Datum van inontvangstneming	:	04/08/2025

Zaak C-427/25 [Uffida] [i]

Samenvatting van het verzoek om een prejudiciële beslissing overeenkomstig artikel 98, lid 1, van het Reglement voor de procesvoering van het Hof van Justitie

Datum van indiening:

26 juni 2025

Verwijzende rechter:

Tribunale di Catania (Italië)

Datum van de bekendmaking van de verwijzingsbeslissing:

26 juni 2025

Indiener van een aangifte in het kader van een strafzaak tegen onbekende daders:

A.B.

Voorwerp van de procedure in het hoofdgeding

In het kader van een strafzaak betreffende het strafbare feit van het zich uitgeven voor iemand anders in de zin van artikel 494 van de codice penale (wetboek van strafrecht; hierna: „c.p.") die is ingeleid naar aanleiding van de aangifte van A.B., heeft het openbaar ministerie bij Procura della Repubblica di Catania (parket Catania, Italië) de rechter belast met het vooronderzoek verzocht om toestemming voor het verkrijgen van externe telecommunicatiegegevens met het oog op de identificatie van de dader van de feiten.

Voorwerp en rechtsgrondslag van de prejudiciële verwijzing

1 De prejudiciële verwijzing krachtens artikel 267 VWEU betreft uitlegging van artikel 15, lid 1, van richtlijn 2002/58, zoals gewijzigd bij richtlijn 2009/136, gelezen tegen de achtergrond van de artikelen 7, 8, 11 en 52 van het Handvest van de grondrechten van de Europese Unie en in het kader van de nieuwe regeling voor elektronisch bewijsmateriaal (artikelen 3 en 5 van verordening 2023/1543),

[i] Dit is een fictieve naam, die niet overeenkomt met de werkelijke naam van enige partij in de procedure.

teneinde na te gaan of een nationale wettelijke regeling die het verkrijgen van telematicagegevens (begrepen als verkeersgegevens) enkel toestaat voor ernstige strafbare feiten verenigbaar is met het Unierecht.

Prejudiciële vragen

1. Kan artikel 15, lid 1, van richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, zoals gewijzigd bij richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, gelezen tegen de achtergrond van de artikelen 7, 8, 11 en 52 van het Handvest van de grondrechten van de Europese Unie en in het kader van de nieuwe regeling voor elektronisch bewijsmateriaal (artikelen 3 en 5 van verordening 2023/1543), aldus worden uitgelegd dat de toegang van overheidsinstanties tot telematicagegevens die als logbestanden kunnen worden aangemerkt en bestaan in gegevens betreffende het in- en uitloggen (log-in en log-out) door een gebruiker van het systeem of de applicatie met bijbehorende IP-adressen en tijdstempels (dat wil zeggen betrekking hebbende op een bepaalde tijdspanne), waarbij de toegang tot die gegevens uitsluitend bedoeld is om de dader van een strafbaar feit te identificeren – in het kader van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten –, een inmenging inhoudt in de grondrechten van de personen op wie de gegevens betrekking hebben die – anders dan bij verkeers- en geolocatiegegevens – niet dermate ernstig is dat deze toegang tot de bestrijding van zware criminaliteit moet worden beperkt maar zich kan uitstrekken tot alle strafbare feiten?

2. Subsidiair, voor het geval dat het Hof oordeelt dat de toegang tot logbestanden (bestaande in gegevens betreffende het in- en uitloggen door een gebruiker van het systeem of de applicatie met bijbehorende IP-adressen en tijdstempels), hoewel deze enkel bedoeld zijn om de dader van een strafbaar feit te identificeren, kan leiden tot een ernstige inmenging in de in het Handvest neergelegde grondrechten van de personen op wie de gegevens betrekking hebben: kan artikel 15 van richtlijn 2002/58/EG aldus worden uitgelegd dat het vereiste van opsporing en vervolging van door middel van het telematicanetwerk gepleegde strafbare feiten – wanneer de dader alleen kan worden geïdentificeerd door middel van het verkrijgen van telematicagegevens zoals bovengenoemde logbestanden, en rekening houdend met de typische anonimiteit op het netwerk – de toegang tot persoonsgegevens die door dienstaanbieders worden verwerkt (met inbegrip van verkeers- en locatiegegevens) rechtvaardigt, ongeacht de „ernst” van deze strafbare feiten zoals gedefinieerd door de lidstaten, en kan derhalve een nationale wettelijke regeling die daarin voorziet worden beschouwd als passend, evenredig aan het nagestreefde doel en noodzakelijk in een democratische samenleving, mede gelet op de bescherming van het recht van de slachtoffers van die strafbare feiten op bescherming van de privésfeer en op identiteit?

Aangevoerde bepalingen van Unierecht en rechtspraak van de Unie

Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), zoals gewijzigd bij richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, artikel 15

Richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen [en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad], overweging 14

Verordening (EU) 2023/1543 van het Europees Parlement en de Raad van 12 juli 2023 betreffende het Europees verstrekkingsbevel en het Europees bewaringsbevel voor elektronisch bewijsmateriaal in strafzaken en de tenuitvoerlegging van vrijheidsstraffen als gevolg van een strafprocedure; overweging 41, artikelen 3 en 5

Handvest van de grondrechten van de Europese Unie (hierna: „Handvest”); artikelen 7, 8, 11 en 52

De verwijzende rechter onderzoekt een aantal arresten van het Hof van Justitie van de Europese Unie (hierna: „Hof”), die hierna worden genoemd, betreffende het verkrijgen van externe elektronischecommunicatiegegevens, onder meer met het oog op het voorkomen, opsporen en vervolgen van strafbare feiten, in het licht van de grondrechten die zijn neergelegd in de artikelen 7 en 8 van het Handvest (eerbiediging van het privéleven en bescherming van persoonsgegevens), artikel 11 van het Handvest (vrijheid van meningsuiting) en artikel 52, lid 1, van het Handvest (beperkingen op de uitoefening van die rechten).

Arresten van het Hof (Grote kamer)

– van 21 december 2016, Tele2 Sverige en Watson e.a., gevoegde zaken C-203/15 en C-698/15, ECLI:EU:C:2016:970 (dictum);

– 2 oktober 2018, Ministerio Fiscal, C-207/16, ECLI:EU:C:2018:788, (dictum);

– 2 maart 2021, Prokuratuur (Voorwaarden voor toegang tot elektronische-communicatiegegevens), C-746/18, ECLI:EU:C:2021:152, (punt 35);

– 30 april 2024, Procura della Repubblica presso il Tribunale di Bolzano, C-178/22, EU:C:2024:371, (punten 45-48);

– 30 april 2024, La Quadrature du Net e.a. (Persoonsgegevens en bestrijding van namaak), C-470/21, ECLI:EU:C:2024:370, (punten 65, 116, 117 e 154).

Aangevoerde bepalingen van nationaal recht

Codice penale (wetboek van strafrecht; hierna: „c.p.”); artikel 494, met het opschrift „Zich uitgeven voor iemand anders” luidt als volgt: „Eenieder die, om voor zichzelf of voor anderen een voordeel te verkrijgen of anderen schade te berokkenen, iemand misleidt door zich op onrechtmatige wijze uit te geven voor een ander, of door aan zichzelf of aan anderen een valse naam of een valse status toe te kennen, of een hoedanigheid waaraan de wet rechtsgevolgen toekent, wordt, indien het feit geen ander strafbaar feit tegen de openbare trouw vormt, gestraft met een gevangenisstraf van ten hoogste één jaar.”

Decreto legislativo 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali, come modificato dal decreto-legge 30 settembre 2021 n. 132, convertito dalla legge 23 novembre 2021, n. 17 (wetsbesluit nr. 196 van 30 juni 2003 betreffende de bescherming van persoonsgegevens, zoals gewijzigd bij voorlopig wetsbesluit nr. 132 van 30 september 2021, omgezet in wet nr. 17 van 23 november 2021; hierna: „d.lgs. 196/2003”), met het oog op het in overeenstemming brengen van het nationale rechtskader met de beginselen die het Hof in zijn arrest van 2 maart 2021, zaak C-746/2018, heeft uiteengezet.

– Artikel 121, onder h), van d.lgs. 196/2003 definieert „verkeersgegevens” als „gegevens die worden verwerkt met het oog op het overbrengen van communicatie via een elektronisch communicatienetwerk of de facturering ervan”.

– Artikel 132, lid 3, staat toegang tot verkeersgegevens toe in het kader van strafrechtelijke onderzoeken door middel van een toestemmingbesluit van de rechter belast met het vooronderzoek voor twee soorten strafbare feiten: a) ernstige strafbare feiten (waarvoor levenslange gevangenisstraf of een gevangenisstraf van ten minste drie jaar kan worden opgelegd); b) strafbare feiten in verband met het telefonisch bedreigen, intimideren of storen van personen, mits de bedreiging, intimidatie en verstoring in de praktijk als ernstig worden beschouwd.

Korte uiteenzetting van de feiten en de procedure

2 A.B., 19 jaar oud, heeft aangifte gedaan van het feit dat hij ongeveer een maand ervoor had opgemerkt dat online een Facebook-profiel aanwezig was met als profielfoto een persoonlijke foto van hem, met vermelding van zijn voornaam en de achternaam bij hij bij zijn geboorte had gekregen, terwijl hij deze achternaam al enkele jaren niet meer gebruikte ten gunste van die van zijn adoptieouders. Dit sociale profiel was meer dan een maand na de eerste ontdekking nog steeds actief met valse en misleidende gegevens die tot hem herleidbaar waren en waarvoor hij geen toestemming had gegeven. Het profiel bevatte nog meer verwijzingen naar zijn oorspronkelijke familie.

3 Op basis van de aangifte en het rapport van de postpolitie heeft het openbaar ministerie de rechter belast met het vooronderzoek van de Tribunale di Catania (rechter in eerste aanleg Catania), de verwijzende rechter, verzocht om toestemming voor het verkrijgen van de logbestanden van het account dat ogenschijnlijk nep is, met inbegrip van het IP-adres, de datum en de toegangstijden in de periode tussen 24 november 2024 en de datum van kennisgeving van het rechterlijk toestemmingsbesluit.

4 De rechter, die het eens was met de opmerking van het openbaar ministerie dat de gevraagde telematicagegevens het enige onderzoeksmiddel waren aan de hand waarvan de dader van de feiten kon worden geïdentificeerd, heeft het verzoek afgewezen op grond dat, ten eerste, het voor het strafbare feit bedoeld in artikel 494 c.p. niet is toegestaan om telematicagegevens (opgevat als verkeersgegevens) in de zin van artikel 132 van d.lgs. 196/2003 te verkrijgen, aangezien dit strafbare feit wordt bestraft met een gevangenisstraf van ten hoogste één jaar, en daarmee onder de minimumdrempel die de regeling inzake verkeersgegevens vereist, en, ten tweede, dat de feiten niet konden worden gekwalificeerd als een van de andere soorten strafbare feiten waarvoor telematicaverkeersgegevens kunnen worden verkregen.

5 Naar aanleiding van deze beslissing heeft het openbaar ministerie de rechter verzocht de zaak te seponeren, omdat het van mening was dat het onderzoek niet kon worden voortgezet zonder de gevraagde logbestanden te verkrijgen. De rechter heeft de terechtzitting echter vastgesteld, aangezien hij van oordeel was dat hij geen gevolg moest geven aan het verzoek om de zaak te seponeren en hij de behandeling van de zaak op tegenspraak tussen partijen moest openen. Volgens deze rechter moet immers eerst worden nagegaan of het Unierecht zich in het licht van de relevante rechtspraak van het Hof verzet tegen de uitsluiting van logbestanden van de categorie „telematicaverkeersgegevens” en, hoe dan ook, of het zich verzet tegen de mogelijkheid om toestemming te verlenen voor de toegang tot deze telematicagegevens (de hier gevraagde logbestanden), wanneer zij onontbeerlijk zijn voor de identificatie van de dader van een strafbaar feit, ook buiten vormen van zware criminaliteit. Na partijen te hebben gehoord, heeft de rechter besloten om het Hof een verzoek om een prejudiciële beslissing voor te leggen over uitlegging van artikel 15 van richtlijn 2002/58.

Korte uiteenzetting van de motivering van de prejudiciële verwijzing

6 De onderhavige prejudiciële verwijzing vloeit voort uit de noodzaak om, gelet op de ontwikkeling van het Unierecht zoals uitgelegd door het Hof, ook in het licht van de exponentiële toename van cybercriminaliteit en de daarmee samenhangende technologische ontwikkeling, na te gaan of de in casu en in andere soortgelijke zaken gevraagde logbestanden, wanneer zij onontbeerlijk zijn om de dader van de veronderstelde strafbare gedragingen te identificeren, niet als „verkeersgegevens” kunnen worden aangemerkt en daarom op verschillende manieren kunnen worden verkregen, of, subsidiair, hoe dan ook kunnen worden

verkregen los van de kwalificatie als „zware criminaliteit” van de strafbare feiten waarop zij betrekking hebben, wanneer ervan wordt uitgegaan dat het om verkeersgegevens gaat.

7 De Italiaanse wetgeving bevat geen specifieke en uitdrukkelijke verwijzing naar de soorten telematicaverkeersgegevens en noemt logbestanden niet uitdrukkelijk als telematicaverkeersgegevens. De enige nuttige verwijzingen zijn de artikelen 121 en 132 van d.lgs. nr. 196/2003 die zonder nadere precisering verwijzen naar de enige categorie, namelijk „telematicaverkeersgegevens”.

8 De Suprema Corte di Cassazione (hoogste rechter in burgerlijke en strafzaken in Italië) heeft evenmin de gelegenheid gehad om de aard van logbestanden te onderzoeken. Deze rechter heeft echter verklaard dat onder logbestanden bestanden in tekstformaat worden verstaan, waarin de handelingen worden vermeld die een gebruiker tijdens een werksessie op zijn elektronische apparaat verricht. Volgens de rechtsleer gaat het om echte „vingerafdrukken 2.0” die bijzonder belangrijk zijn in het kader van het onderzoek, aangezien deze het mogelijk maken om verschillende gebruiksprofielen van het apparaat te identificeren, waaronder: a) de tijdstippen en de duur van de internetaansluiting met haar IP-adres (unieke identificatiecode van een apparaat op het internet of in een lokaal netwerk); b) de informatie die het apparaat via hetzelfde adres heeft verzonden of ontvangen; c) de persoonsgegevens van de houder van een gebruikscontract.

9 Volgens een deel van de rechtsleer zijn de logbestanden slechts de gegevens over de verbinding die aan een IP-adres van bestemming wordt toegewezen, waarmee websites die door de gebruiker zijn bezocht kunnen worden geïdentificeerd en die zijn losgekoppeld van enige telematicacommunicatie tussen twee of meer op het netwerk aangesloten apparaten. Deze vallen niet binnen de werkingssfeer van artikel 132 van d.lgs. [196/2003]. Volgens een ander deel van de rechtsleer stemmen de begrippen logbestanden en telematicaverkeersgegevens als bedoeld in artikel 132 van d.lgs. 196/2003 volledig met elkaar overeen; sterker nog, alleen de logbestanden bevatten telematicaverkeersgegevens, met vermelding van de toegang tot het netwerk dat heeft plaatsgevonden, de websites die zijn bezocht, de duur van de verbinding, alle gegevens, dat wil zeggen informatie over de persoonlijke levenssfeer en de keuzen van de gebruikers van het netwerk.

10 In de praktijk van strafrechtelijke onderzoeken is het gangbaar om logbestanden, ook al zijn zij enkel bedoeld om de dader te identificeren, als „telematicaverkeersgegevens” te beschouwen en vallen deze uit dien hoofde onder de voorwaarden van artikel 132 van d.lgs. 196/2003, met de beperkingen die daaruit voortvloeien voor de vaststelling van bepaalde strafbare feiten. De onduidelijke en vage inhoud van deze regels kan leiden tot uiteenlopende rechterlijke beslissingen, en soms kan de onmogelijkheid om toegang te verkrijgen tot deze bestanden ertoe leiden dat bepaalde strafbare feiten niet worden vervolgd.

11 Het Hof heeft in zijn arrest van 2 oktober 2018, Ministerio Fiscal, C-207/16, de mogelijkheid gehad om te verklaren dat hoe ernstiger de inmenging in het privéleven en de vertrouwelijkheid van elektronische communicatie is, des te meer de mogelijkheid om aan aanbieders te verzoeken om gegevens te verkrijgen met het oog op het strafrechtelijk onderzoek moet worden beperkt tot zware vormen van criminaliteit. Zo kunnen de autoriteiten toegang krijgen als er sprake is van veel minder ernstige inmengingen zoals het verkrijgen van gegevens betreffende de burgerlijke identiteit van een gebruiker (identificatiegegevens van de houder van een simkaart die met een gestolen mobiele telefoon is geactiveerd, zoals de achternaam, de voornaam en het adres, die aan de orde waren in zaak C-207/16, Ministerio Fiscal), met het oog op het vaststellen van om het even welk strafbaar feit, en niet alleen van ernstige feiten.

12 Logbestanden zoals die waarom in deze zaak wordt verzocht, zijn in eerdere arresten van het Hof niet uitdrukkelijk in aanmerking genomen. Hoewel deze geen „statische" informatieverzameling vormen, zoals de persoonsgegevens in de zaak Ministerio Fiscal, C-207/16 (voornaam, achternaam, adres van de houder van een simkaart of een account) en het IP-adres in de zaak Quadrature du Net 2, C-470/21, die veeleer een reeks van tijdgegevens (gegevens betreffende het in- en uitloggen in een bepaalde tijdspanne) vormen, lijken deze echter niet het typische kenmerk van verkeersgegevens in de zin van het Unierecht te bezitten, namelijk dat daaruit precieze conclusies kunnen worden getrokken over het privéleven en de levenskeuzen van de persoon van wie de gegevens zijn bewaard, zoals zijn dagelijkse gewoonten, verblijfsplaatsen, dagelijkse of andere verplaatsingen, ontplooide activiteiten, zijn sociale relaties en de sociale kringen waarin hij verkeert.

13 Uit een toelichting van de postpolitie blijkt dat deze gegevens een veel beperktere informatieve waarde hebben vanuit het oogpunt van de inmenging in het privéleven van de gebruikers van het netwerk. In deze nota wordt met name gepreciseerd dat bij telematicacommunicatie het logbestand een gedetailleerd register is waarin de volgende mogelijke gebeurtenissen kunnen worden vermeld:

a) het in- en uitloggen van een gebruiker van het systeem of de applicatie met de betreffende IP-adressen en tijdstempels; b) door de gebruiker verrichte handelingen, zoals het verzenden van berichten, het vragen van een dienst of raadplegen van een bron, enz.); c) fouten of storingen in het systeem. De logbestanden waarom specifiek in de onderzoeken wordt gevraagd bevatten slechts: I) IP-adressen voor het aanmaken van het sociale profiel van een persoon, niet altijd gekoppeld aan de datum en het tijdstip (tijdstempel), in voorkomend geval met een gecontroleerd telefoonnummer en/of e-mailadres; II) IP-adressen – met datum en tijdstip – van de toegang tot het profiel gedurende de gevraagde periode (vanaf een bepaalde datum en tijdstip tot een andere datum en tijdstip) en gedurende een maximaal, hoe dan ook beperkt, tijdsbestek.

14 Daarom kan worden geconcludeerd dat de gevraagde bestanden naar hun aard uitsluitend tot doel hebben de pleger te identificeren van een gedraging (die op het

netwerk heeft plaatsgevonden en ten aanzien waarvan een onderzoek wordt ingesteld) en daarentegen geen uitgebreidere en verdergaande informatie kunnen verschaffen over de persoonlijke levenssfeer van de personen van wie de gegevens zijn bewaard.

15 Dit gezegd zijnde, kan uit de tekst van verordening (EU) 2023/1543 een uitlegging worden afgeleid die logbestanden uitsluit van de categorie verkeersgegevens in eigenlijke zin van artikel 15 van richtlijn 2002/58. Deze verordening, die vanaf 26 augustus 2026 in werking zal treden (zie artikel 34), voorziet in vormen van rechtstreekse en flexibelere samenwerking tussen justitiële of onderzoeksautoriteiten die bevoegd zijn bewijsmateriaal te verzamelen in de respectieve nationale systemen van de EU-landen en „aanbieders van elektronischecommunicatiediensten” met het oog op het verstrekken en voorlopig bewaren van elektronisch bewijsmateriaal. Daartoe worden „certificaten” (certificaat inzake het Europees verstrekkingsbevel, CEV, en certificaat inzake het Europees bewaringsbevel, CEB) in het leven geroepen waarin de inhoud van relevante rechterlijke beslissingen, de verplichtingen tot antwoorden van aanbieders, de gecodificeerde gronden voor een eventuele weigering, bepaalde termijnen, en de onderling verbonden, beveiligde en omschreven communicatieplatforms worden vastgelegd.

16 Hoewel dit rechtskader geen betrekking heeft op alle gevallen van het verkrijgen van externe communicatiegegevens, maar alleen op gevallen die worden verstrekt door aanbieders van bepaalde diensten en die gevestigd zijn in een andere lidstaat dan de rechterlijke autoriteit die deze gegevens wil verkrijgen, en dus in het kader van rechtstreekse justitiële samenwerking met dienstaanbieders en de rechterlijke autoriteiten van de lidstaten van vestiging, maakt dit al deel uit van het Unierecht en is het nuttig als basis voor de hernieuwde uitlegging van dit onderwerp, met name omdat dit is vastgesteld op basis van een bewuste gelijkstelling met de rechtspraak van het Hof over verkeers- en geolocatiegegevens.

17 Artikel 3 van deze verordening („Definities”) maakt duidelijk onderscheid tussen „gegevens die uitsluitend worden opgevraagd met het oog op de identificatie van de gebruiker” (IP-adressen en, indien nodig, de relevante bronpoorten en tijdstempel, met name de datum en het tijdstip, of de technische equivalenten van die identificatoren alsook daarmee verband houdende informatie, wanneer rechtshandhavingsinstanties of rechterlijke autoriteiten hierom verzoeken met als enig doel de gebruiker te identificeren in het kader van een specifiek strafrechtelijk onderzoek (artikel 3, onder 10)), en „verkeersgegevens” (gegevens in verband met de verlening van een door een dienstaanbieder aangeboden dienst, die dienen om achtergrondinformatie of aanvullende informatie over die dienst te verstrekken en door een informatiesysteem van de dienstaanbieder zijn gegenereerd of verwerkt, zoals de herkomst en de bestemming van een bericht of een ander type interactie, de locatie van het apparaat, de datum, het tijdstip, de duur, de omvang, de route, de vorm, het gebruikte protocol en het type compressie, en andere elektronischecommunicatiemetagegevens, en gegevens, andere dan abonneegegevens, betreffende de aanvang en beëindiging van een

toegangssessie van een gebruiker tot een dienst, zoals de datum en het tijdstip van het gebruik, het inloggen in en het uitloggen uit de dienst) (artikel 3, onder 11)).

18 Artikel 5 van deze verordening dat overeenkomstig artikel 3 de voorwaarden voor de uitgifte van het Europese verstrekkingsbevel vaststelt, omschrijft het soort strafbare feiten waarvoor de gegevens kunnen worden opgevraagd en verkregen. Voor abonneegegevens en gegevens die uitsluitend worden opgevraagd met het oog op de identificatie van de gebruiker (die als minder gevoelige gegevens worden beschouwd), met inbegrip van de in artikel 3, onder 10), bedoelde gegevens, mag voor alle strafbare feiten een verstrekkingsbevel worden uitgevaardigd; voor verkeersgegevens, met uitzondering van gegevens die uitsluitend worden opgevraagd met het oog op de identificatie van de gebruiker op grond van deze verordening, en inhoudelijke gegevens geldt de beperking tot ernstige strafbare feiten.

19 De in artikel 3, onder 10), van de verordening opgesomde gegevens lijken echter overeen te stemmen met de telematicagegevens van het type logbestanden waarom in de onderhavige procedure wordt verzocht (gegevens betreffende het in- en uitloggen van een gebruiker van het systeem of de applicatie met de bijbehorende IP-adressen en tijdstempels, dat wil zeggen in een bepaalde tijdspanne), waarnaar ook wordt verwezen in de overwegingen 32, 33 en 34 van deze verordening.

20 Bijgevolg kan men tot de conclusie komen dat in de onderhavige zaak de toegang tot deze logbestanden, die geen betrekking hebben op „telematicaverkeersgegevens”, kan vallen onder andere bepalingen van de codice di procedura penale (wetboek van strafvordering; hierna: „c.p.p.”), zoals met name artikel 234-bis c.p.p. (in het geval van gegevens die zijn verkregen door in het buitenland gevestigde aanbieders) en artikel 256 c.p.p. (in het geval van gegevens die door een Italiaanse aanbieder als exploitant van de openbare dienst moeten worden verkregen), en niet onder artikel 132 van d.lgs. 196/2003 (met de beperking van de aard van de strafbare feiten waarvoor vervolging wordt ingesteld en het toestemmingsbesluit van de rechter), op grond waarvan het openbaar ministerie deze gegevens kan verkrijgen zonder rechterlijke toestemming.

21 Subsidiair, voor het geval dat zou worden geconcludeerd dat de logbestanden tot de „verkeersgegevens” behoren omdat deze het mogelijk maken precieze en gevoelige informatie te verkrijgen over het privéleven van de betrokkenen wier gegevens zijn bewaard, is de onderhavige prejudiciële verwijzing noodzakelijk.

22 Het verbod op toegang tot elektronischecommunicatiegegevens in geval van ogenschijnlijk niet-ernstige gedragingen – zoals diefstal van digitale identiteit, poging tot huiselijk geweld en bedreiging tussen twee personen – kan nog onredelijker zijn als men bedenkt dat gedragingen die plaatsvinden langs digitale en telematische weg, bijvoorbeeld tussen gebruikers van applicaties en/of platforms, over het algemeen zichtbaar zijn voor een breed publiek van gebruikers en bijgevolg het slachtoffer blootstellen aan een verdergaande imagoschade

waarop het slachtoffer geen invloed kan uitoefenen, behalve door een strafprocedure in te leiden.

23 Verordening nr. 1543/2023 kan in dit verband nog andere nuttige verwijzingen bevatten. In overweging 41 wordt gepreciseerd dat „in de meeste gevallen waarin het strafbaar feit door middel van een informatiesysteem wordt gepleegd, [...] de toepassing van dezelfde drempel als voor andere soorten strafbare feiten, in hoge mate tot straffeloosheid [zou] leiden. Dit rechtvaardigt dat deze verordening ook wordt toegepast op dergelijke strafbare feiten waarvoor een maximale vrijheidsstraf van minder dan drie jaar geldt."

24 Wat betreft het belang van diefstal van digitale identiteit die volgens het nationale recht deel uitmaakt van het in artikel 494 c.p. bedoelde strafbare feit van het zich uitgeven voor iemand anders waarop de onderhavige procedure betrekking heeft, kan de toenemende aandacht ervoor in het Unierecht worden afgeleid uit richtlijn 2013/40 die in overweging 14 benadrukt dat „het nemen van doeltreffende maatregelen tegen identiteitsdiefstal en andere identiteitsgerelateerde strafbare feiten [...] een ander belangrijk onderdeel [is] van een geïntegreerde aanpak van cybercriminaliteit".

25 Tot slot biedt de Franse wetgeving een nuttig criterium ter vergelijking met een strafbaar feit dat volledig vergelijkbaar is met het Italiaanse strafbare feit van het zich uitgeven voor iemand anders in de digitale sfeer en met betrekking tot de daarmee samenhangende regeling voor het verkrijgen van telematicaverkeersgegevens.

26 Het in artikel 226-4-1 van het Franse wetboek van strafrecht bedoelde strafbare feit van identiteitsmisbruik (usurpation d'identité) stelt het misbruik van identiteit van een derde of het gebruik van een of meer gegevens van welke aard ook waarmee hij kan worden geïdentificeerd teneinde zijn rust of die van een ander te verstoren of zijn eer of goede naam aan te tasten, strafbaar met een gevangenisstraf van ten hoogste één jaar gevangenisstraf en een geldboete van 15.000 EUR. Het strafbare feit wordt bestraft met dezelfde straffen wanneer het wordt gepleegd via een openbaar online communicatienetwerk.

27 Wat betreft het verkrijgen van verkeers- en locatiegegevens in een procedure worden in artikel 60-1-2 van het Franse wetboek van strafvordering, dat is ingevoerd bij de wet van 2 maart 2022, twee voorwaarden gesteld: 1) de eerste is dat de vereisten van de procedure dit vorderen; 2) de tweede betreft de straf: het moet gaan om misdrijven of delicten (crimes o délits) die strafbaar zijn gesteld met een maximumstraf van ten minste drie jaar gevangenisstraf) of, om te voldoen aan het vereiste om strafbare feiten van cybercriminaliteit met een wezenlijke omvang er niet buiten te laten vallen, strafbare feiten waarop een maximumstraf van ten minste één jaar gevangenisstraf staat, indien zij worden gepleegd met behulp van een elektronisch communicatienetwerk en het verkrijgen van verkeersgegevens uitsluitend plaatsvindt met het oog op de identificatie van de

dader van het strafbare feit. Dit maakt het bijvoorbeeld mogelijk om strafbare feiten zoals identiteitsmisbruik of diefstal van een digitale identiteit op te nemen.

28 De verwijzende rechter verzoekt het Hof de zaak te behandelen volgens de versnelde procedure (artikel 105 van het Reglement voor de procesvoering van het Hof). Ten eerste mogen deze gegevens door de aanbieders van digitale diensten namelijk slechts voor een beperkte periode worden bewaard, zodat het verstrijken van de tijd de mogelijkheid om deze gegevens te verkrijgen definitief teniet kan doen; ten tweede werpt de zaak uitleggingsvragen op die zowel in de Italiaanse rechtsorde als in de rechtsorden van de andere lidstaten onmiddellijke gevolgen kunnen hebben voor strafprocedures die in de fase van het vooronderzoek aanhangig zijn en vergelijkbaar zijn met deze zaak.