len k *pokusu o prístup k* údajom, ktoré napokon nebolo možné získať.

51. Podľa Komisie by sa naopak v záujme potrebného účinku smernice 2016/680 mal uprednostniť výklad jej predmetu úpravy, ktorý nebude obmedzený na spracúvanie údajov v užšom zmysle, ale ktorý bude zahŕňať aj otázky priamo súvisiace s týmto spracovaním. Komisia sa domnieva, že jednou z týchto otázok je pokus o prístup k údajom, ktoré sa majú spracúvať.[15]

52. Podľa môjho názoru bez toho, aby bolo potrebné posunúť hranice pôsobnosti smernice 2016/680[16], jej uplatnenie na prejednávaný prípad nie je odôvodnené preto, lebo došlo k zaisteniu mobilného telefónu[17], ale je odôvodnené následným postupom policajných orgánov, ktorého cieľom bolo získať z neho určité osobné údaje dotknutej osoby, pričom na tento účel sa pokúsili odblokovať ho a umožniť prístup k jeho obsahu.

[14] Mám na mysli konkrétne rakúsku, francúzsku, holandskú a nórsku vládu.

[15] Podľa Komisie „je irelevantné, či boli pokusy napokon úspešné alebo nie. Vznik technických ťažkostí, ktoré bránia úspechu pokusom o prístup, je okolnosťou, ktorú nemožno vopred zistiť a ktorá nemá vplyv na riziká pre ochranu osobných údajov“.

[16] Považujem najmä za zbytočné použiť články 27 a 28 smernice 2016/680, ako to navrhuje Komisia vo svojich písomných pripomienkach. „Posúdenie vplyvu na ochranu údajov“ stanovené v článku 27 sa všeobecne týka „typ[u] spracúvania“, a nie konkrétnych alebo osobitných spracúvaní. Vyplýva to z odôvodnenia 58 smernice 2016/680, v ktorom sa uvádza, že „posúdenia vplyvu by sa mali týkať príslušných systémov a procesov spracovateľských operácií, ale *nie konkrétnych prípadov*“ (kurzívou zvýraznil generálny advokát). Komisia na pojednávaní spresnila dôvody, pre ktoré sa odvolala na tieto dve ustanovenia, pričom uviedla, že ich citovala len s cieľom poukázať na to, že smernica 2016/680 tiež upravuje situácie predchádzajúce spracúvaniu údajov v pravom zmysle slova.

[17] Smernica 2016/680 neupravuje zaistenie telefónu ako dôkazného prostriedku v rámci trestného vyšetrovania.

53. Medzi operáciami, ktoré sú v článku 3 bode 2 smernice 2016/680 vymedzené ako „spracúvanie“, sa nachádza „poskytovanie [osobných údajov] iným spôsobom“, ktoré sa vykonáva v priebehu trestného vyšetrovania. Domnievam sa, že ak policajný orgán zaistí telefón, v ktorom sú uložené tieto údaje, a manipuluje s ním s cieľom získať z neho tieto údaje, začne spracovateľskú „operáciu“, hoci táto operácia pre technické dôvody týkajúce sa šifrovacieho zabezpečenia zlyhá.

54. Na neúspešný pokus o prístup k osobným údajom uchovávaným v mobilnom telefóne počas trestného vyšetrovania sa uplatní smernica 2016/680 z dôvodov podobných dôvodom, pre ktoré Súdny dvor rozhodol, že smernica 2002/58 sa uplatní na (rovnako neúspešný) pokus o získanie povolenia súdu na účely získania prístupu k určitým údajom vyšetrovanej osoby, ktorými disponuje poskytovateľ elektronických komunikačných služieb. [18]

55. Za uvedených okolností, ak by vnútroštátny súd musel rozhodnúť o nezákonnosti postupu policajných orgánov (ktorú rakúska vláda – ako som už uviedol – uznáva), jej posúdenie by mohlo závisieť od zákonnosti účelu, ktorý sa má týmto postupom dosiahnuť, a to tak v prípade, ak bolo toto opatrenie úspešné, ako aj v prípade, ak sa len neúspešne začalo vykonávať.

B. O veci samej

1. Prvá prejudiciálna otázka

56. Vnútroštátny súd sa pýta, či podľa článku 15 ods. 1 (prípadne v spojení s článkom 5) smernice 2002/58 a vzhľadom na články 7 a 8 Charty „prístup orgánov verejnej moci k údajom uloženým v mobilných telefónoch predstavuje zásah do základných práv, ktoré sú zakotvené v týchto článkoch Charty, ktorý je taký závažný, že tento prístup pri zabránení, vyšetrovaní, odhaľovaní a stíhaní trestných činov musí byť obmedzený na boj proti závažnej trestnej činnosti“.

57. Ak by bol návrh na začatie prejudiciálneho konania prípustný, vzhľadom na neuplatniteľnosť smernice 2002/58 by bolo potrebné preformulovať prvú otázku, aby sa v odpovedi Súdneho dvora podal výklad smernice 2016/680.

58. V uvedenej odpovedi by sa muselo postupne objasniť, či možno v prípadoch, ako je prejednávaný prípad, hovoriť o zásahu, a ak ide o zásah, či smernica 2016/680 vyžaduje, aby bol prístup k údajom obmedzený na prípady boja proti závažnej trestnej činnosti.

59. Operácie spracúvania údajov môžu, prirodzene, ohroziť právo na rešpektovanie súkromného života (článok 7 Charty) a na ochranu osobných údajov (článok 8 Charty). Orgány verejnej moci preto musia pri odôvodnení svojho zásahu do výkonu uvedených základných práv dodržiavať podmienky stanovené v článku 52 ods. 1 Charty.

60. Zásah do práv chránených článkami 7 a 8 Charty je o to väčší, ak sa ním: a) má získať prístup k citlivým údajom, ktoré sa obvykle uchovávajú v mobilných telefónoch a ktorých znalosť môže odhaliť aspekty života ich majiteľov, o ktorých sa tretie osoby nesmú dozvedieť, a b) umožňuje prístup k obsahu komunikácie.

[18] Rozsudok z 2. októbra 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788).

61. Zo všeobecného hľadiska a vzhľadom na jej obsah však smernicu 2016/680 nemožno vykladať v tom zmysle, že spracúvanie údajov, ktorých sa táto smernica týka, je obmedzené len na prípady boja proti závažnej trestnej činnosti.

62. Predmetom úpravy smernice 2016/680 je ktorákoľvek operácia spočívajúca v spracúvaní [19] osobných údajov príslušnými orgánmi na účely predchádzania *všetkým druhom* trestných činov, ich vyšetrovania, odhaľovania alebo stíhania.

63. Zo zásad, ktoré smernica 2016/680 zavádza, pokiaľ ide o spracúvanie osobných údajov s uvedeným účelom (článok 4), alebo z podmienok zákonnosti tohto spracúvania (článok 8) nevyplýva, že spracúvanie údajov je spravidla prípustné len v prípadoch týkajúcich sa závažnej trestnej činnosti.

64. Obmedzenie len na prípady týkajúce sa boja proti závažnej trestnej činnosti by nemohlo byť založené ani na automatickom uplatnení judikatúry Súdneho dvora týkajúcej sa smernice 2002/58 [20] na prípady, ako je prejednávaný prípad.

65. Podľa môjho názoru to nie je možné preto, lebo – bez toho, aby boli dotknuté nižšie uvedené úvahy – spomenutá judikatúra sa týka všeobecného a nediferencovaného uchovávania osobných údajov všeobecného a neurčeného okruhu osôb, ktoré systematicky vykonávajú poskytovatelia elektronických komunikačných služieb. Vzhľadom na závažnosť zásahu, ktorý takéto uchovávanie predstavuje pre celú spoločnosť, Súdny dvor postupoval pri uložení zákazu takého uchovávania a stanovení výnimiek z tohto zákazu obzvlášť prísne.

66. Nie je to tak v prípade, ak sa požadovaný prístup nedotýka všetkých obyvateľov alebo veľkých skupín obyvateľov (teda osobných údajov všeobecného a neurčeného okruhu osôb), ale informácií uložených v konkrétnom mobilnom telefóne v rámci trestného vyšetrovania, ktoré je tiež konkrétne a ktoré osobitne upravuje smernica 2016/680.

67. Predmetom úpravy smernice 2016/680 je práve spracúvanie údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania, pričom ide o všetky druhov trestných činov, a nie len o závažné trestné činy.

68. Okrem toho, ako zdôraznili niektorí z účastníkov prejudiciálneho konania, pokiaľ v smernici 2016/680 nie je vôbec uvedená závažnosť trestných činov, je možné, že táto smernica by sa neuplatňovala v členských štátoch jednotne, keďže posudzovanie miery závažnosti trestného činu v jednotlivých vnútroštátnych právnych poriadkoch sa značne odlišuje. [21]

69. Smernica 2016/680 v konečnom dôsledku nestanovuje ako podmienku zákonnosti, že spracúvanie osobných údajov, ktoré je v nej upravené, je možné len na účely boja proti závažnej trestnej činnosti.

[19] Okruh „operácií“ uvedených v článku 3 bode 2 smernice 2016/680 je veľmi široký. Pozri citáciu tohto ustanovenia v bode 9 vyššie.

[20] Rozsudok La Quadrature du Net, ako aj rozsudky z 21. decembra 2016, Tele2 Sverige a Watson a i. (C-203/15 a C-698/15, EU:C:2016:970; ďalej len „rozsudok Tele2 Sverige a Watson“); z 2. októbra 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788); zo 6. októbra 2020, Privacy International (C-623/17, EU:C:2020:790), a z 2. marca 2021, Prokuratuur (Podmienky prístupu k údajom týkajúcim sa elektronických komunikácií) (C-746/18, EU:C:2021:152; ďalej len „rozsudok Prokuratuur“).

[21] Francúzska vláda uvádza ako príklad trestné činy prechovávania omamných látok a obchodovania s nimi, ktorých závažnosť sa podľa rakúskych a francúzskych trestných predpisov posudzuje odlišne. V podobnom zmysle sa vyjadrila švédska vláda.

70. Vyššie uvedené nebráni tomu, aby sa spracúvanie údajov, ktoré chcú príslušné orgány uskutočniť na základe smernice 2016/680, na základe zásady proporcionality v individuálnom prípade muselo prispôsobiť v závislosti od: a) povahy trestných činov, pre ktoré sa vedie trestné stíhanie, a b) druhu osobných údajov, ktoré majú byť predmetom tohto spracúvania.

71. V uvedenom zmysle súhlasím s niektorými tvrdeniami nemeckej vlády týkajúcimi sa obmedzenia prístupu k údajom na zaistenom telefóne, ak vzhľadom na digitálny obsah tohto telefónu umožňujú vytvoriť úplný profil osobnosti jeho majiteľa. Podľa nemeckej vlády by mal byť uvedený prístup obmedzený na údaje, ktoré sú potrebné ako dôkazný prostriedok v konkrétnom prípade, a nemusel by byť primeraný v prípade faktorov, akými sú „malá závažnosť vyšetrovaného trestného činu alebo nízka dôkazná hodnota údajov, ktoré sa majú získať“ [22].

72. Z *abstraktného* hľadiska teda zo smernice 2016/680 nevyplýva, že prístup k osobným údajom uloženým v mobilnom telefóne s cieľom uľahčiť vyšetrovanie týkajúce sa skutkov, ktoré možno zaradiť medzi všeobecné alebo bežné trestné činy, je systémovo nezákonný. Otázku, či je tento prístup v *konkrétnom* prípade prípustný, musí príslušný orgán posúdiť v danej situácii, a to so zreteľom na jeho nevyhnutnosť a na kritérium proporcionality, ktoré som spomenul vyššie.

73. Podľa môjho názoru to vyplýva z ustanovení smernice 2016/680, ktoré stanovujú podmienky platnosti spracúvania osobných údajov v rámci boja proti trestnej činnosti:

– článok 4 ods. 1 písm. a), podľa ktorého údaje musia byť „spracúvané zákonným spôsobom“,

– článok 8 ods. 1, v ktorom sa zdôrazňuje, že spracúvanie musí byť *nevyhnutné* a založené na práve Únie alebo na práve členského štátu.

2. Druhá prejudiciálna otázka

74. Svojou druhou prejudiciálnou otázkou sa vnútroštátny súd pýta, či článok 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8, 11 a 52 ods. 1 Charty „bráni vnútroštátnej právnej úprave, akou je § 18 v spojení s § 99 ods. 1 [StPO], podľa ktorej si bezpečnostné orgány v rámci trestného vyšetrovania bez povolenia súdu alebo nezávislého správneho orgánu samy zaobstarajú úplný a nekontrolovaný prístup ku všetkým digitálnym údajom uloženým v mobilnom telefóne“.

75. Znenie tejto otázky je do určitej miery nejednoznačné. Vnútroštátny súd:

– uznáva, že § 110 ods. 2 StPO stanovuje, že na zaistenie veci sa v zásade vyžaduje povolenie prokuratúry. Policajný orgán môže zaistiť vec bez takého povolenia len v mimoriadnych situáciách uvedených v § 110 ods. 3 StPO (o ktoré v tomto prípade zrejme nejde);

– však ďalej uvádza, že analýza informácií uložených v mobilných telefónoch „nie je [v StPO] jednoznačne upravená“ a že bezpečnostné orgány ju môžu vykonať z vlastnej iniciatívy bez predchádzajúceho povolenia.

[22] Písomné pripomienky nemeckej vlády, bod 20.

76. Rakúska vláda uvádza znenie vnútroštátnej právnej úpravy, ktoré sa nezhoduje so znením uvedeným v rozhodnutí vnútroštátneho súdu. Najmä tvrdí, že podľa vnútroštátneho práva sú tak zaistenie telefónu (s výnimkou naliehavých prípadov), ako aj analýza údajom, ktoré sú v ňom uložené, možné len s povolením prokuratúry.[23] Využitie údajov uložených v tomto telefóne bez príkazu prokuratúry policajnými orgánmi je nezákonné.

77. Je úlohou vnútroštátneho súdu overiť znenie vnútroštátnej právnej úpravy. V konaní podľa článku 267 ZFEÚ nemá Súdny dvor právomoc vykladať vnútroštátne právo a jedine vnútroštátnemu súdu prináleží určiť presný rozsah vnútroštátnych zákonov, iných právnych predpisov a správnych opatrení.[24]

78. Hoci nechcem zasahovať do sporu týkajúceho sa výkladu rakúskeho práva, považujem za zložité vyvodiť len z ustanovení, ktoré uvádza vnútroštátny súd (§ 18 v spojení s § 99 ods. 1 StPO) dôsledok, ktorý vyvodzuje tento súd. Opakujem však, že o tom môže rozhodnúť len uvedený súd.

79. V každom prípade vnútroštátny súd sa domnieva, že na prípad, o aký ide v prejednávanej veci, možno uplatniť judikatúru sformulovanú v rozsudku Prokuratuur[25], ktorá sa týka predchádzajúceho preskúmania prístupu k uchovávaným údajom zo strany súdu alebo nezávislého správneho orgánu.

80. Holandská vláda naopak zastáva názor, že uvedenú judikatúru treba chápať v kontexte vnútroštátnej právnej úpravy, ktorá dovoľovala *všeobecný* prístup príslušných orgánov ku *všetkým* uchovávaným údajom o prenose dát a polohe. Tvrdí, že to vysvetľuje požiadavku predchádzajúceho súdneho povolenia, ktorá však nemusí byť opodstatnená v prípade prístupu k údajom na jedinom mobilnom telefóne.

81. Nórska vláda v tom istom zmysle tvrdí, že medzi mnohými zárukami stanovenými v smernici 2016/680[26] nie je výslovne uvedená záruka nevyhnutnosti predchádzajúceho povolenia súdu alebo nezávislého správneho orgánu.

82. Komisia, ktorá vychádza z toho, že ustanovenia smernice 2016/680 sa majú vykladať vzhľadom na Chartu, tvrdí, že povinnosť uložená členským štátom v článku 8 ods. 1 tejto smernice (podmienky zákonnosti spracúvania) zahŕňa potrebu rešpektovať základné práva zaručené v článkoch 7 a 8 Charty.

83. Súhlasím s Komisiou v tom, že vnútroštátni zákonodarcovia sú – pri rešpektovaní uvedených ustanovení Charty – povinní vymedziť pravidlá potrebné na zabezpečenie toho, aby prístup k údajom bol v každom prípade odôvodnený a obmedzený na to, čo je striktne nevyhnutné a primerané.

[23] Bod 19 písomných pripomienok rakúskej vlády. Táto vláda cituje rozhodnutie Oberster Gerichtshof (Najvyšší súd, Rakúsko) z 13. októbra 2020 (vec 11 Os 56/20z), v ktorom sa konštatuje, že analýza údajov v mobilnom telefóne kriminálnou políciou bez povolenia prokuratúry je nezákonná, lebo porušuje subjektívne práva dotknutej osoby.

[24] Pozri napríklad rozsudok z 28. apríla 2022, SeGEC a i. (C-277/21, EU:C:2022:318, bod 21).

[25] Rozsudok Prokuratuur (bod 51): „je nevyhnutné, aby prístup príslušných vnútroštátnych orgánov k uchovávaným údajom podliehal predchádzajúcemu preskúmaniu zo strany súdu alebo nezávislého správneho orgánu a aby rozhodnutie tohto súdu alebo orgánu nasledovalo po odôvodnenej žiadosti týchto orgánov podanej v rámci konania týkajúceho sa predchádzania trestným činom, ich odhaľovania a stíhania“.

[26] Okrem záruk stanovených v článkoch 4 a 8 sú to záruky obsiahnuté v kapitolách III („Práva dotknutej osoby“), IV („Prevádzkovateľ a sprostredkovateľ“), VI („Nezávislé dozorné orgány“) a VIII („Prostriedky nápravy, zodpovednosť a sankcie“).

84. Také vnútroštátne predpisy však nemusia osobitne upravovať prístup k osobným údajom uloženým – tak ako v tomto prípade – v mobilnom telefóne, ale môžu to byť predpisy, ktoré vo vnútroštátnom práve všeobecne upravujú získavanie dôkazov.

85. V tejto súvislosti som už citoval bod 103 rozsudku La Quadrature du Net, pokiaľ ide o opatrenia členských štátov, ktoré sa týkajú dôvernosti elektronických komunikácií, bez toho, aby ukladali povinnosť spracovávania poskytovateľom takýchto komunikačných služieb.[27]

86. Bez toho, aby bolo potrebné vyvodiť zo smernice 2016/680 *osobitné* procesné pravidlá na zaručenie zákonnosti prístupu k údajom uloženým v mobilnom telefóne,[28] sa preto uplatnia vnútroštátne predpisy, ktoré upravujú výkon právomocí vykonať prehliadku a zaistiť vec v rámci trestného stíhania.[29]

87. Odkaz na vnútroštátne právne predpisy na účely zaručenia zákonnosti prístupu podľa smernice 2016/680 je navyše v súlade s judikatúrou ESĽP. Práve v prípade týkajúcom sa Rakúskej republiky, ktorý sa týkal článku 8 EDĽP (právo na rešpektovanie súkromného a rodinného života, ako aj obydlia a korešpondencie), ESĽP konštatoval, že rakúske právne predpisy týkajúce sa zaistenia vecí a najmä listín sa uplatnia na prehliadku a zaistenie údajov uchovávaných na elektronických nosičoch.[30]

88. Ak – ako tvrdí rakúska vláda, ktorá cituje judikatúru Oberster Gerichtshof (Najvyšší súd, Rakúsko) – policajné orgány nie sú oprávnené získať prístup k údajom uloženým v určitom mobilnom telefóne bez povolenia prokuratúry, druhá prejudiciálna otázka je do veľkej miery bezpredmetná.

89. V každom prípade odpoveď na uvedenú otázku nemôže vylúčiť, že prístup k osobným údajom v zaistenom telefóne povedie k „rekonštrukcii veľmi podrobného a hĺbkového obrazu takmer všetkých oblastí súkromného života“ dotknutej osoby.[31] Ak je to tak, policajné orgány nemôžu konať bez predchádzajúceho povolenia, ktoré bolo spomenuté v rozsudku Prokuratuur.

90. Na prvý pohľad by sa mohlo zdať, že toto konštatovanie nie je v súlade s neuplatnením smernice 2002/58 (ktorej výklad bol podaný v rozsudku Prokuratuur) na prejednávaný prípad, ako som to uviedol vyššie. Domnievam sa však, že *ratio* tohto rozsudku podporuje rovnaké riešenie.

91. V spore, v ktorom bol vydaný rozsudok Prokuratuur, boli síce pri prístupe získané údaje (metaúdaje) poskytovateľov elektronických komunikačných služieb, no tento spor sa týkal – tak ako prejednávaná vec – konkrétneho trestného vyšetrovania vedeného proti určitej osobe. Išlo o získanie „údajov viacerých telefónnych čísel [tejto osoby] a jej rôznych medzinárodných identifikačných kódov mobilného zariadenia“[32].

27 Pozri bod 36 vyššie.

28 O náročnosti tejto činnosti svedčí skutočnosť, že Komisia sa v bodoch 34 až 39 svojich písomných pripomienok pokúsila prispieť k vymedzeniu jasných a presných pravidiel na stanovenie hraníc a primeraných záruk v súvislosti s prístupom k údajom v mobilnom telefóne.

29 Ako pripomína napríklad dánska a írska vláda, tieto predpisy nepatria do pôsobnosti práva Únie, ale môžu slúžiť na splnenie požiadavky vyplývajúcej z práva Únie.

30 Rozsudok ESĽP zo 16. októbra 2007, Wieser a Bicos Beteiligungen v. Rakúsko (CE:ECHR:2007:1016JUD007433601, bod 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 Pozri konštatovania vnútroštátneho súdu citované v bode 44 vyššie.

32 Rozsudok Prokuratuur (bod 17).

92. V rozsudku Prokuratuur možno podľa môjho názoru rozlíšiť dve roviny: a) rovinu, v ktorej sa spochybňuje všeobecná právna úprava členského štátu týkajúca sa všeobecného a nediferencovaného uchovávania a neskoršieho prístupu k údajom, ktoré majú k dispozícii poskytovatelia služby, a b) rovinu predchádzajúceho preskúmania prístupu k týmto metaúdajom v konkrétnom prípade, ak umožňujú vytvoriť presný profil súkromného života určitej osoby.

93. Nazdávam sa, že okolnosť, že v prejednávanej veci údaje týkajúce sa súkromného života nemajú k dispozícii poskytovatelia služby a tieto údaje boli získané (alebo došlo k pokusu o ich získanie) z jediného zaisteného telefónu, má druhoradý význam v porovnaní s dôvodom existencie povinnosti týkajúcej sa predchádzajúceho preskúmania, na ktorú sa poukazuje v rozsudku Prokuratuur.

94. Toto predchádzajúce preskúmanie je v konečnom dôsledku založené na ochrane, ktorú zaručujú články 7 a 8 Charty. Orgán, ktorý ho vykonáva, musí byť „schopný zabezpečiť spravodlivú rovnováhu medzi záujmami súvisiacimi s potrebami vyšetrovania v rámci boja proti trestnej činnosti na jednej strane a základnými právami na rešpektovanie súkromného života a na ochranu osobných údajov osôb, ktorých údaje sú predmetom prístupu, na druhej strane“ [33].

3. Tretia prejudiciálna otázka

95. Treťou prejudiciálnou otázkou sa vnútroštátny súd pýta, či článok 47 (prípadne v spojení s článkami 41 a 52) Charty bráni právnej úprave, akou je rakúska právna úprava, [34] ktorá „umožňuje digitálnu analýzu mobilného telefónu bez toho, aby sa dotknutá osoba o nej dozvedela predtým alebo aspoň po prijatí tohto opatrenia“.

96. Domnievam sa, že takto sformulovaná otázka by mohla byť zbytočná na vyriešenie sporu, lebo dotknutá osoba mohla uplatniť právo zakotvené v článku 47 Charty a navrhnúť, aby vnútroštátny súd určil, že úkony policajných orgánov týkajúcich sa zaisteného telefónu, ktorých súčasťou bolo neskoršie (neúspešné) využitie údajov uložených v tomto telefóne, sú neplatné.

97. V súvislosti s týmito dvoma úkonmi policajných orgánov by bolo potrebné rozlíšiť:

– pokiaľ ide o zaistenie telefónu ako také, informácie obsiahnuté v spise svedčia o tom, že dotknutá osoba o ňom vedela a pri jeho zaistení odmietla poskytnúť policajným orgánom kód na jeho odblokovanie,

– pokiaľ ide o pokus o analýzu údajov, všetko nasvedčuje tomu, že prevádzkovateľ neinformoval dotknutú osobu o spracúvaní, aj keď rakúska vláda tvrdí, že táto osoba vedela o správe, v ktorej boli uvedené úkony kriminálnej polície týkajúce sa telefónu. [35]

98. Existujú teda určité nejasnosti týkajúce sa využitia údajov a vedomosti dotknutej osoby o ich využití, ktoré – ako som už poznamenal – mal vnútroštátny súd objasniť vo svojom návrhu na začatie prejudiciálneho konania a ktoré bránia účinnému zodpovedaniu tretej prejudiciálnej otázky.

[33] Rozsudok Prokuratuur (bod 52).

[34] Opäť sa odvoláva na § 18 v spojení s § 99 StPO.

[35] Bod 37 jej písomných pripomienok.

99. Pre prípad, že by Súdny dvor nepovažoval túto otázku za neprípustnú, sa k nej vyjadrím. V takom prípade by – vzhľadom na neuplatniteľnosť smernice 2002/58 – bolo potrebné preformulovať túto otázku vzhľadom na smernicu 2016/680, ktorej články 13, 15 a 54 poskytujú usmernenia na jej zodpovedanie.

100. Podľa smernice 2016/680 sa dotknutej osobe musia poskytnúť informácie o spracúvaní jej údajov, ktoré sú potrebné okrem iného na to, aby táto osoba mohla: a) podať sťažnosť dozornému orgánu [článok 13 ods. 1 písm. d)] a b) podať účinný súdny prostriedok nápravy v prípade porušenia práv zaručených smernicou 2016/680, a to bez toho, aby boli dotknuté dostupné správne alebo mimosúdne prostriedky nápravy (článok 54).

101. Netreba však zabúdať na to, že tak článok 13 ods. 3, ako aj článok 15 ods. 1 smernice 2016/680 dovoľujú členským štátom, aby prijali legislatívne opatrenia, ktorými

– sa poskytovanie informácií dotknutej osobe podľa článku 13 ods. 2 odloží, obmedzí alebo sa od neho upustí,

– sa úplne alebo čiastočne obmedzuje právo dotknutej osoby na prístup k spracúvaným údajom v takom rozsahu a na tak dlho, ako toto obmedzenie predstavuje nevyhnutné a primerané opatrenie s cieľom zabrániť mareniu úradného alebo súdneho vyšetrovania alebo konania alebo ohrozeniu vyšetrovania trestných činov. [36]

102. V každom prípade zákonnosť spracúvania údajov nezávisí od toho, či si príslušné orgány splnia (neskoršie) povinnosti, ktoré im ukladá článok 13 smernice 2016/680, ale od zákonnosti účelu, ktorým bolo toto spracúvanie odôvodnené, teda od toho, či uvedené správne orgány boli oprávnené vykonať spracúvanie osobných údajov.

103. Z tohto hľadiska otázka, či dotknutá osoba bolo informovaná o pokusoch o prístup k údajom uloženým v jej telefóne, ktorý bol zaistený, sama osebe nesúvisí so zákonnosťou hmotnoprávnych dôvodov úkonov policajných orgánov. Správanie prevádzkovateľa, ktoré je prípadne v rozpore s povinnosťami, ktoré mu vyplývajú z článku 13 smernice 2016/680, môže mať iné dôsledky, ale – pripomínam – ako také nemá vplyv na zákonnosť alebo nezákonnosť tohto spracúvania.

104. Prináleží vnútroštátnemu súdu určiť, či vnútroštátna právna úprava umožňuje, aby dotknutá osoba účinným spôsobom uplatnila uvedené práva.

V. Návrh

105. Vzhľadom na vyššie uvedené navrhujem, aby Súdny dvor rozhodol, že návrh na začatie prejudiciálneho konania, ktorý podal Landesverwaltungsgericht Tirol (Krajinský správny súd spolkovej krajiny Tirolsko, Rakúsko), je neprípustný.

[36] Pozri v tomto zmysle rozsudok Tele2 Sverige a Watson (bod 121). Judikatúru týkajúcu sa smernice 2002/58, ktorá je v ňom obsiahnutá, možno uplatniť aj na smernicu 2016/680 v súvislosti so zárukou súdnej ochrany práv majiteľov spracúvaných údajov.

Subsidiárne navrhujem odpovedať na uvedený návrh takto:

1. Článok 4 ods. 1 písm. a) a článok 8 ods. 1 smernice Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV v spojení s článkami 7, 8 a 52 Charty základných práv Európskej únie

   sa majú vykladať v tom zmysle, že:

   prístup orgánov verejnej moci k osobným údajom uloženým v mobilnom telefóne na účely ich spracúvania v rámci trestného vyšetrovania nie je obmedzený na prípady boja proti závažnej trestnej činnosti.

   Uvedený prístup musí byť v každom prípade odôvodnený a obmedzený na to, čo je striktne nevyhnutné a primerané, v závislosti od povahy vyšetrovaných trestných činov a osobných údajov, ku ktorým sa má získať prístup.

   Policajné orgány nemôžu samy a bez predchádzajúceho povolenia súdu v rámci trestného vyšetrovania získať úplný a nekontrolovaný prístup ku všetkým údajom uloženým v mobilnom telefóne, ak pomocou nich možno vytvoriť presný obraz o osobnom živote určitej osoby.

2. Články 13, 15 a 54 smernice 2016/680 v spojení s článkami 47 a 52 Charty

   sa majú vykladať v tom zmysle, že:

   bez toho, aby boli dotknuté obmedzenia povolené článkom 15 ods. 1 smernice 2016/680 alebo iné dostupné správne alebo mimosúdne prostriedky nápravy, majiteľ mobilného telefónu musí byť informovaný o spracúvaní osobných údajov uložených v tomto telefóne, ktoré vykonali príslušné orgány, v čase a za podmienok, ktoré sú potrebné na zaručenie účinného výkonu jeho práva podať účinný súdny prostriedok nápravy v prípade možného porušenia práv priznaných v smernici 2016/680.