ISSN 2432-6089

法と情報雑誌

The Law and Information Magazine

第 7 巻第 1 号（通巻第 47 号・2022 年 1 月）

法と情報研究会　編

（第 3 分冊）

本 号 目 次

Privacy International 判決 C-623/17 先決裁定事件 ECLI:EU:C:2020:790

[参考訳]

2022 年 1 月 8 日

明治大学法学部教授

丸　橋　　透

＊＊＊

REQUEST for a preliminary ruling under Article 267 TFEU from the Investigatory Powers Tribunal (United Kingdom), made by decision of 18 October 2017, received at the Court on 31 October 2017, in the proceedings **Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service**

欧州連合司法裁判所(CJEU) 2020 年 10 月 6 日付大法廷判決 C-623/17 先決裁定事件 ECLI:EU:C:2020:790 に基づき、和訳を試みた。英語版テキスト(正文)は、EUR-Lex Web サイトから入手した。

https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62017CJ0623
[2022 年 1 月 8 日確認]

本判決に先立つ 2020 年 1 月 15 日付独立弁論官(Advocate General) Campos Sánchez-Bordona 意見(書) ECLI:EU:C:2020:5 英語版テキスト(正文はスペイン語)は同じく EUR-Lex から入手できる。

https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62017CC0623
[2022 年 1 月 8 日確認]

―解　説―

1.　基本権憲章と e-Privacy 指令 2002/58/EC

本判決は、欧州連合基本権憲章第 7 条、第 8 条、第 11 条及び第 52 条(1)並びに欧州連合条約(TEU)第 4 条(2)に照らしたいわゆる e-privacy 指令 2002/58/EC の解釈を判示している。

欧州連合基本権憲章は、EUR-Lex からテキストを入手できる。

https://eur-lex.europa.eu/eli/treaty/char_2012/oj
[2022 年 1 月 8 日確認]

基本権憲章の解説その他の関連情報は、European Union Fundamental Rights Agency (欧州連合基本権庁)のサイトに集約されている。

https://fra.europa.eu/en/eu-charter
[2022 年 1 月 8 日確認]

指令 2002/58/EC は EUR-Lex から入手できる。

https://eur-lex.europa.eu/eli/dir/2002/58/oj
[2022 年 1 月 8 日確認]

指令 2002/58/EC は改正されており、現在有効な改正後の指令は EUR-Lex から入手できる。

https://eur-lex.europa.eu/eli/dir/2002/58/2009-12-19
[2022 年 1 月 8 日確認]

2. 参考訳作成における基本方針

この参考訳においては，C-623/17 事件の先決裁定判決全文を訳出した。

この参考訳は，あくまでも C-623/17 事件の先決裁定判決の私的な和訳である。公式訳でも確定訳でもない。

この参考訳は，現時点における研究成果を反映するものである。将来，更に研究を深めた結果として修正すべき部分を発見したときは，その時点において，改訂版等を作成すべきかどうかを検討する。

訳出に際しては原則として直訳とすることとしたが，直訳のままでは日本語になりにくい箇所に関しては，やむを得ず意訳とした。

この参考訳に若干の訳注を付した。判決文には原注はない。

読みやすさを重視し，引用条文中の項(paragraph)は判決文の表記通り(1)(2)・・・としている。同様に EU の法令の略も判決文中の略式表記通り(たとえば「指令 2002/58」)としている。

連合王国法での項(subsection)号(paragraph)の表記は、条文が省略していなければ、そのまま「subsection(1)」は「第(1)項」、「paragraph(1)」は「第(1)号」としている。

この参考訳は，EUR-Lex のデータ二次利用条件を遵守して作成した。

3. 訳語に関する補足的説明

連合王国の「Investigatory Powers Tribunal」は、捜査権限審判所又は調査権限行政審判所などと訳されることがある。TFEU(欧州連合機能(を機能させる)条約)第 267 条(2)により先決裁定を請求できる資格がある法廷かどうかについては争われた様子がない。実際、判決文中でも照

会元裁判所(referring court)として扱われている。同条の請求資格に関する解釈については、CJEU の各国裁判所/法廷向けの先決裁定手続開始に関する勧告(Recommendations to national courts and tribunals in relation to the initiation of preliminary ruling proceedings(2019/C 380/01))が、CJEU の先例をまとめており、法定された組織であること、恒久的であること、その管轄が強制的であること、手続が対審構造であること、法の支配を適用すること、独立していること等の要素により判断するとしている(第 4 項)。そのため、少なくとも EU 法の側面では、それらの要件のいくつかを満たした法廷として考えることができる。又、「investigatory powers」には、具体的な捜査とは言えない諜報目的の活動権限が含まれるのが明らかであるので、「調査権限」と訳す方が適切と考える。この参考訳では、「Investigatory Powers Tribunal」を「調査権限法廷」と訳した。

「main proceeding」は「主手続」と直訳した。上述の TFEU 第 267 条(2)の解釈のとおり、照会元の courts and tribunals の「proceeding」は実際には「裁判手続」そのもの、又は極めてそれに近い性質のものしかあり得ないが、法定の専属的仲裁手続も含まれるとした判例(CJEU 2014 年 2 月 13 日付決定 C-555/13 事件第 15 項から第 25 項)もあるので、「手続」としている。

「national security」は「国家安全保障」よりも簡潔に「国家保安」と訳した。「safeguarding ～」「protecting～」と続ける場合は、重畳感があるが、一律「国家保安」「の防護/を防護する」としてある。実際、強調するために使用していると思われる使用例もあるからである。「public security」も同様である。なお「State security」は「(EU)構成国の（自国の/国内の）保安」の意味であるので、「構成国の保安」と訳している。

「bulk communication data」単に大量というよりも対象のほとんど全量、大半というニュアンスを表す適切な日本語に思い当たらなかったため、「バルク通信データ」とした。

「general and indiscriminate～」転送(transmission)又は方法（way）として表現されているメタデータのバルク移転又は保持の形容については、「網羅的かつ無差別の」と意訳した。「general」の直訳は「一般的」であるが、意味するところは「網羅的一般的」であると解した。「indiscriminate」が意味するところは、後掲 *tele2* 事件での「標的を絞った」(targeted)に対する「標的を絞っていない」(non-targeted)保持態様であるからである。もちろん「網羅的一般的かつ無差別の」でも良いと思われる。

4. 関連参考訳及び参考文献

本判決は、2020 年 10 月 6 日付 La Quadrature du Net and Others 判決 C- 511/18、C- 512/18 及び C- 520/18 併合事件 ECLI:EU:C:2020:791（本号所収）と同日になされ、相互に関係が深いが、引用は、本判決からの一方向になっている。ECLI としては、本判決の番号が一つ若いが、判決の順序としては逆の扱いとなっている。

本判決を受け連合王国調査権限法廷は、1984 年通信法第 94 条の無効を宣言した([2021]UKIPTrib IPT/15/110/CH)。以下のサイトから入手できる。

https://www.ipt-uk.com/judgments.asp?id=60
[2022 年 1 月 8 日確認]

夏井高人明治大学教授による法と情報雑誌所収の本判決に関連する EU の法令及びサイバー犯罪条約の説明書の翻訳は以下のとおりである。*を付したものはウェブ版として公開され、**を付したものは法と情報雑誌が公開されており、http://cyberlaw.la.coocan.jp/index2.html からダウンロードできる。

欧州連合基本権憲章(2012/C 326/02) [参考訳]	第 1 巻第 2 号 1～33 頁
個人データ保護指令 95/46/EC [参考訳・改訂版]	第 2 巻第 5 号 332～365 頁
指令 97/66/EC [参考訳・改訂版]	第 3 巻第 7 号 109～123 頁*
電子商取引指令 2000/31/EC [参考訳]	第 3 巻第 1 号 110～141 頁*
指令 2002/21/EC(枠組み指令) [参考訳]	第 3 巻第 7 号 76～108 頁
指令 2002/58/EC(プライバシー及び電子通信指令)[参考訳] 指令 2006/24/EC 及び指令 2009/136/EC による改正後の条文 [参考訳]	第 1 巻第 2 号 117～150 頁 第 1 巻第 2 号 151～162 頁
指令 2006/24/EC[参考訳]	第 1 巻第 5 号 47～65 頁
指令 2002/58/EC の改正案[参考訳]　（丸橋との共訳）	第 2 巻 4 号 195～248 頁
規則(EU) 2016/679(一般データ保護規則)[参考訳・再訂版]	第 3 巻第 5 号 1～114 頁*
指令(EU) 2016/680 [参考訳・改訂版]	第 6 巻 6 号 339～466 頁**
サイバー犯罪条約（ETS No.185）の説明書 [参考訳]	第 1 巻第 6 号 1～132 頁*

判決中引用されている法令の訳は原則として上記参考訳をそのまま引用した。著者が変更、追加した箇所は、そのための誤訳、誤記はすべて著者の責任である。

引用されている CJEU 判例（間接的に引用されているものも含む）のうち、法と情報雑誌所収の著者による参考訳は以下にある。

2015 年 10 月 6 日付 *Schrems* 判決 C-362/14 事件 ECLI:EU:C:2015:650	第 3 巻 7 号 358～397 頁
2016 年 9 月 8 日付意見 1/15 (*EU-カナダ PNR 協定*)独立弁論官	第 2 巻第 5 号 366～437

意見 ECLI:EU:C:2016:656	頁
2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 ECLI:EU:C: 2016:970	第 2 巻第 1 号 1〜40 頁
2017 年 7 月 26 日付意見 1/15(*EU-カナダ PNR 協定*) ECLI:EU:C:2017:592	第 2 巻第 8 号 186〜256 頁
2020 年 10 月 6 日付 *La Quadrature du Net and Others* 判決 C- 511/18 、 C- 512/18 及び C- 520/18 併合事件 ECLI:EU:C:2020:791	第 7 巻 1 号 444〜525 頁

上記判例の分析を含む著者のこれまでの見解は、以下の論文に記した。

丸橋透「加欧 PNR 協定案 CJEU 大法廷意見 1/15 の分析：マス・サーヴェイランス及びデータ保持法制との距離を踏まえて」 (2019-03) 17 情報ネットワーク・ローレビュー

丸橋透「欧州連合の通信メタデータ保持法制の検討 (村山眞維教授古稀記念論文集)" (2018)」91 法律論叢 279 <https://ci.nii.ac.jp/naid/120006552119/>

RIPA(Regulation of Investigatory Powers Act 2000)については、横山潔「イギリス「調査権限規制法」の成立; 情報機関等による通信傍受・通信データの取得等の規制」外国の立法. 2002. No. 214p. 47 が参考になる。RIPA を改正した DRIPA(Data Retention and Investigatory Powers Act 2014)については、今岡 直子「イギリスにおけるデータ保全及び調査権限法の制定 : EU データ保全指令の無効裁定を踏まえて」外国の立法 : 立法情報・翻訳・解説 2015-06. No. 264p. 3-12 が参考になる。

RIPA は、IPA2016 により改正済である。改正後のバルク通信データ移転法制は、Privacy International 判決とともに GDPR に基づく連合王国による個人データの十分な保護に関する委員会実装決定 (EU) 2021/1772(ELI: http://data.europa.eu/eli/dec_impl/2021/1772/oj)にも言及されているが、そもそも連合王国内の通信事業者が加入者から直接取得する個人データについての規律なので EU 市民が直接加入者となる場合も含め、EU 域内からの個人データの移転に関する十分性認定審査対象外であると断った上で、念のため調査したという位置づけである。

その他本判決と *La Quadrature du Net and Others* 判決の判例批評その他論評が含まれる以下の文献を参照した。

Cameron I, "Court of Justice Metadata Retention and National Security: Privacy International and La Quadrature Du Net" (2021) 58 Common Market Law Review 1433

Juszczak A and Sason E, “Recalibrating Data Retention in the EU” (2021) eucrim <https://doi.org/10.30709/eucrim-2021-020>

Maxwell J and Tomlinson J, “Privacy Int’l V. Secretary of State for Foreign & Commonwealth Affairs and La Quadrature Du Net V. Premier Ministre (C.J.E.U.)” (2021-04) 60 International Legal Materials 464

Rojszczak M, “The Uncertain Future of Data Retention Laws in the EU: Is a Legislative Reset Possible?” (2021-07) 41 Computer Law & Security Review 105572

Tracol X, “The Two Judgments of the European Court of Justice in the Four Cases of Privacy International, La Quadrature Du Net and Others, French Data Network and Others and Ordre Des Barreaux Francophones Et Germanophone and Others: The Grand Chamber Is Trying Hard to Square the Circle of Data Retention” (2021-07) 41 Computer Law & Security Review 105540

Kuner C, Bygrave L and Docksey C, “The EU General Data Protection Regulation (GDPR): A Commentary - 2021 Update” (Oxford University Press, 2021)

Korff D and Brown I, “Exchanges of Personal Data After the Schrems II Judgment” IPOL_STU(2021)694678

Rojszczak M, “National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts” [2021-11] European Constitutional Law Review 1

この参考訳には夏井高人教授の重要な助言が反映されている。

＊＊＊

2020 年 10 月 6 日付欧州連合司法裁判所(大法廷)判決[1]

(先決裁定の照会 — 電子通信分野における個人データの処理 — 電子通信サービスのプロバイダ — トラフィックデータ及び位置情報データの網羅的かつ無差別の保持 — 国家保安の防護— 指令 2002/58/EC — 適用範囲 — 第 1 条(3)及び第 3 条 — 電子通信の機密性 — 保護 — 第 5 条及び第 15 条(1) — 欧州連合基本権憲章 — 第 7 条、第 8 条、第 11 条及び第 52 条(1) — TEU[2]第 4 条(2))

C-623/17 事件において、

2017 年 10 月 18 日付決定により調査権限法廷(連合王国)から出され、2017 年 10 月 31 日に当裁判所において受領した、以下の手続に関する TFEU[3]第 267 条に基づく先決裁定請求において、

Privacy International

対

外務・コモンウェルス大臣、内務大臣、政府通信本部、保安局、秘密諜報部

当裁判所(大法廷)は、

裁判所長官である K. Lenaerts、裁判所副長官である R. Silva de Lapuerta、小法廷裁判長である J.-C. Bonichot、 A. Arabadjiev、A. Prechal、M. Safjan、P.G. Xuereb 及び L.S. Rossi、裁判官である J. Malenovský、L. Bay Larsen、T. von Danwitz (進行・報告裁判官[4])、C. Toader、K. Jürimäe、C. Lycourgos 及び N. Piçarra

独立弁論官[5]を M. Campos Sánchez-Bordona、

訴廷管理担当官[6]を 事務官 C. Strömholm

として構成され、

---

1 正文は英語
2 欧州連合条約。最新の consolidated version は ELI: http://data.europa.eu/eli/treaty/teu_2016/oj 参照。
3 欧州連合を機能（させること）に関する条約 Treaty on the Functioning of the European Union。 最新の consolidated version は、ELI: http://data.europa.eu/eli/treaty/tfeu_2016/oj 参照。
4 Rapporteur
5 Advocate General
6 Registrar

書面交換手続及びそれに引き続く 2019 年 9 月 9 日及び 10 日の口頭弁論手続に鑑み、

以下の者を代表して提出された意見陳述書を検討した上で、

- Privacy International、代理として B. Jaffey QC 及び T. de la Mare QC、D. Cashman ソリシター、及び H. Roy 弁護士(avocat)、
- 連合王国政府、訟務代理として Z. Lavery、D. Guðmundsdóttir 及び S. Brandon、代理として G. Facenna QC 及び D. Beard QC、並びに C. Knight 及び R. Palmer バリスター
- ベルギー政府、訟務代理として P. Cottin 及び J.-C. Halleux 並びに J. Vanpraet 弁護士(advocaat)及び E. de Lophem 弁護士(avocat)、
- チェコ政府、訟務代理として M. Smolek、J. Vláčil 及び O. Serdula、
- ドイツ政府、訟務代理として当初 M. Hellmann、R. Kanitz、D. Klebs 及び T. Henze、その後 J. Möller、M. Hellmann、R. Kanitz 及び D. Klebs、
- エストニア政府、訟務代理として A. Kalbus、
- アイルランド、訟務代理として M. Browne、G. Hodge 及び A. Joyce、並びに D. Fennelly バリスター
- スペイン政府、訟務代理として当初 L. Aguilera Ruiz 及び M.J. García-Valdecasas Dorrego、その後 L. Aguilera Ruiz
- フランス政府、訟務代理として当初 E. de Moustier、E. Armoët、A.-L. Desjonquères、F. Alabrune、D. Colas 及び D. Dubois、その後 E. de Moustier、E. Armoët、A.-L. Desjonquères、F. Alabrune 及び D. Dubois、
- キプロス政府、訟務代理として E. Symeonidou 及び E. Neofytou、
- ラトビア政府、訟務代理として当初 V. Soņeca 及び I. Kucina、その後 V. Soņeca、
- ハンガリー政府、訟務代理として当初 G. Koós、M.Z. Fehér、G. Tornyai 及び Z. Wagner、その後 G. Koós 及び M.Z. Fehér
- オランダ政府、訟務代理として C.S. Schillemans 及び M.K. Bulterman
- ポーランド政府、訟務代理として B. Majczyna、J. Sawicka 及び M. Pawlicka、
- ポルトガル政府、訟務代理として L. Inez Fernandes、M. Figueiredo 及び F. Aragão Homem、
- スウェーデン政府、訟務代理として当初 A. Falk、H. Shev、C. Meyer-Seitz、L. Zettergren 及び A. Alriksson、その後 H. Shev、C. Meyer-Seitz、L. Zettergren 及び A. Alriksson

－　ノルウェー政府、訟務代理として T.B. Leming、M. Emberland 及び J. Vangsnes

－　欧州委員会、訟務代理として当初 H. Kranenborg、M. Wasmeier、D. Nardi 及び P. Costa de Oliveira、その後 H. Kranenborg、M. Wasmeier 及び D. Nardi、

－　欧州データ保護監督官、訟務代理として T. Zerdick 及び A. Buchta

2020 年 1 月 15 日の弁論期日において独立弁論官の意見を聴取した後に、

以下のとおり言い渡した。

判　　決

1 この先決裁定請求は、欧州議会及び理事会の 2009 年 11 月 25 日の指令 2009/136/EC (OJ 2009 L 337, p. 11)により改正された電子通信分野における個人データの処理及びプライバシーの保護に関する欧州議会及び理事会の 2002 年 7 月 12 日の指令 2002/58/EC(プライバシー及び電子通信に関する指令)(OJ 2002 L 201, p. 37)(「指令 2002/58」)第 1 条(3)及び第 15 条(1)の TEU 第 4 条(2)及び欧州連合の基本権憲章(「憲章」)第 7 条及び第 8 条及び第 52 条(1)に照らした解釈に関連する。

2 その請求は、Privacy International と外務・コモンウェルス大臣(連合王国)、内務大臣(連合王国)、政府通信本部(連合王国)(「GCHQ」)、保安局(連合王国)(「MI5」)及び秘密諜報部(連合王国)(「MI6」)との間の保安機関及び諜報機関によるバルク通信データ[7]の入手と使用を承認する法令の適法性に関する手続中に行われた。

法的枠組み

欧州連合法

指令 95/46

3 個人データの自動的な処理と関連する個人の保護及びそのデータの支障のない移転に関する欧州議会及び理事会の 1995 年 10 月 24 日の指令 95/46/EC(OJ 1995 L 281, p31)は 2018 年 5 月 25 日を施行日として、個人データの取扱いと関連する自然人の保護に関する、及び、そのデータの自由な移転に関する、並びに、指令 95/46/EC を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の規則(EU) 2016/679 (OJ 2016 L 119, p. 1)により廃止された。「適用範囲」と題する当該指令第 3 条は、以下の通り規定する:

「1. この指令は、その全部又は一部が自動的な手段による個人データの処理に対し、並びに、自動的な手段以外の方法による個人データの処理であって、それをファイリングシステムの一部を構成するもの、又は、ファイリングシステムの一部として構成することが予定されているものに対し適用される。

2. この指令は、以下の個人データの処理には適用されない:

— [TEU]第 5 款及び第 6 款に定める活動のような、欧州共同体法の適用範囲外にある活動の過程で行われる場合、並びに、公共の保安、国防、構成国の保安(処理業務が構成国の

[7] bulk communication data. 単に大量というよりも対象の全量というニュアンスがあるため、「バルク」とした。

保安事項と関係する場合には、構成国の経済成長を含む。)及び刑事法の分野における国の活動と関係する処理業務の場合、

－ 自然人によって、純粋に私的な行為又は家庭内の行為の中で行われる場合。」

指令 2002/58

4 指令 2002/58 の前文第 2 項、第 6 項、第 7 項、第 11 項、第 22 項、第 26 項及び第 30 項は以下の通り規定する:

「 (2) この指令は、基本的な権利の尊重を求めるものであり、特に[憲章]によって認められた諸原則に留意している。この指令は、とりわけ、同憲章の第 7 条及び第 8 条に定める権利を完全に尊重することの確保を求めている。

…

(6) インターネットは、広範な電子通信サービスを供給するための共通でグローバルなインフラを提供することによって、在来の市場構造を転覆している。インターネット上の公衆が利用可能な電子通信サービスは、その利用者に対して新たな可能性を拓くものではあるが、その個人データ及びプライバシーに対して新たなリスクをもたらすものでもある。

(7) 公衆通信ネットワークの場合においては、自然人の基本的権利及び自由並びに法人の正当な利益を保護するために、特に、自動的な記録保存並びに加入者及び利用者に関するデータの処理の能力が増大しつつあることに関して、特別の法令、規則及び技術基準が提供されなければならない。

…

(11) [指令 95/46[8]]と同様に、この指令は、[EU]の法律によって規律されていない行為に関する基本的な権利及び自由の保護の問題に対応していない。それゆえ、個人のプライバシーの権利と、公共の保安、防衛、構成国の国内保安(その活動が構成国の国内保安上の事柄と関連するときは、構成国の経済発展を含む。)及び刑事法の執行のために必要となるこの指令の第 15 条(1)に示す措置を構成国が遂行する可能性との間の既存のバランスに対しては何らの変更も加えられない。その結果として、この指令は、これらの目的のいずれかのために必要があり、かつ、欧州人権裁判所の判決によって解釈される[1950 年 11 月 4 日にローマで署名された]人権及び基本的自由の保護に関する欧州条約に従う場合

[8] 初出だが、Directive 95/46/EC の定義されていない短縮形である。

には、電子通信の適法な傍受その他の措置を遂行するための構成国の権限に影響を与えることはない。そのような構成国の措置は、民主的な社会の中において、適切であり、その目的と厳格に比例するものであり、かつ、必要なものであることを要し、かつ、人権及び基本的自由の保護に関する欧州条約に従い、適切な安全性確保措置が講じられるべきである。

…

(22) 利用者以外の者によって、又は利用者の同意なくなされる通信及び関連するトラフィックデータの記録保存の禁止は、それが電子通信ネットワーク内での通信の遂行の目的によってのみなされるものである限り、その情報の自動的に中間的な処理としてなされる一時的な記録保存を禁止しようとするものではないが、ただし、その情報は、送受信及びトラフィック管理のために必要な期間を超えて記録保存されてはならず、かつ、記録保存されている期間内は、その機密性が保証され続けなければならない。公衆が利用可能な情報を、その受信者の求めに応じて、そのサービスの他の受信者に対して送信することをより効果的なものとする必要があるときは、この指令は、そのような情報がさらに記録保存されることを妨げるものではないが、ただし、その情報は、いかなる場合においても、制限なく公衆からアクセス可能であることを要し、かつ、そのような情報を求める個々の加入者又は利用者を示すデータは消去されなければならない。

…

(26) 電子通信ネットワーク内で接続を確立し、情報を送信するために処理される加入者と関連するデータには、自然人の私生活に関する情報が含まれ、その通信を尊重する権利に関連し、法人の正当な利益と関連する。そのようなデータは、課金若しくは相互接続料金支払請求の目的でのサービスの提供のために必要な範囲内で、かつ、時間を限定してなされる場合においてのみ、記録保存され得る。そのようなデータを別の目的で処理することは、…そのプロバイダが遂行しようとしている別の目的による処理のタイプ、そのような処理について加入者が同意を拒否する権利及び彼又は彼女の同意を撤回することのできる権利について、当該公衆が利用可能な電子通信サービスのプロバイダから、正確かつ完全な情報が加入者に対して提供されていることを前提とした上で、当該加入者がその処理について同意している場合においてのみ、認められる。電子通信サービスのマーケティング…のために用いられるトラフィックデータは、そのサービスの提供が終了した後は、消去され、又は、匿名化されなければならない…。

…

(30) 電子通信ネットワーク及びサービスの提供に用いられるシステムは、必要な個人データの処理を厳格にミニマムなものとして制限するように設計されなければならない。…」

5 「適用範囲及び目的」と題する指令 2002/58 第 1 条は、以下の通り規定する:

「1. この指令は、電子通信分野における個人データの処理と関連する基本的権利及び自由、とりわけプライバシー及び機密性への権利の均一なレベルでの保護を確保し、かつ、[欧州連合]の中におけるそのようなデータの自由な移転及び電子通信機器類とサービスの自由な移転を確保すべきことが求められる構成国の法令を、整合性のとれたものとする。

2. この指令にある条項は、第 1 項で示した目的のために、[指令 95/46] の特則を定め、これを補完する。更に、この指令にある条項は、法人である加入者の正当な利益の保護を提供する。

3. この指令は、欧州連合条約の第 5 款及び 6 款が適用されるような[TFEU]の適用範囲外の活動には適用されない。また、公共の保安、防衛、構成国の保安(その活動が構成国の保安上の事柄と関連するときは、構成国の経済発展を含む。)及び刑事法の分野に属する構成国の活動にも適用されない。」

6 「定義」と題する当該指令第 2 条によると:

「他に定めがある場合を除き、[指令 95/46] 及び電子通信ネットワークとサービスのための共通の規律の枠組みに関する欧州議会及び理事会の 2002 年 5 月 7 日の指令 2002/21/EC(枠組み指令)[(OJ 2002 L 108, p. 33)]にある定義が適用される。

また、以下の定義も適用される:

(a) 「利用者」とは、私的な目的又は業務上の目的で、当該サービスへの加入を必要とせずに、公衆が利用可能な電子通信サービスを利用する自然人を意味する;

(b) 「トラフィックデータ」とは、電子通信ネットワークにおいて通信を送信する目的で提供されるデータ、又は、その課金のために提供されるデータを意味する;

(c) 「位置データ」とは、電子通信ネットワークで処理され、公衆が利用可能な電子通信サービスの利用者の端末機器の地理的位置を示すデータを意味する;

(d) 「通信」とは、公衆が利用可能な電子通信サービスによって、一定数の当事者間で情報を交換し又はそれを送信することを意味する。これは、その情報を受信する識別可能な加入者又は利用者と関連させることのできる情報である場合を除き、電子通信ネットワーク上で公衆に対して提供される放送サービスの一部として送信される情報を含まない;

…」

7 「関連するサービス」と題する当該指令の第 3 条は、以下の通り規定する:

「この指令は、個人データの収集及び個人識別の仕組みを有する公衆通信ネットワークを含め、[欧州連合]の公衆通信ネットワーク内の公衆が利用可能な電子通信サービスの提供と関

連する個人データの処理に適用される。」

8 「通信の機密性」と題する指令 2002/58 第 5 条上:

「1. 構成国は、自国の立法を通じて、公衆通信ネットワーク及び公衆が利用可能な電子通信サービスによる通信及びトラフィックデータの機密性を確保しなければならない。構成国は、第 15 条(1)に従い適法な権限に基づいてなされるものを除き、とりわけ、利用者以外の者により利用者の同意なくなされる通信及び関連するトラフィックデータの聴取、盗聴、記録保存その他の傍受行為又は監視行為を禁止しなければならない。本項は、機密性の原則を妨げることなく、通信の送信のために必要な技術上の記録保存を妨げるものではない。

…

3. 構成国は、関連する加入者及び利用者に対して、就中、処理の目的に関して、[指令 95/46]に従い、明瞭で理解しやすい情報が提供された上で、関係する加入者又は利用者が彼若しくは彼女の同意を与えている場合においてのみ、当該加入者又は利用者の端末機器に情報を記録保存し、又は、そこに既に記録保存されている情報へアクセスすることができることを確保しなければならない。このことは、電子通信ネットワーク上での通信の送信を遂行する目的のみでなされる場合、又は、加入者又は利用者から明示で求められた情報社会サービスのプロバイダがサービスを提供するために必須のものである場合には、技術的な記録保存又はアクセスを妨げるものではない。」

9 「トラフィックデータ」と題する指令 2002/58 第 6 条は以下の通り規定する:

1. 公衆通信ネットワーク又は公衆が利用可能な電子通信サービスのプロバイダによって処理若しくは記録保存された加入者及び利用者に関するトラフィックデータは、通信の送信の目的のために不必要となった場合には、本条の第 2 項、第 3 項及び第 5 項並びに第 15 条(1)を妨げることなく、消去され、又は、匿名化されなければならない。

2. 加入者への課金及び相互接続料金支払請求のために必要なトラフィックデータは、これを処理することができる。課金について適法に検討することのできる期間又は支払の請求がなされている期間の最終日までは、そのような処理をすることが許される。

3.電子通信サービスのマーケティング目的又は付加価値サービスの提供の目的のためには、公衆が利用可能な電子通信サービスのプロバイダは、当該データと関連する加入者又は利用者が彼若しくは彼女の事前の同意を提供している限り、そのようなサービス又はマーケティングのために必要な範囲及び期間内で、第 1 項に示すデータを処理することができる。利用者又は加入者は、トラフィックデータの処理に対して与えた同意をいつでも撤回する可能性を与えられなければならない。

…

5. 第 1 項、第 2 項、第 3 項及び第 4 項に従ってなされるトラフィックデータの処理は、公衆通信ネットワーク及び公衆が利用可能な通信サービスのプロバイダの課金、トラフィック管理、顧客対応、詐欺の検出、通信サービスのマーケティング又は付加価値サービスの提供を取扱う権限に基づいて活動する者に限定されなければならず、また、そのような活動の目的のために必要な範囲内に限定されなければならない。」

10 「トラフィックデータ以外の位置データ」と題する当該指令第 9 条はその第 1 項において以下の通り規定する:

「1. トラフィックデータ以外の位置データが処理され得る場合、そのようなデータは、それらが匿名化されている場合、又は付加価値サービスの提供のために必要な範囲内及びその期間内で、利用者又は加入者の同意がある場合に限り、これを処理することができる。そのサービスプロバイダは、利用者又は加入者に対し、その同意を得る以前に、処理されることになるトラフィックデータ以外の位置データのタイプ、処理の目的及び期間、並びに、付加価値サービスの提供の目的のために当該データが第三者に移転されるか否かについて、通知しなければならない。…」

11 「[指令 95/46]の条項の適用」と題する当該指令第 15 条は、その第 1 項において以下の通り規定する:

「1. 構成国は、当該制限が、[指令 95/46]の第 13 条(1)に示すような自国の保安の防護(すなわち EU 構成国の保安)、防衛、公共の保安、犯罪行為又は電子通信システムの無権限使用の防止、捜査、検出及び訴追のために必要、適切、かつ、民主的な社会の中において比例的な措置となる場合には、この指令の第 5 条、第 6 条、第 8 条(1)、(2)、(3)及び(4)に規定する権利及び義務の範囲を制限するための立法的措置を採択することができる。この目的のために、構成国は、就中、本項に定める根拠に基づき限定された期間内だけ正当化されるデータの保持について定める立法上の措置を講ずることができる。本項に示す全ての措置は、欧州連合条約第 6 条(1)及び(2)に示すものを含め、[EU]法の基本原則に従うものでなければならない。」

規則 2016/679

12 規則 2016/679 第 2 条は以下の通り規定する:

「1. この規則は、その全部又は一部が自動的な手段による個人データの処理に対し、並びに、自動的な手段以外の方法による個人データの処理であって、ファイリングシステムの一部を構成するもの、又は、ファイリングシステムの一部として構成することが予定されているものに対し、適用される。

2. この規則は、以下の個人データの処理には適用されない:

(a) 欧州連合の法律の適用範囲外にある活動の過程で行われる場合;

(b) 構成国によって TEU 第 5 款第 2 章の適用範囲内にある活動が行われる場合;

…

(d) 公共の保安に対する防護及びその脅威の防止を含め、職務権限を有する機関によって犯罪行為の防止、捜査、検知若しくは訴追又は刑罰の執行のために行われる場合。

…」

13 当該規則第 4 条は以下の通り規定する:

「この規則の目的のために:

…

(2)「処理」とは、それが自動的な手段によって行われるか否かを問わず、収集、記録、編集、構成、記録保存、修正若しくは変更、検索、参照、使用、送信による開示、配布又は、それら以外に利用可能なものとすること、整列若しくは結合、制限、消去又は破壊のような、個人データ若しくは一群の個人データに実施される業務又は一群の業務のことを意味する;

…」

14 当該規則第 23 条(1)上:

「データの管理者若しくは処理者が服する欧州連合の法律又は構成国の法律は、その制限が基本的な権利及び自由の本質的部分を尊重するものであり、かつ、以下の対象を防護するために民主主義社会において必要かつ比例的な措置である場合には、第 12 条ないし第 22 条に定める権利及び義務にそれらの法律の条項が対応する範囲内で、立法措置によって、第 12 条ないし第 22 条及び第 34 条並びに第 5 条に定める義務及び権利の適用範囲を制限することができる:

(a) 国家保安;

(b) 防衛;

(c) 公共の保安;

(d) 公共の保安に対する防護及びその脅威への防止を含め、犯罪行為の防止、捜査、検知若しくは訴追又は刑罰の執行;

(e) 欧州連合又は構成国の一般的な公共の利益の上記以外の重要な対象、とりわけ、出納、予算及び税務上の事項を含め、欧州連合又は構成国の重要な経済的な利益若しくは財政上の利益、公衆衛生及び社会保障;

(f) 司法権の独立の保護及び司法手続の保護;

(g) 規制を受ける職種における違背行為の防止、捜査、検知及び訴追;

(h) (a)ないし(e)及び(g)に示す場合において、一時的なものを含め、公的な権限の行使と関係する監視、監督及び規制の権能;

(i) データ主体の保護、又は、それ以外の者の権利及び自由の保護;

(j) 民事訴訟の執行確保。」

15 規則 2016/679 第 94 条(2)上:

「廃止される指令への参照は、この規則への参照として解釈される。[指令 95/46]の第 29 条によって設立された個人データの処理と関連する個人の保護に関する作業部会に対する参照は、この規則によって設立される欧州データ保護委員会への参照として解釈される。」

連合王国法

16 1984 年電気通信法第 94 条の、主手続における事実に適用される版(「1984 年法」)[9]において、「国家保安等の利益における指示」と題されるものは、以下の通り規定する:

「(1) 国務大臣は、本条が適用される者の意見を聞いた後、国家保安又は連合王国外の国又は地域の政府との関係の利益のため必要となる旨国務大臣が思える一般的な特徴の指示をその者に対して発出できる。

(2) 国務大臣が国家保安又は連合王国外の国又は地域の政府との関係の利益のためにそうする必要があると思われる場合、国務大臣は、本条が適用される者と協議した後、その者に、(事案の状況に応じて)その指示中に指定された特定のことをする、又はしないことを要求する指示を発出できる。

(2A) 国務大臣は、指示によって要求される行為がその行為によって達成されることが求められていることに比例すると彼が信じない限り、第(1)項又は第(2)項に基づく指示を与えてはならない。

(3) 本条が適用される者は、2003 年通信法の第 1 部又は第 2 部第 1 章によって、又はその下で課せられたその他の義務にもかかわらず、本条に基づいて国務大臣から与えられた指示に効力付与[10]しなければならず、そして、公衆電子通信ネットワークのプロバイダへの指示の

---

[9] この先決裁定を受け、主手続では、1984 年法第 94 条の EU 法不適合が判決により宣言されている。[2021] UKIPTrib IPT_15_110_CH para 25.

[10] give effect

場合、それがそのようなネットワークのプロバイダ以外の立場で彼に関係しているにもかかわらず、効力付与しなければならない。

(4) 国務大臣は、彼が、指示の開示が国家保安又は連合王国外の国若しくは地域の政府との関係の利益又は任意の者の商業的利益に反する旨の意見を有していない限り、各議院に本条に基づいて与えられたすべての指示の写しを提示しなければならない。

(5) 国務大臣が、国務大臣はある事柄の開示が国家保安又は連合王国外の国若しくは地域の政府との関係の利益又は任意の者の商業的利益に反する旨の意見であることを通知した場合、通知を受けた者は、本条に基づいて行われたいかなることも開示したり、立法又はその他の方法で開示を要求したりしてはならない。

…

(8) 本条は、[通信庁(OFCOM)]及び公衆電子通信ネットワークのプロバイダに適用される。」

17 2000 年調査権限規則法[11]（「RIPA」）第 21 条(4)及び(6)は以下の通り規定する:

「(4) … 「通信データ」は以下のいずれかを意味する―

(a) 送信中又は送信される可能性のある郵便サービス又は電気通信システムの目的で、通信に含まれる、又は通信に(送信者によるかどうかを問わず)添付されるトラフィックデータ;

(b) 通信の内容を(第(a)号に該当する情報を除き)含まず、任意の者による以下に関する利用―

(i) 郵便サービス又は電気通信サービス;又は

(ii) 電気通信サービスの任意の者への提供又は任意の者による利用に関連する、電気通信システムの任意の部分;

(c) 郵便サービス又は電気通信サービスを提供する者によって、彼がサービスを提供する相手方に関して保持又は取得される、第(a)号又は第(b)号に該当しない情報。

…

(6) …「トラフィックデータ」は任意の通信に関して、以下を意味する ―

(a) そこから、又はそれに対する通信が送信される、又は送信される可能性のある者、装置、又は場所を特定する、又は特定することを目的とするデータ、

[11] Regulation of Investigatory Powers Act 2000

(b) 通信が、その手段により又はそれを通じて、送信されるか又は送信される可能性のある装置を識別する若しくは選択する、又は識別する若しくは選択することを目的とする、データ、

(c) 任意の通信の送信を(全体的又は部分的に)有効化するための電気通信システムの目的で使用される装置の起動のための信号により構成される任意のデータ、及び

(d) データを識別するデータ、又は、特定の通信に含まれるか若しくは添付されるデータであるその他のデータを識別するデータ。

…」

18 RIPA 第 65 条から第 69 条は調査権限法廷(連合王国)の機能と管轄に関する規則を定めている。RIPA 第 65 条上、データが不適切に取得されたと信じる理由がある場合は、調査権限法廷に裁判を申し立てる[12]ことができる。

主手続の争点及び先決裁定のために照会された質問

19 2015 年初頭、連合王国のさまざまな保安機関及び諜報機関、すなわち GCHQ、MI5、及び MI6 によるバルク通信データの取得及び使用に関する実務の存在が、議会諜報及び保安委員会(連合王国)による報告書中のものを含み、明らかとなった。 2015 年 6 月 5 日、非政府組織である Privacy International は、それらの実務の適法性を争い、外務及びコモンウェルス大臣、内務大臣、及びそれらの保安機関及び諜報機関に対して、調査権限法廷(連合王国)に訴訟を提起した。

20 照会元裁判所は、まず、国内法及び 1950 年 11 月 4 日にローマで署名された人権及び基本的自由の保護に関する欧州条約[13](「ECHR」)の、そしてその後、EU 法の規定に照らして、これらの実務の適法性を検討した。 2016 年 10 月 17 日の判決において、当該裁判所は、主手続の被告は、これらの機関がその活動において、たとえば、経歴データ若しくは旅行データ、財務情報若しくは商業情報、専門家の秘密若しくはジャーナリスティックな資料の対象となるセンシティブなデータを含むおそれのある通信データなどのバルク個人データのセットを取得して使用したことを認めたと判示した。さまざまな、場合によっては秘密の手段によって取得されたそのデータは、クロスチェックと自動処理によって分析され、そして他者や他の当局に開示され、外国のパートナーと共有できた。その文脈では、保安機関及び諜報機関は、とりわけ、1984 年法第 94 条に基づいて国務大臣によって発出された指示の下で、公衆電子通信ネットワークのプロバイダから取得したバルク通信データも使用していた。GCHQ と MI5 は、それぞれ 2001 年と 2005 年からこれを行っていた。

---

[12] complaint

[13] European Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5)

21 照会元裁判所は、データの取得と使用に関するこれらの措置は国内法に合致しており、2015 年以降、これらの措置及び第三者へのデータの送信の比例性に関して引き続き検討されている問題次第では、ECHR 第 8 条にも合致すると認定した。その点、特に保安機関及び諜報機関がデータにアクセスし、外部に開示するための手続、データを保持するための措置、及び独立した監督の措置に関して、適用可能な防護措置に関する証拠が提出されたと述べた。

22 EU 法に照らしての、主手続で争点となっている取得及び使用手段の適法性に関して、照会元裁判所は、2017 年 9 月 8 日の判決において、これらの措置が EU 法の適用範囲内にあるかどうか、そしてその場合、それらが EU 法に適合しているかどうかを検討した。当該裁判所は、バルク通信データに関して、電子通信ネットワークのプロバイダは、1984 年法の第 94 条に基づき、国務大臣がその旨の指示を発出すれば、保安機関及び諜報機関に彼らの EU 法の適用範囲内にある経済活動の過程において収集されたデータを提供する義務があると判断した。しかし、そのような強制権限を使用せずにこれらの機関によって取得された他のデータはそうではない。その解釈に基づいて、照会元裁判所は、1984 年法第 94 条に起因するような制度が EU 法の適用範囲内にあるかどうか、そして、もしそうであるなら、2016 年 12 月 21 日付 *Tele2 Sverige and Watson and Others* 判決(C-203/15 及び C-698/15 併合事件 EU:C:2016:970;「*Tele2*」)から生じた判例法によって定められた要件が当該制度に適用されるか、そしてどのように適用されるかを判断するために当裁判所に質問を照会する必要があると考えた。

23 その点に関して、その先決裁定請求において、照会元裁判所は、1984 年法第 94 条に従い、国務大臣は、電子通信サービスのプロバイダに、国家保安又は外国政府との関係の利益のために必要と思われる一般的又は特定の指示を与えることができると述べている。RIPA 第 21 条(4)及び(6)に定められた定義を参照して、当該裁判所は、関連するデータには、その規定の意味の範囲内で、トラフィックデータ及びサービス利用情報が含まれ、通信の内容のみが除外されると述べた。 このようなデータと情報により、特に、通信の「誰が、どこで、いつ、どのように」を知ることができる。そのデータは保安機関及び諜報機関に送信され、それらの活動の目的のためにそれらによって保持される。

24 照会元裁判所によると、主手続で問題となっている制度は、2016 年 12 月 21 日の *Tele2* 判決(C-203/15 及び C-698/15 併合事件 EU:C:2016:970)をもたらした 2014 年データ保持及び調査権限法[14]による制度とは異なる。なぜなら、後者の制度では、電子通信サービスのプロバイダによるデータ保持と、国家保安の利益のための保安機関及び諜報機関に対するだけでなく、その他の当局に対する、それらの需要に応じたそのデータの利用可能性が規定されているからである。さらに、その判決は国家保安ではなく、犯罪捜査に関するものだった。

25 照会元裁判所は、保安機関及び諜報機関によって集約されたデータベースは、未知の脅威を発見することを目的として、バルク、不特定かつ自動的な処理の対象になると付け加えた。

[14] Data Retention and Investigatory Powers Act 2014

その点、照会元裁判所は、このように集約されたメタデータのセットは、そこに隠された「針」を見つけるために「干し草の山」を持つように、可能な限り包括的でなければならなかったと述べている。これらの機関によるバルクデータ取得とそのデータを照会するための手法の有用性に関して、当該裁判所は、特に、当時、連合王国テロリズム法独立審査官であった David Anderson QC によって作成された 2016 年 8 月 19 日付報告書の調査結果に言及するが、Anderson QC はそのレポートを作成する際に、諜報専門家のチームによって実施された審査と、保安機関及び諜報機関の公務員の証言に依拠した。

26 また、照会元裁判所は、Privacy International によれば、主手続で問題となっている制度は EU 法に照らして違法であり、一方、主手続の被告は、その制度によって規定される、データを移転する義務、当該データへのアクセス及びその使用は、特に、国家保安は各加盟国の固有の責任として残存するとする TEU 第 4 条(2)に従って、欧州連合の権限の範囲内にはない、と考えている、と述べる。

27 その点に関して、調査権限法廷は、公共の保安を防護する目的での搭乗者名記録データの移転に関する 2006 年 5 月 30 日付 *Parliament v Council and Commission* 判決(C-317/04 及び C-318/04 併合事件 EU:C:2006:346 第 56 項から第 59 項)に基づいて、国家保安を防護する目的でデータを処理及び移転する商業事業者の活動は、EU 法の適用範囲に含まれないようである、と判断した。照会元裁判所にとって、問題の活動がデータ処理を構成するかどうかではなく、そのような活動の目的が、TEU 第 4 条(2)の意味の範囲内で、公共の保安に関連する公共当局によって確立された枠組みを通じて、実質的にも効果としても、各構成国の不可欠な機能を前進させることであるかどうかのみを審査する必要がある。

28 それにもかかわらず、主手続で問題となっている措置が EU 法の適用範囲に入る場合、照会元裁判所は、2016 年 12 月 21 日付 *Tele2* 判決(C-203/15 及び C-698/15 併合事件 EU:C:2016:970)第 119 項から第 125 項に定められた要件は、国家保安の文脈では不適切であるように思われ、国家保安に対する何らかの脅威に取り組む保安機関及び諜報機関の能力を弱体化させる、と考える。

29 そのような状況において、調査権限法廷は手続を中断し、先決裁定のために以下の質問を当裁判所に照会することを決定した:

「次のような:

(a) 提供された[バルク通信データ]を利用する[保安機関及び諜報機関の]権能は、テロ対策、スパイ対策、及び核拡散対策の分野を含む、連合王国の国家保安の防護に不可欠であって;

(b) [保安機関及び諜報機関]による[バルク通信データ]の利用の基本的な特徴は、[これらのデータ]の一カ所への集約に依存する、標的を絞らないバルク技術手段によって国家保安に対するこれまで知られていなかった脅威を発見することである。その主な有用性は、

迅速なターゲットの特定及び促進、並びに差し迫った脅威に直面した場合の行動の基盤を提供することにあり;

(c) その後、電子通信ネットワークのプロバイダは、[バルク通信データ]を(通常のビジネスに必要な期間を超えて)保持する義務はなく、それは、構成国([保安機関及び諜報機関])のみによって保持され;

(d) 構成国の裁判所は、[保安機関及び諜報機関]による[バルク通信データ]の使用を取り巻く防護措置が ECHR の要件と合致していることを(特定の留保された問題を別にして)認定済であり;そして

(e) 構成国の裁判所が、[2016 年 12 月 21 日付 *Tele2* 判決(C-203/15 及び C-698/15 併合事件 EU:C:2016:970)の第 119 項から第 125 項]に記された要件を課すことは、もし適用されると、[保安機関及び諜報機関]が国家保安を防護するために講じた措置を妨げ、それによって連合王国の国家保安を危険にさらすことになると認定した;

状況では

(1) TEU 第 4 条及び[指令 2002/58]第 1 条(3)に鑑み、国務大臣による指示における電子通信ネットワークのプロバイダに対して、バルク通信データを構成国の[保安機関及び諜報機関]に提供しなければならないという義務付けは、欧州連合法及び[指令 2002/58]の適用範囲に含まれるか?

(2) 質問(1)の回答が「はい」の場合、[2016 年 12 月 21 日付 *Tele2* 判決(C-203/15 及び C-698/15 併合事件 EU:C:2016:970) 第 119 項から第 125 項に記載されている保持された通信データに適用される要件]又はその他 ECHR によって課された要件以上の要件は、国務大臣によるそのような指示に適用されるか?そして、もしそうなら、国家保安を防護するためにバルク取得と自動処理の技術を使用する[保安機関及び諜報機関]の不可欠な必要性と、それ以外の場合は ECHR に準拠しており、そのような要件を課すことによって重大な障害が生じる可能性がある、そのような能力の範囲を考慮に入れて、それらの要件はどのように、そしてどの程度適用されるか?」

照会された質問の検討

質問1

30 照会元裁判所はその最初の質問で、要するに、TEU 第 4 条(2)に照らして読む指令 2002/58 の第 1 条(3)は、構成国の当局が電子通信サービスのプロバイダに国家保安を防護する目的でトラフィックデータと位置データを保安機関及び諜報機関に転送することを要求することを可能にする国内法が当該指令の適用範囲に含まれることを意味するものと解釈されるのかどうかを問う。

31 この点、Privacy International は、要するに、指令 2002/58 の適用範囲に関して司法裁判所の判例法から導き出された指針に鑑みると、1984 年法第 94 条に基づいて保安機関及び諜報機関がこれらのプロバイダからデータを取得すること、及びこれらの機関がそのデータを利用することの双方は、そのデータがリアルタイムで実施される送信によって取得されるか、その後に取得されるかにかかわらず、当該指令の適用範囲に含まれると主張している。特に、国家保安の防護という目的が同指令の第 15 条(1)に明示的に記載されていることは、同指令がそのような状況に適用されないことを意味するものではなく、その評価は TEU 第 4 条(2)の影響を受けないと主張している。

32 対照的に、連合王国、チェコ及びエストニア政府、アイルランド、並びにフランス、キプロス、ハンガリー、ポーランド及びスウェーデン政府は、要するに、指令 2002/58 は主手続で争点となっている国内法令には適用されない、なぜなら当該法令の目的は国家保安を防護することだからと主張する。これらの政府は、保安機関及び諜報機関の活動は法及び秩序の維持並びに国家保安及び領土保全の防護に関する不可欠な構成国の機能であり、それゆえに、特に TEU 第 4 条(2)第 3 文で証明されるように加盟国に固有の責任であると主張する。

33 これらの政府によれば、したがって、指令 2002/58 を、国家保安の防護に関する国内措置がその適用範囲に含まれることを意味すると解釈することはできない。当該指令第 1 条(3)は当該指令の適用範囲を規定しており、指令 95/46 の第 3 条(2)の第 1 インデントで以前に規定されていたように、公共の保安、防衛、及び構成国の保安に関する活動は当該適用範囲から除外されている。これらの規定は TEU 第 4 条(2)に定められている権限の分配を反映しており、国家保安分野の措置が指令 2002/58 の要件を満たす必要がある場合には、実務的な効果が奪われることになる。さらに、指令 95/46 の第 3 条(2)の最初のインデントに関する 2006 年 5 月 30 日の *Parliament v Council and Commission* 判決(C-317/04 及び C-318/04 併合事件 EU:C:2006:346)から派生した当裁判所の判例法は指令 2002/58 の第 1 条(3)に類推適用することができる。

34 この点、指令 2002/58 はその第 1 条(1)上、電子通信分野における個人データの処理に関して基本的権利と自由、特にプライバシーと機密性への権利の均等な保護レベルを確保するために、就中、必要な国内規定の整合化を規定していることを述べておくべきである。

35 当該指令第 1 条(3)はその適用範囲から、刑事法の分野並びに公共の保安、防衛、構成国の保安、そして、その活動が構成国の保安上の事柄と関連するときは、構成国の経済発展を含む、特定された分野における「構成国の活動」を除外している。このように例示により言及された活動は、いずれにせよ、構成国の活動又は構成国当局の活動であって、個人が活発な分野とは無関係である(2018 年 10 月 2 日付 *Ministerio Fiscal* 判決 C-207/16 事件 EU:C:2018:788 第 32 項及び引用された判例法)。

36 加えて、指令 2002/58 第 3 条は、当該指令が、個人データの収集及び個人識別の仕組みを有する公衆通信ネットワークを含め、欧州連合の公衆通信ネットワーク内の公衆が利用可能な

電子通信サービス(「電子通信サービス」)の提供と関連する個人データの処理に適用されると規定する。したがって、当該指令は、そのようなサービスのプロバイダの活動を規制するものとみなされなければならない(2018 年 10 月 2 日付 *Ministerio Fiscal* 判決 C-207/16 事件 EU:C:2018:788 第 33 項及び引用された判例法)。

37 その文脈では、指令 2002/58 第 15 条(1)は、構成国が、規定された条件に服すかぎり、「[当該指令]第 5 条、第 6 条、第 8 条(1)、(2)、(3)及び(4)並びに第 9 条に規定する権利及び義務の範囲を制限するための立法的措置」を採択することができる、と規定する(2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 71 項)。

38 指令 2002/58 第 15 条(1)は、それが、当該指令が規定する条件を充足するときにのみ、構成国が立法的措置を採択することを明示的に許可しているため、言及されている構成国の立法的措置が当該指令の適用範囲内であることを必然的に前提としている。さらに、そのような措置は、当該条項に言及されている目的では、電子通信サービスのプロバイダの活動を規制する(2018 年 10 月 2 日付 *Ministerio Fiscal* 判決 C-207/16 事件 EU:C:2018:788 第 34 項及び引用された判例法)。

39 当裁判所が、指令 2002/58 第 15 条(1)は、その第 3 条と相俟って読むと、当該指令の適用範囲は、電子通信サービスのプロバイダにトラフィックデータ及び位置データを保持することを義務づける立法的措置だけではなく、彼らが当該データへの職務権限を有する当局のアクセスを許すことを義務づける立法的措置にも拡張することを意味すると解釈されねばならない、と判示してきたのは、就中、上述の考え方に照らしたものである。そのような立法的措置は、それらのプロバイダによるそのデータの処理を必然的に伴い、そしてそれらのプロバイダの活動を規制する限りにおいて、指令 2002/58 第 1 条(3)に規定する構成国に特徴的な活動であるとみなすことはできない(この点、2018 年 10 月 2 日付 *Ministerio Fiscal* 判決 C-207/16 事件 EU:C:2018:788 第 35 項及び 37 項並びに引用された判例法を参照)。

40 職務権限を有する当局が電子通信サービスのプロバイダに対し、バルクデータを送信により保安機関及び諜報機関に開示する指示を与えることができることを根拠づける 1984 年法第 94 条のような立法措置については、規則 2016/679 第 4 条(2)に規定された定義に従い、当該規則第 94 条(2)と併せて読む指令 2002/58 第 2 条に基づき適用される「個人データの処理」の概念が、「自動的な手段によって行われるか否かを問わず、収集、… 記録保存、… 照会、使用、送信による開示、配布又は、それら以外に利用可能なものとする、個人データ若しくは一群の個人データに実施される業務又は一群の業務」のことを指すことに留意すべきである。

41 そうすると、データの記録保存又はその他の方法で利用可能にすることと同様に、送信による個人データの開示は指令 2002/58 第 3 条の目的のための処理を構成し、したがって、当該指令の適用範囲に入ることになる(この点については、2008 年 1 月 29 日付 *Promusicae* 判決 C-275/06 事件 EU:C:2008:54 第 45 項を参照)。

42 加えて、上記第 38 項に記した考え方及び指令 2002/58 の一般的な構造に鑑みると、当該措置が追求しなければならない目的が当該同じ指令の第 1 条(3)に言及される活動が追求する目的と相当重複しているためにその第 15 条(1)に言及される立法措置が当該指令の適用範囲から除外されるという当該指令の解釈は、その第 15 条(1)の実効を一切奪うことになる(この点、2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 72 項及び第 73 項参照)。

43 指令 2002/58 第 1 条(3)に示された「活動」の概念は、したがって、独立弁論官により、要するに、彼の *La Quadrature du Net and Others* (C-511/18 及び C-512/18 併合事件 EU:C:2020:6)の意見第 75 項において指摘されたとおり、当該指令第 15 条(1)に示された立法措置を包含するものと解釈することはできない。

44 本判決第 32 項に列挙した政府が参照する TEU 第 4 条(2)は、当該結論を無効にできない。実際、当裁判所の確立した判例法によると、構成国の不可欠な保安の利益を定義し、彼らの域内及び域外の保安を確保する適切な措置を採択するのは、構成国であるが、国家保安を防護する目的で各国の措置が講じられたという単なる事実により EU 法を不適用とすることはできず、構成国の EU 法を遵守する義務から構成国を免除することはできない(この点、2013 年 6 月 4 日付 *ZZ* 判決 C-300/11 事件 EU:C:2013:363 第 38 項; 2018 年 3 月 20 日付 *Commission v Austria (State printing office)*判決 C-187/16 事件 EU:C:2018:194 第 75 項及び第 76 項; 2020 年 4 月 20 日付 *Commission v Poland, Hungary and Czech Republic* (国際的庇護の申請者の移送に関する暫定措置)判決 C-715/17、C-718/17 及び C-719/17 併合事件 EU:C:2020:257 第 143 項及び第 170 項参照)。

45 確かに、2006 年 5 月 30 日付 *Parliament v Council and Commission* 判決 (C-317/04 及び C-318/04 併合事件 EU:C:2006:346 第 56 項から第 59 項)において、当裁判所は、航空会社から第三国の公共当局へのテロリズム及び他の重大な犯罪を防止し、それらと闘う目的での個人データの移転は、指令 95/46 第 3 条(2)第 1 段落により、当該移転が公共の保安に関する公共の当局により確立された枠組みに入るため、当該指令の適用範囲には入らない、と判示した。

46 しかしながら、本判決第 36 項、第 38 項及び第 39 項に記された考え方に鑑み、当該判例法は指令 2002/58 第 1 条(3)の解釈に類推適用できない。実際、独立弁論官が彼の *La Quadrature du Net and Others* (C-511/18 及び C-512/18 併合事件 EU:C:2020:6)の意見第 70 項から第 72 項において指摘したとおり、要するに、当該判例法が関係する指令 95/46 第 3 条(2)の第 1 段落は、一般的方法で、当該指令の適用範囲から「公共の保安、国防、[及び]構成国の保安に関する処理業務」を、だれが関連するデータ処理作業を実行したかによりいかなる区別もせず、除外している。対照的に、指令 2002/58 第 1 条(3)を解釈する文脈では、そのような区別をする必要がある。上記第 37 項から第 39 項及び第 42 項から明らかなとおり、電子通信サービスのプロバイダにより実行される個人データを処理するすべての業務は、公共当局によりそのようなプロバイダに課された義務によりなされる処理業務も含み、当該指令 2002/58 の適用範

囲に入るが、一方、そのような処理業務が、適切な場合には、反対に、指令 95/46 第 3 条(2)の第 1 段落に規定する、公共の保安、国防又は構成国の保安に関するすべての処理業務を含む例外の範囲に、当該条項の広汎な書きぶりのために、それらの業務が実行される者にかかわらず、入る可能性はある。

47 さらに、2006 年 5 月 30 日付 *Parliament v Council and Commission* (C-317/04 及び C-318/04 併合事件 EU:C:2006:346)判決をもたらして事件の争点となった指令 95/46 が、規則 2016/679 第 94 条(1)にしたがい、2018 年 5 月 25 日を発効日として廃止され、当該規則により置き換えられたことに留意すべきである。当該規則がその第 2 条(2)(d)において、「職務権限を有する当局により」就中、公共の保安に対する脅威の防護と防止を含む刑事犯罪の防止と検知の目的で、実行された処理作業には適用されないと規定するものの、当該規則第 23 条(1)(d)及び(h)からは、同じ目的で個人により実行された個人データの処理が、当該規定の適用範囲に入るのは明らかである。したがって、指令 2002/58 第 1 条(3)、第 3 条及び第 15 条(1)の上記解釈は、当該指令により補完され、指定された規則 2016/679 の適用範囲の定義と一貫性を有する。

48 対照的に、構成国が、電子通信サービスのプロバイダに処理義務を課すことなく電子通信を秘密として守るという定めから逸脱する措置を直接実装する場合、関係する者のデータの保護は指令 2002/58 ではなく、犯罪行為の防止、捜査、検知若しくは訴追のため、又は刑罰の執行のために職務権限を有する当局によって処理される個人データについての自然人の保護及び個人データの支障の無い移転についての、かつ理事会枠組み決定 2008/977/JHA を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の指令(EU) 2016/680 (OJ 2016 L 119, p. 89) の適用を条件として、自国の法のみが適用され、その結果、当該問題となる措置は、就中、自国の憲法及び ECHR の緒要件を遵守しなければならない。

49 上述の検討内容に鑑み、最初の質問に対する回答は、指令 2002/58 の第 1 条(3)、第 3 条及び第 15 条(1)は、TEU 第 4 条(2)に照らして読むと、構成国の当局が電子通信サービスのプロバイダに国家保安を防護する目的でトラフィックデータ及び位置データを保安機関及び諜報機関に転送するよう義務づけることを可能とする国内立法が当該指令の適用範囲に入ることを意味すると解釈されなければならない、となる。

質問2

50 照会元裁判所はその第 2 の質問により、要するに、指令 2002/58 の第 15 条(1)が TEU の第 4 条(2)並びに憲章の第 7 条、第 8 条、第 11 条及び第 52 条(1)に照らして読むと、構成国の当局が、電子通信サービスのプロバイダに、国家保安を防護する目的で保安機関及び情報機関へのトラフィックデータと位置データの網羅的かつ無差別な送信を実施することを義務づけることを可能にする国内法令を排除するものと解釈されるかどうかを確認しようとしている。

51 予備的な観点として、先決裁定の請求書に記された情報によると、1984 年法第 94 条では、

国務大臣が国家保安又は外国政府との関係の利益のために必要であると考えた場合、指示によって電子通信サービスのプロバイダにバルク通信データを保安機関及び諜報機関に転送するよう要求することを許可していることを念頭におくべきである。このデータには、RIPA 第 21 条(4)及び(6)に基づき、利用されたサービスに関する情報だけではなく、トラフィックデータ及び位置データが含まれる。当該条項は、就中、(i)通信の発信元及び発信先を識別特定し、(ii)通信の日時、長さ、種類を決定し、(iii) 使用されているハードウェアを識別特定し、(iv) 端末機器及び通信の位置を特定するために必要なデータを対象としている。そのデータには、就中、利用者の名前及び住所、電話をかけた者の電話番号及びその者にかけられた電話番号、通信の発信元及び宛先の IP アドレス並びに訪問したウェブサイトのアドレスなどが含まれる。

52 このような送信によるデータの開示は、電子通信手段のすべての利用者に関係するものであり、その送信がリアルタイムで行われるか、それともその後に行われなければならないかが特定されていない。一旦送信されたデータは、先決裁定の請求に記載された情報によれば、保安機関及び諜報機関によって保持され、これらの機関が維持する他のデータベースと同様に、これらの機関により彼らの活動の目的のために利用可能であり続ける。特に、このようにして取得されたデータは、バルク自動処理及び分析の対象となり、異なるカテゴリーのバルク個人データを含む他のデータベースと照合されたり、これらの機関の外部及び第三国に開示されたりする可能性がある。最後に、これらの業務は、裁判所や独立行政当局からの事前承認を必要とせず、いかなる場合も関係者への通知が伴わない。

53 指令 2002/58 の目的は、就中、その前文第 6 項及び第 7 項から明らかなように、新技術、特にデータの自動化された記録保存と処理の能力の増大に起因する個人データとプライバシーへのリスクから電子通信サービスの利用者を保護することである。とりわけ、当該指令はその前文第 2 項に記載されているとおり、憲章第 7 条及び第 8 条に規定される権利が完全に尊重されることを確保することを追求している。この点、指令 2002/58 を生み出した電子通信分野における個人データの処理とプライバシーの保護に関する欧州議会と理事会の指令の提案(COM (2000) 385 final)の説明書からは、EU の立法者が「使用される技術にかかわらず、個人データとプライバシーの高レベルの保護がすべての電子通信サービスで継続して保証されることを確保する」ことを追求していることが明らかである。

54 そのため、指令 2002/58 の第 5 条(1)では、「構成国は、自国の立法を通じて、公衆通信ネットワーク及び公衆が利用可能な電子通信サービスによる通信及び関連するトラフィックデータの機密性を確保しなければならない。」と規定する。当該情報は、「[構成国]が、第 15 条(1)に従い適法な権限に基づいてなされるものを除き、とりわけ、利用者以外の者により利用者の同意なくなされる通信及び関連するトラフィックデータの聴取、盗聴、記録保存その他の傍受行為又は監視行為を禁止しなければならない。」ことも強調し、「本項は、機密性の原則を妨げることなく、通信の送信のために必要な技術上の記録保存を妨げるものではない。」と規定する。

55 このように、当該指令第 5 条 1 項は、電子通信とそれに関連するトラフィックデータの双方の機密性の原則を謳っており、就中、利用者以外の者が利用者の同意なしにこれらの通信とデータを記録保存することを原則として禁止することを求めている。その文言の一般的な性質を考慮すると、この規定は、通信の送信以外の目的で、第三者が通信とそれに関連するデータを知ることができるような作業を必然的に対象としている。

56 指令 2002/58 の第 5 条(1)に定める通信とそれに関連するデータの傍受の禁止は、したがって、トラフィックデータと位置データがその後どのように利用されるかにかかわらず、保安機関及び諜報機関などの公共機関による当該データの保持だけではなく、電子通信サービスのプロバイダが当該機関に当該データを利用可能にするあらゆる状況を包含する。

57 このように、当該指令を採択するにあたり、EU の立法者は、電子通信サービスの利用者が、原則として、彼らの通信及び、関連するデータが、匿名のままであって記録されてはならないことを、彼らが別段の合意をしない限り、期待する権利を有するように、憲章第 7 条及び第 8 条に謳われた権利について具体的な表現をした(2020 年 10 月 6 日付 *La Quadrature du Net and Others* 判決 C-511/18、C-512/18 及び C-520/18 併合事件第 109 項)。

58 しかしながら、指令 2002/58 第 15 条(1)は、構成国が個人データの機密性を確保するための当該指令第 5 条(1)に規定する義務の原則及び就中、当該指令第 6 条及び第 9 条に示される関連する義務への例外を、そのような制限が、国家保安、防衛、公共の保安を防護するため、及び、犯罪行為又は電子通信システムの無権限使用の防止、捜査、検知及び訴追のために民主的な社会の中において必要、適切、かつ、比例的な措置となる場合には、導入できるようにしている。そのため、構成国は、就中、これらの理由のうち一つにより正当化される限定された期間のデータの保全を規定する立法措置を採択できる。

59 とはいえ、指令 2002/58 第 5 条、第 6 条及び第 9 条に規定する権利及び義務から逸脱する選択権は、電子通信及びそれに関連するデータの機密性を確保するための原則の義務、とりわけ、当該指令第 5 条に明示的に規定されている当該データの記録保存の禁止に対する例外が規範となることまでは許容できない(2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 89 項及び第 104 項、並びに 2020 年 10 月 6 日付 *La Quadrature du Net and Others* 判決 C-511/18、C-512/18 及び C-520/18 併合事件第 111 項参照)。

60 加えて、指令 2002/58 第 15 条(1)第 3 文から、当該指令第 5 条、第 6 条及び第 9 条に規定された権利と義務の適用範囲を制限する立法措置を採択することを、比例性の原則を含む EU 法の一般原則及び憲章により保障された基本的権利にしたがわない限り、構成国が許されていないことは明らかである。この点、当裁判所は、構成国により構成国法令によって、必要な場合、職務権限を有する当局が利用可能にする目的で、電子通信サービスのプロバイダに課されたトラフィックデータを保持する義務が、プライバシーの保護及び個人データの保護にそれぞれ関係する憲章第 7 条及び第 8 条だけではなく、表現の自由に関係する憲章第 11 条への適合性の問題を生じることを以前から判示している(この点、2014 年 4 月 8 日付 *Digital*

Rights Ireland and Others 判決 C-293/12 及び C-594/12 併合事件 EU:C:2014:238 第 25 項及び第 70 項、2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 91 項及び第 92 項並びに引用された判例法参照)。

61 それらの同じ問題は、利用者以外の者への当該データの送信又はその利用を目的とした当該データへのアクセスといった他の種類のデータ処理についても生じる(類推により、2017 年 7 月 26 日付意見 1/15(*EU-カナダ PNR 協定*)EU:C:2017:592、122 項及び 123 項並びに引用された判例を参照)。

62 したがって、指令 2002/18 第 15 条(1)の解釈には、当裁判所の判例法から生じたとおり、憲章第 7 条により保障されるプライバシーへの権利及びその第 8 条により保障される個人データを保護される権利の重要性と並んで、表現の自由への権利の重要性も、憲章第 11 条で保障される当該基本権が、多元的な民主的社会の不可欠の土台を構成し、かつ TEU 第 2 条上、欧州連合がその上に築かれた価値観の一つであることを踏まえ、考慮に入れなければならない(この点、2001 年 3 月 6 日付 *Connolly v Commission* 判決 C-274/99 P 事件 EU:C:2001:127 第 39 条及び 2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 93 項参照)。

63 しかしながら、憲章第 7 条、第 8 条及び第 11 条に謳われている権利は絶対的な権利ではなく、社会における機能との関係で検討されなければならない(この点、2020 年 7 月 16 日付 *Facebook Ireland and Schrems* 判決 C-311/18 事件 EU:C:2020:559 第 172 項及び引用された判例を参照)。

64 確かに、憲章第 52 条 1 項から見て取れるように、当該規定は、これらの権利の行使に制限を加えることを認めているが、ただし、これらの制限が、法律で規定されており、これらの権利の本質を尊重し、比例性の原則にしたがって、必要であり、かつ、欧州連合が認めた一般的利益の目的又は他人の権利と自由を保護する必要性を真に満たす、という条件下である。

65 基本的権利の行使に対するいかなる制限も法律によって規定されなければならないという要件は、これらの権利への干渉を許可する法的根拠自体が、関連する権利の行使に対する制限の範囲を定義しなければならないことを意味することを付言すべきである(2020 年 7 月 16 日付 *Facebook Ireland and Schrems* 判決 C-311/18 事件 EU:C:2020:559 第 175 項及び引用された判例法)。

66 比例性の原則の遵守に関連して、指令 2002/58 第 15 条(1)前段は、構成国は当該規定に定める目的を考慮して、当該措置が「民主的社会の中で…必要、適切かつ比例的」である場合には、通信及び関連するトラフィックデータが秘密にされるという原則を逸脱する措置を採用できる旨規定している。同指令前文第 11 項は、このような性質の措置は、企図された目的に「厳密に」比例していなければならないと規定している。

67 この点、当裁判所の確立した判例法によれば、プライバシーへの基本権の保護は、個人デー

タの保護についての逸脱及び制限が、厳格に必要な場合にのみ適用しなければならないことを要求していることに留意すべきである。加えて、一般的利益の目的は、当該一般的利益の目的を問題となっている基本的権利と適切に均衡を取ることにより、その措置から影響を受ける基本的権利との整合をとらなければならない、という事実を鑑みずに追求してはならない(この点、2008 年 12 月 16 日付 *Satakunnan Markkinapörssi and Satamedia* 判決 C-73/07 事件 EU:C:2008:727 第 56 項; 2010 年 11 月 9 日付 *Volker und Markus Schecke and Eifert* 判決 C-92/09 及び C-93/09 併合事件 EU:C:2010:662 第 76 項、第 77 項及び第 86 項;並びに 2014 年 4 月 8 日付 *Digital Rights* 判決 C-293/12 及び C-594/12 併合事件 EU:C:2014:238 第 52 項; 2017 年 7 月 26 日付意見 1/15 *(EU-Canada PNR Agreement)*EU:C:2017:592 第 140 項参照)。

68 比例性の要件を満たすためには、法令は問題の措置の適用範囲及び実装を統制し、最小限の防護措置を課す明瞭で精緻な規則を、その個人データが影響を受ける者が、当該データが非違行為のリスクから効果的に保護されることの十分な保障を有するよう、規定しなければならない。当該法令は国内法上、法的拘束力を有し、とりわけ、どの状況で、かつどの条件の下そのようなデータの処理を規定する措置が採択できるかを示さなければならず、それにより干渉が厳格に必要な範囲に限定されていることを確保する。そのような防護措置の必要性は、個人データが自動化された処理の対象となる場合、とりわけ当該データへの違法なアクセスの多大なリスクがある場合、さらに大きい。これらの考え方は、特に、機微なデータである特定の種類の個人データの保護が問題となっている場合、適用される(この点、2014 年 4 月 8 日付 *Digital Rights Ireland and Others* 判決 C-293/12 及び C-594/12 併合事件 EU:C:2014:238 第 54 項及び第 55 項、2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 117 項、2017 年 7 月 26 日付意見 1/15*(EU-Canada PNR Agreement)*EU:C:2017:592 第 141 項を参照のこと)。

69 主手続で問題となっているような国内法が指令 2002/58 第 15 条(1)の要件を満たしているかどうかという問題については、憲章第 7 条、第 8 条、第 11 条及び第 52 条(1)に照らして読むと、保安機関及び諜報機関のような利用者以外の者へのトラフィックデータ及び位置データの送信は機密性の原則を逸脱することに留意すべきである。本事件の事実のようにその運用が網羅的かつ無差別に行われる場合、それはデータの機密性を確保する原則の義務に対する例外を規則にする効果があるが、他方、指令 2002/58 によって確立されたシステムではその例外は例外のままであることが要求される。

70 加えて、当裁判所の確立された判例法によれば、トラフィックデータ及び位置情報データの第三者への送信は、当該データがその後どのように使用されるかにかかわらず、憲章の第 7 条及び第 8 条に謳われた基本的権利への干渉を構成する。この点、人の私生活に関連する問題の情報が機微であるかどうか、あるいはその干渉のために関係する者が何らかの形で不便を被っているかどうかは問題ではない(この点、2017 年 7 月 26 日付意見 1/15(*EU-カナダ PNR 協定*)EU:C:2017:592 第 124 項及び第 126 項、並びに引用された判例、並びに 2020 年 10 月 6 日付 *La Quadrature du Net and Others* 判決 C-511/18、C-512/18 及び C-520/18 併合事件第 115 項

及び第 116 項参照)。

71 トラフィックデータと位置データを保安機関及び諜報機関に送信することによってもたらされる憲章第 7 条に謳われた権利への干渉は、就中、当該データが提供する可能性のある情報の機微な性質、当該情報が実際の通信の内容に劣らず機密性が高いこと、特に、当該データに基づいて関連する者のプロフィールを確立する可能性を考慮すると、特に深刻であると考えなければならない。さらに、それは、関連する者の心の中に、自分の私的生活が常に監視の対象であるという感覚を生み出すおそれがある(類推により、2014 年 4 月 8 日付 *Digital Rights Ireland and Others* 判決 C-293/12 及び C-594/12 併合事件 EU:C:2014:238 第 27 項及び第 37 項、及び 2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 99 項及び第 100 項を参照)。

72 また、保安目的でトラフィックデータや位置データを公的機関に送信することは、それ自体、憲章第 7 条に謳われている通信を尊重される権利を侵害し、電子通信手段の利用者が憲章第 11 条で保障された表現の自由を行使することを萎縮させるおそれがあることに留意すべきである。そのような萎縮は、とりわけ自己の通信が、職業上の機密保持義務にかかる者及びその行為が連合法違反を通報した者の保護に関する欧州議会及び理事会の 2019 年 10 月 23 日の指令(EU) 2097/1937 (OJ 2019 L 305, p. 17)によって保護される公益通報者に影響を与え得る。さらに、その萎縮効果は、保持されるデータの量と範囲を考えると、より深刻である(この点、2014 年 4 月 8 日付 *Digital Rights Ireland and Others* 判決 C-293/12 及び C-594/12 併合事件 EU:C:2014:238 第 28 項、2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 101 項、2020 年 10 月 6 日付 *La Quadrature du Net and Others* 判決 C-511/18、C-512/18 及び C-520/18 事件第 118 項参照)。

73 最後に、一般的な保持手段によって継続的に保持される大量のトラフィックデータと位置データ、及びそれらのデータが提供する可能性のある情報の機微性を考慮すると、電子通信サービスのプロバイダがそれらのデータを単に保持するだけでも、非違行為と不法なアクセスのリスクが必然的に生ずる。

74 このような干渉を正当化する目的、特に主手続で問題となっている国家保安を防護する目的については、TEU 第 4 条(2)が国家保安は各構成国の単独の責任として残されていると規定していることを最初に指摘しておく。その責任は、構成国の不可欠な機能と社会の基本的な利益を保護するという主たる利益に対応するものであり、一国の憲法上、政治的、経済的、又は社会的な基本的構造を著しく不安定にする、そして、特にテロリストの活動のような社会、住民、構成国自体を直接脅かす可能性がある活動の予防及び処罰を含む(2020 年 10 月 6 日付 *La Quadrature du Net and Others* 判決 C-511/18、C-512/18 及び C-520/18 併合事件第 135 項)。

75 TEU 第 4 条(2)に照らして読むと、国家保安の防護の目的の重要性は、指令 2002/58 第 15 条(1)に言及される他の目的、就中、一般的な犯罪との闘い、それどころか重大犯罪との闘い及び公共の保安の防護の目的の重要性を超える。上記第 74 項に言及されているような脅威は、

その性質及び特別な深刻度から、公共の保安に影響する緊張又は混乱が生じる、たとえそれが深刻な性質であるとしても、一般的なリスクと区別できる。憲章第 52 条(1)に規定するその他の要件の充足を条件に、国家保安の防護の目的は、従って、基本権へのより深刻な干渉を必然的に伴う措置を、それら他の目的により正当化できるかもしれない措置よりも、正当化できる。(2020 年 10 月 6 日付 *La Quadrature du Net and Others* 判決 C-511/18、C-512/18 及び C-520/18 併合事件第 136 項)。

76 しかしながら、個人データの保護からの逸脱及び制限は厳密に必要な限りにおいてのみ適用されなければならないという上記 67 項で言及された比例性の要件を満たすためには、憲章第 7 条及び第 8 条に謳われた基本的権利への干渉を伴う国内法は、上記第 65 項、第 67 項及び第 68 項で引用された判例法に由来する要件に合致しなければならない。

77 特に、当局の個人データへのアクセスに関しては、法律は、当局のデータへのアクセスが当該法律の追求する目的と合致していることを要求するだけにとどまることはできず、その使用を統制する実体的及び手続的条件も定めなければならない(2017 年 7 月 26 日付意見 1/15(*EU-カナダ PNR 協定*)、EU:C:2017:592、192 項及び引用された判例法を類推して参照)。

78 したがって、追求された目的と少なくとも間接的な繋がりがあるかどうかにかかわらず、保持されたすべてのデータへの一般的なアクセスは、厳格に必要なものに限定されているとみなすことはできないため、トラフィックデータ及び位置データへのアクセスを統制する国内法は、職務権限を有する国内当局が問題となっているデータへのアクセスを認められる状況及び条件を定義するために、客観的な基準に依拠しなければならない(この点、2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 119 項及び引用された判例を参照)。

79 これらの要件は、立法措置に基づき、職務権限を有する国内当局が、電子通信サービスのプロバイダに対し、網羅的かつ無差別な送信により、トラフィックデータ及び位置データを保安機関及び諜報機関に開示するよう求めることができる、主手続で問題となっているような立法措置にも、よりいっそう、適用される。当該送信は、当該データを公的機関が利用できるようにする効果がある(2017 年 7 月 26 日付意見 1/15(*EU-カナダ PNR 協定*)、EU:C:2017:592、第 212 項を類推して参照)。

80 トラフィックデータと位置情報の送信が網羅的かつ無差別に行われることから、電子通信サービスを利用するすべての人に影響を与えるという点で包括的である。したがって、その行為が、間接的又は遠いものでさえも、国家保安の防護の目的との連関がある可能性があることを示唆する証拠がなく、特に、送信されるデータと国家保安への脅威との間にいかなる関係も確立されていない者にも適用される(この点、2014 年 4 月 8 日付 *Digital Rights Ireland and Others* 判決 C-293/12 及び C-594/12 併合事件 EU:C:2014:238 第 57 項及び第 58 項、並びに 2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 105 項参照)。このようなデータを公共当局に送信することは、上記第 79 項の判示に従えば、アクセスと均

等であるという事実に鑑みると、公共当局へのデータの網羅的かつ無差別な送信を許可する法律は、網羅的なアクセスを必然的に伴うものであると判断しなければならない。

81 そうすると、電子通信サービスのプロバイダが網羅的かつ無差別に送信する手段でトラフィックデータと位置情報を保安機関及び諜報機関に開示することを義務付ける構成国法は厳格に必要な範囲を超えており、TEU 第 4 条(2)並びに憲章第 7 条、第 8 条、第 11 条及び第 52 条(1)に照らして読む指令 2002/58 第 15 条(1)で要求されるように民主主義社会の中で正当化されるとは考えられない。

82 前述のすべての検討に照らして、第 2 の質問に対する回答は、指令 2002/58 の第 15 条(1)は、TEU 第 4 条(2)並びに憲章第 7 条、第 8 条、第 11 条及び第 52 条(1)に照らして読むと、構成国の当局が、電子通信サービスのプロバイダに国家保安を防護する目的で保安機関及び諜報機関へのトラフィックデータと位置データの網羅的かつ無差別な送信を実行することを義務づけることを可能にする国内法を排除するものと解釈されなければならない。

費用

83 この手続は、主手続の当事者にとって、国内裁判所に係属中の訴訟の一段階であるため、費用に関する決定は当該裁判所の問題である。裁判所に意見書を提出する際に発生した費用は、当該当事者の費用を除き、回収できない。

これらの理由により、当裁判所(大法廷)はここに判決する:

1. 欧州議会及び理事会の 2009 年 11 月 25 日の指令 2009/136/EC により改正された電子通信分野における個人データの処理及びプライバシーの保護に関する欧州議会及び理事会の 2002 年 7 月 12 日の指令 2002/58/EC(プライバシー及び電子通信に関する指令)第 1 条(3)、第 3 条及び第 15 条(1)は、TEU 第 4 条(2)に照らして読むと、構成国の当局が電子通信サービスのプロバイダに対して、トラフィックデータ及び位置データを、国家保安を防護する目的で保安機関及び諜報機関に転送することを義務づけることを可能とする国内立法は、当該指令の適用範囲に入ることを意味すると解釈されなければならない。

2. 指令 2009/136/により改正された指令 2002/58 の第 15 条(1)は、TEU 第 4 条(2)並びに欧州連合の基本権憲章第 7 条、第 8 条、第 11 条及び第 52 条(1)に照らして読むと、構成国の当局が、電子通信サービスのプロバイダに国家保安を防護する目的で保安機関及び諜報機関へのトラフィックデータと位置データの網羅的かつ無差別な送信を実行することを義務づけることを可能にする国内法を排除するものと解釈されなければならない。

Lenaerts　Silva de Lapuerta　Bonichot

Arabadjiev　Prechal　Safjan

Xuereb	Rossi	Malenovský
Bay Larsen	von Danwitz	Toader
Jürimäe	Lycourgos	Piçarra

ルクセンブルグの公開法廷で 2020 年 10 月 6 日に言い渡した。

A. Calot Escobar	K. Lenaerts
Registrar	President

La Quadrature du Net and Others 判決
C-511/18、C-512/18 及び C-520/18 先決裁定併合事件 ECLI:EU:C:2020:791

[参考訳]

2022 年 1 月 9 日

明治大学法学部教授

丸　橋　　透

＊＊＊

REQUESTS for a preliminary ruling under Article 267 TFEU from the Conseil d'État (Council of State, France), made by decisions of 26 July 2018, received at the Court on 3 August 2018 (C-511/18 and C-512/18), and from the Cour constitutionnelle (Constitutional Court, Belgium), made by decision of 19 July 2018, received at the Court on 2 August 2018 (C-520/18), in the proceedings **La Quadrature du Net** (C-511/18 and C-512/18), **French Data Network** (C-511/18 and C-512/18), **Fédération des fournisseurs d'accès à Internet associatifs** (C-511/18 and C-512/18), **Igwan.net** (C-511/18) **v Premier ministre** (C-511/18 and C-512/18), **Garde des Sceaux, ministre de la Justice** (C-511/18 and C-512/18), **Ministre de l'Intérieur** (C-511/18), **Ministre des Armées** (C-511/18), interveners: **Privacy International** (C-512/18), **Center for Democracy and Technology** (C-512/18), and **Ordre des barreaux francophones et germanophone**, **Académie Fiscale ASBL**, **UA**, **Liga voor Mensenrechten ASBL**, **Ligue des Droits de l'Homme ASBL**, **VZ**, **WY**, v **Conseil des ministres**, interveners: **Child Focus** (C-520/18)

2020 年 10 月 6 日付欧州連合司法裁判所(CJEU)大法廷判決 C-511/18、C-512/18 及び C-520/18 先決裁定併合事件 ECLI:EU:C:2020:791 英語版テキスト(正文はフランス語)に基づき、和訳を試みた。英語版テキストは、EUR-Lex Web サイトから入手した。

https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62018CJ0511
[2022 年1月 8 日確認]

本判決に先立つ 2020 年 1 月 15 日付独立弁論官(Advocate General) Campos Sánchez-Bordona の C-511/18 及び C512/18 併合事件に関する意見(書) ECLI:EU:C:2020:6 英語版テキスト(正文はスペイン語)並びに C520/18 事件に関する意見(書)ECLI:EU:C:2020:7 英語版テキスト(正文はフランス語)は同じく EUR-Lex から入手できる。

https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62018CC0511
https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62018CC0520
[2022 年 1 月 8 日確認]

―解　説―

1. EU 法と構成国法関係の解説

本判決は EU の指令 2002/58/EC(プライバシー及び電子通信に関する指令)(OJ 2002 L 201, p. 37)第 15 条(1)、指令 2000/31/EC(電子商取引指令)(OJ 2000 L 178, p. 1)第 12 条から第 15 条の欧州連合基本権憲章(「憲章」)第 4 条、第 6 条、第 7 条、第 8 条、第 11 条及び第 52 条(1) 並びに欧州連合条約第 4 条(2)及びに照らして読む解釈を判示している。

電子商取引に関する指令は、Eur-LEX からテキストを入手できる。

https://eur-lex.europa.eu/eli/dir/2000/31/oj
[2022 年 1 月 8 日確認]

その他 EU の法令については、国内保安目的での大量のメタデータの当局への移転という隣接したテーマを判示した同日付 *Privacy International* 判決 C-623/17 先決裁定事件 ECLI:EU:C:2020:790[参考訳]（本号 410 頁所収）の解説を参照。

本先決裁定判決を受けて、フランス国務院は、2021 年 4 月 21 日付で判決した(Case no. 393099, ECLI:FR:CEASS:2021:393099.20210421)。英訳が以下のサイトから入手できる。

https://www.conseil-etat.fr/en/judging
https://www.conseil-etat.fr/arianewebtraduite/#/view-document/529　(英訳への直リンク)
[2022 年 1 月 8 日確認]

この判決を受けた法令改正の現状は、脚注に記した。

また、ベルギー憲法裁判所は、2021 年 4 月 22 日付判決(Arrêt n° 57/2021)により、関連するベルギー法を無効とし、各データの種類に応じて CJEU 判決に沿うよう厳格に必要な範囲に干渉を限定するよう再起案するよう命じたとされる。

2. 参考訳作成における基本方針

この参考訳においては，La Quadrature du Net and Others 判決の全文を訳出した。

この参考訳は，あくまでも La Quadrature du Net and Others 判決の私的な和訳である。公式訳でも確定訳でもない。

この参考訳は，現時点における研究成果を反映するものである。将来，更に研究を深めた結果として修正すべき部分を発見したときは，その時点において，改訂版等を作成すべきかどうかを検討する。

訳出に際しては原則として直訳とすることとしたが，直訳のままでは日本語になりにくい箇所に関しては，やむを得ず意訳とした。

判決文原文には原注はない。読みやすさのため英語以外の言語の原語表記等を注釈とした他、若干の訳者の注釈を付した。

読みやすさを重視し，引用条文中の項(paragraph) 号(point)の表記は判決英語版の表記通り(1)(2)・・・、(a)(b)・・・としている。

フランスの法文の構造については、調査しきれていない。たとえば、「Article L. 851-1」の「-1」は枝番と思われるが、「bis」を使った条文もある。この参考訳では、「第 L. 851-1 条」、「bis」についてだけ「の 2」のように訳した。

この参考訳は，Eur-lex のデータ二次利用条件を遵守して作成した。

3. 訳語に関する補足的説明

4. 関連参考訳及び参考文献

Privacy International 判決 C-623/17 先決裁定事件 ECLI:EU:C:2020:790[参考訳]（本号 410 頁所収）の解説を参照。

この参考訳には夏井高人教授の重要な助言が反映されている。

＊＊＊

2020 年 10 月 6 日付欧州連合司法裁判所（大法廷）判決[1]

(先決裁定の照会 — 電子通信分野における個人データの処理 — 電子通信サービスのプロバイダ —トラフィックデータ及び位置情報データの網羅的かつ無差別の保持 — データの自動化された分析 — データへのリアルタイムアクセス — 国家保安の防護及びテロリズムとの闘い — 指令 2002/58/EC — 適用範囲 — 第 1 条(3)及び第 3 条 — 電子通信の機密性 — 保護 — 第 5 条 及び 第 15 条(1) 指令 2000/31/EC — 適用範囲 — 欧州連合基本権憲章 — 第 4 条、第 6 条、第 7 条、第 8 条、第 11 条及び第 52 条(1) — 欧州連合条約第 4 条(2))

C-511/18、C512/18 及び C-520/18 併合事件において、

2018 年 7 月 26 日付決定によりフランス国務院[2]から出され、2018 年 8 月 3 日に当裁判所において受領した(C-511/18 及び C-512/18)及び 2018 年 7 月 19 日付決定によりベルギー憲法裁判所[3]から出され、2018 年 8 月 2 日に当法廷で受領した(C-520/18)、以下の手続に関する TFEU[4] 第 267 条に基づく先決裁定請求において、

La Quadrature du Net (C-511/18 及び C-512/18)、**French Data Network** (C-511/18 及び C-512/18)、**Fédération des fournisseurs d'accès à Internet associatifs** (C-511/18 及び C-512/18)、**Igwan.net** (C-511/18)

対

首相[5] (C-511/18 及び C-512/18)、**国璽尚書兼法務大臣**[6] (C-511/18 及び C-512/18)、**内務大臣**[7](C-511/18)、**軍大臣**[8](C-511/18)、

参加人: **Privacy International** (C-512/18)、**Center for Democracy and Technology** (C-512/18)

及び

---

1 正文はフランス語
2 Conseil d'État
3 Cour constitutionnelle
4 Treaty on the Functioning of the European Union 最新の consolidated text は、ELI: http://data.europa.eu/eli/treaty/tfeu_2016/2020-03-01 参照。
5 Premier ministre
6 Garde des Sceaux, ministre de la Justice
7 Ministre de l'Intérieur
8 Ministre des Armées

Ordre des barreaux francophones et germanophone、Académie Fiscale ASBL、UA、Liga voor Mensenrechten ASBL、Ligue des Droits de l'Homme ASBL、VZ、WY、XX

対

閣僚会議[9]

参加人: **Child Focus**

(以上 C-520/18)

当裁判所(大法廷)は、

裁判所長官である K. Lenaerts、裁判所副長官である R. Silva de Lapuerta、小法廷裁判長である J.-C. Bonichot、 A. Arabadjiev、A. Prechal、M. Safjan、P.G. Xuereb 及び L. S. Rossi、裁判官である J. Malenovský、L. Bay Larsen、T. von Danwitz (進行・報告裁判官10)、C. Toader、K. Jürimäe、C. Lycourgos 及び N. Piçarra

独立弁論官[11]を M. Campos Sánchez-Bordona、

訴廷管理担当官[12]を 事務官 C. Strömholm

として構成され、

書面交換手続及びそれに引き続く 2019 年 9 月 9 日及び 10 日の口頭弁論手続に鑑み、

以下の者を代表して提出された意見陳述書を検討した上で、

- La Quadrature du Net、the Fédération des fournisseurs d'accès à Internet associatifs、 Igwan.net 及び the Center for Democracy and Technology、代理として A. Fitzjean Ò Cobhthaigh 弁護士 (avocat)、
- French Data Network、代理として Y. Padova 弁護士(avocat)、
- Privacy International、代理として H. Roy 弁護士(avocat)、
- the Ordre des barreaux francophones et germanophone、代理として E. Kiehl、P. Limbrée、 E.

9 Conseil des ministres
10 Rapporteur
11 Advocate General
12 Registrar

Lemmens、A. Cassart 及び J.-F. Henrotte 弁護士(avocats)、

- the Académie Fiscale ASBL 及び UA、代理として J.-P. Riquet
- the Liga voor Mensenrechten ASBL、代理として J. Vander Velpen 弁護士(avocat)、
- the Ligue des Droits de l'Homme ASBL、代理として R. Jespers 及び J. Fermon 弁護士(avocats)
- VZ、WY 及び XX、代理として D. Pattyn 弁護士(avocat)、
- Child Focus、代理として N. Buisseret、K. De Meester 及び J. Van Cauter 弁護士(avocats)、
- フランス政府、訟務代理として当初 D. Dubois、F. Alabrune、D. Colas、E. de Moustier 及び A.-L. Desjonquères、その後 D. Dubois、F. Alabrune、E. de Moustier 及び A.-L. Desjonquères
- ベルギー政府、訟務代理として PJ.-C. Halleux、P. Cottin 及び C. Pochet、代理として J. Vanpraet、Y. Peeters、S. Depré 及び E. de Lophem 弁護士(avocat)
- チェコ政府、訟務代理として M. Smolek、J. Vláčil 及び O. Serdula、
- デンマーク政府、訟務代理として当初 J. Nymann-Lindegren、M. Wolff 及び P. Ngo、その後 J. Nymann-Lindegren 及び M. Wolff
- ドイツ政府、訟務代理として当初 by J. Möller、M. Hellmann、E. Lankenau、R. Kanitz 及び T. Henze、その後 J. Möller、M. Hellmann、E. Lankenau 及び R. Kanitz、
- エストニア政府、訟務代理として N. Grünberg 及び A. Kalbus、
- アイルランド、訟務代理として A. Joyce 、M. Browne 及び G. Hodge、代理として D. Fennelly バリスター
- スペイン政府、訟務代理として当初 L. Aguilera Ruiz 及び M.J. García-Valdecasas Dorrego、その後 L. Aguilera Ruiz
- キプロス政府、訟務代理として E. Neofytou、
- ラトビア政府、訟務代理として V. Soņeca、
- ハンガリー政府、訟務代理として当初 M.Z. Fehér 及び Z. Wagner、その後 M.Z. Fehér、
- オランダ政府、訟務代理として M.K. Bulterman 及び M.A.M. de Ree
- ポーランド政府、訟務代理として B. Majczyna、J. Sawicka 及び M. Pawlicka、

- ポルトガル政府、訟務代理として L. Inez Fernandes、M. Figueiredo 及び F. Aragão Homem、
- スウェーデン政府、訟務代理として当初 H. Shev、H. Eklinder、C. Meyer-Seitz 及び A. Falk、その後 H. Shev、H. Eklinder、C. Meyer-Seitz 及び J. Lundberg、
- 連合王国政府、訟務代理として S. Brandon、代理として G. Facenna QC 及び C. Knight バリスター
- [2020 年 11 月 16 日付命令により削除]
- 欧州委員会、訟務代理として当初 H. Kranenborg、M. Wasmeier 及び P. Costa de Oliveira、その後 H. Kranenborg 及び M. Wasmeier、
- 欧州データ保護監督官、訟務代理として T. Zerdick 及び A. Buchta

2020 年 1 月 15 日の弁論期日において独立弁論官の意見を聴取した後に、

以下のとおり言い渡した。

判　　決

1 これらの先決裁定請求は、欧州議会及び理事会の 2009 年 11 月 25 日の指令 2009/136/EC (OJ 2009 L 337, p. 11)により改正された電子通信分野における個人データの処理及びプライバシーの保護に関する欧州議会及び理事会の 2002 年 7 月 12 日の指令 2002/58/EC(プライバシー及び電子通信に関する指令)(OJ 2002 L 201, p. 37)(「指令 2002/58」)第 15 条(1)及び、域内市場における情報社会サービス、特に電子商取引の特定の法的側面に関する欧州議会及び理事会の 2000 年 6 月 8 日の指令 2000/31/EC(「電子商取引に関する指令」)(OJ 2000 L 178, p. 1)の第 12 条から第 15 条の欧州連合基本権憲章(「憲章」)第 4 条、第 6 条、第 7 条、第 8 条、第 11 条及び第 52 条(1) 並びに TEU[13]第 4 条(2)及びに照らして読む解釈に関連する。

2 C-511/18 事件の請求は、La Quadrature du Net、French Data Network、Fédération des fournisseurs d'Accès à Internet associatifs、Igwan.net を一方当事者として、フランスの首相、国璽尚書兼法務大臣、内務大臣、軍大臣を他方当事者とする、以下の法令の適法性に関する訴訟手続中に行われた: 専門的諜報機関を指定する 2015 年 9 月 28 日の布告第 2015-1185 号[14](2015 年 9 月 29

[13] Treaty on European Union。最新の consolidated text は ELI: http://data.europa.eu/eli/treaty/teu_2016/2020-03-01 参照。

[14] décret no 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement

日のフランス共和国官報[15] (JORF) 1/97「布告第 2015-1185 号」); 許可の対象となる諜報技術の実施及び国家安全保障の問題に関するファイルに関する訴訟についての 2015 年 10 月 1 日の布告第 2015-1211 号[16](2015 年 10 月 2 日の JORF 7/108「布告第 2015-1211 号」); 国内保安法典第 8 巻第 V 款に言及された技術を使用する権限を有する専門的諜報機関以外のサービスの指定に関する、同第 L. 811-4 条に基づいて採択された 2015 年 12 月 11 日の布告第 2015-1639 号[17](2015 年 12 月 12 日の JORF 28/127「布告第 2015-1639 号」);及び諜報収集技術に関する 2016 年 1 月 29 日の布告第 2016-67 号[18](2016 年 1 月 31 日の JORF 2/113「布告第 2016-67 号」)が含まれる。

3 C-512/18 事件の請求は、French Data Network、La Quadrature du Net 及び Fédération des fournisseurs d'accès à Internet associatifs を一方当事者として、フランスの首相及び封印の番人兼法務大臣を他方当事者とする、郵便及び電子通信法典[19](「CPCE」)第 R. 10-13 条及びオンラインに投稿されたコンテンツの作成に寄与した者を特定するために使用できるデータの保持と通信に関する 2011 年 2 月 25 日の布告第 2011-219 号[20](2011 年 3 月 1 日付 JORF 32/170「布告第 2011-219 号」)の適法性に関する訴訟手続中に行われた。

4 C-520/18 事件の請求は、Ordre des barreaux francophones et germanophone、Académie Fiscale ASBL, UA、Liga voor Mensenrechten ASBL、Ligue des Droits de l'Homme ASBL, VZ, WY 及び XX を一方当事者とし、ベルギーの閣僚会議を他方当事者とするその間の訴訟における、電子通信分野におけるデータの収集と保持に関する 2016 年 5 月 29 日の法律[21](2016 年 7 月 18 日ベルギー官報 p. 44717;「2016 年 5 月 29 日の法律」)の適法性に関する訴訟手続中に行われた。

---

15 Journal Officiel de la République Française

16 décret no 2015-1211 du 1er octobre 2015 relatif au contentieux de la mise en ouvre des Techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État

17 décret no 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application of l'article L. 811-4 du code de la sécurité intérieure

18 décret no 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement

19 code des postes et des communications électroniques

20 décret no 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne

21 loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques

法的枠組み

EU 法

指令 95/46

5 個人データの自動的な処理と関連する個人の保護及びそのデータの支障のない移転に関する欧州議会及び理事会の 1995 年 10 月 24 日の指令 95/46/EC(OJ 1995 L 281, p31)は 2018 年 5 月 25 日を施行日として、個人データの取扱いと関連する自然人の保護に関する、及び、そのデータの自由な移転に関する、並びに、指令 95/46/EC を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の規則(EU) 2016/679(OJ 2016 L 119, p1)[22]により廃止された。当該指令第 3 条(2)は、以下の通り規定する:

「この指令は、以下の個人データの処理には適用されない:

- 欧州連合条約の第 5 款及び第 6 款に定める活動のような、欧州共同体法の適用範囲外にある活動の過程で行われる場合、並びに、公共の保安、国防、構成国の保安(処理業務が構成国の保安事項と関係する場合には、構成国の経済成長を含む。)及び刑事法の分野における国の活動と関係する処理業務の場合、
- 自然人によって、純粋に私的な行為又は家庭内の行為の中で行われる場合。」

6 「司法救済、法的責任及び制裁」と題する指令 95/46 第 3 章にある当該指令第 22 条は、以下のとおりの文言である:

「司法機関に対する申立ての前の行政上の救済、就中、第 28 条に示す監督官による救済を妨げることなく、構成国は、当の処理に適用可能な構成国法によって彼に保障された権利のいかなる侵害についても司法救済を求める全ての者の権利を定める。

指令 97/66[23]

7 「通信の機密性」と題する、通信分野における個人データの処理及びプライバシーの保護に関する欧州議会及び理事会の 1997 年 12 月 15 日の指令 97/66/EC 第 5 条上:

「1. 構成国は、自国の法令を介して、公衆通信ネットワーク及び公衆が利用可能な通信サー

---

22 以下「規則 2016/679」と略されている。
23 初出だが指令 97/66/EC を略している。

ビスによる通信の機密性を確保しなければならない。とりわけ、第 14 条第 1 項に従って適法に承認された場合を除き、関係する利用者の同意なしに、当該利用者以外の者によって、通信の聴取、タッピング、記録保存、その他の傍受又は監視が行われることを禁止しなければならない。

2. 第 1 項は、商取引その他の企業活動上の通信の証拠を提供する目的のために適法な企業実務の過程における法的に認められる通信の記録行為に対しては影響を及ぼさない。」

指令 2000/31

8 指令 2000/31 の前文 14 及び 15 は以下の通り規定する:

「(14) 個人データの処理と関連する個人の保護は、情報社会サービスに完全に適用可能な指令[95/46]及び指令[97/66]によってのみ、規律され; これらの指令は、個人データの分野における欧州共同体の法的枠組みを既に確立しており、それゆえ、域内市場の円滑な稼働、とりわけ、構成国間における個人データの支障のない移転を確保するために、この指令内でその問題をカバーすべき必要性はない; この指令の実装及び適用は、個人データの保護と関連する基本原則、とりわけ、望まない商業通信及び中間介在者の責任に関する基本原則を完全に遵守して行われなければならない; この指令は、インターネットのようなオープンネットワークの匿名利用を妨げてはならない。

(15) 通信の秘密は、指令[97/66]第 5 条によって保障される; 同指令に従い、構成国は、法的に認められる場合を除き、送信者及び受信者以外の者によるそのような通信のいかなる種類の傍受又は監視も禁止しなければならない。」

9 指令 2000/31 第 1 条は以下の文言である:

「1. この指令は、構成国間において情報社会サービスの支障の無い移動を確保することにより、域内市場の適正な稼働に貢献することを求める。

2. この指令は、第 1 項に定める目的を達成するために必要となる範囲内で、域内市場と関連する情報社会サービス、サービスプロバイダの事業所、商業通信、電子契約、中間介在者の法的責任、行動準則、訴訟外の紛争解決、訴訟行為及び構成国間の協力に関する一定の国内条項を整合化する。

3. この指令は、それが情報社会サービスを提供する自由を制限しない限り、欧州共同体の法令及びそれを実装する国内立法によって定められている、とりわけ、健康及び消費者の利益の保護のレベルを妨げることなく、情報社会サービスに適用可能な欧州共同体の法律を補充する。

…

5. この指令は、以下に対しては適用されない:

…

(b) 指令[95/46]及び指令[97/66]の適用のある情報社会サービスと関連する問題;

…」

10 指令 2000/31 第 2 条は以下の文言である:

「この指令の目的のために、以下の用語は、以下の意味をもつ:

(a) 「情報社会サービス」:[[欧州議会及び理事会の 1998 年 7 月 20 日の]指令 98/48/EC[(OJ 1998 L 217, p. 18)]による改正後の[技術標準及び技術規則の分野及び情報社会サービス関連法令の分野における情報提供手続を定める欧州議会及び理事会の 1998 年 6 月 22 日の]指令 98/34/EC[(OJ 1998 L 204, p. 37)] の第 1 条(2)の意味におけるサービス;

…」

11 指令 2000/31 第 15 条は以下のとおり規定する:

「1. 構成国は、プロバイダに対し、第 12 条、第 13 条及び第 14 条の範囲内にあるサービスを提供する際、彼らが送信又は記録保存する情報を監視すべき一般的な義務を課してはならず、違法な行為であるとの徴候を示す事実又は状況を積極的に探索すべき一般的な義務を課してもならない。

2. 構成国は、情報社会サービスプロバイダに対し、彼らのサービスを受ける者により違法な行為が行われていること又は提供された情報の疑いを、職務権限を有する行政機関に率先して通知すべき義務、又は、その機関の要請に応じて、彼らが記録保存の合意をもつ彼らのサービスを受ける者の識別を可能とする情報を、職務権限を有する機関に連絡すべき義務を定めることができる。」

指令 2002/21

12 電子通信ネットワーク及びサービスの共通の規制枠組みを定める欧州議会及び理事会の 2002 年 3 月 7 日の指令 2002/21/EC(「枠組み指令」) (OJ 2002 L 108, p. 33)[24]前文第 10 項は以下

[24] 以下「指令 2002/21」と略している。

の通り規定する:

「指令[98/48 により改正された 98/34]第 1 条にある「情報社会サービス」の定義は、オンラインで行われる広範な経済活動を対象としている。これらの活動の大半は、電子通信ネットワーク上の信号の搬送によりその全部又は主要部分が構成されていないため、この指令の適用範囲に含まれない。音声電話及び電子メールの搬送サービスはこの指令の適用範囲内である。たとえばインターネットサービスプロバイダのような同一の事業体は、インターネットへのアクセスのような電子通信サービス及びこの指令の適用範囲外である、ウェブベースのコンテンツの提供のようなサービスの双方を提供できる。」

13 指令 *2002/21* 第 2 条は以下の通り規定する:

「この指令の目的のために:

…

(c) 「電子通信サービス」とは、通常は対価を得るために提供され、放送に用いられる電気通信サービス及びネットワーク上の伝送サービスを含む、その全部又は主要部分が電子通信ネットワーク上の信号の搬送により構成されるサービスであって、電子通信ネットワーク及びサービスを用いて伝送されたコンテンツを提供し又は編集権限をコンテンツに行使するサービスを除外したものを意味し、それは、全部又は主要部分が電子通信ネットワーク上の信号の搬送により構成されない指令[98/34]第 1 条に定義する情報社会サービスを含まない;

…」

指令 2002/58

14 指令 2002/58 前文第 2 項、第 6 項、第 7 項、第 11 項、第 22 項、第 26 項及び第 30 項は以下の通り規定する:

「 (2) この指令は、基本的な権利の尊重を求めるものであり、特に[憲章]によって認められた諸原則に留意している。この指令は、とりわけ、同憲章の第 7 条及び第 8 条に定める権利を完全に尊重することの確保を求めている。

…

(6) インターネットは、広範な電子通信サービスを供給するための共通でグローバルなインフラを提供することによって、在来の市場構造を転覆している。インターネット上の公衆が利用可能な電子通信サービスは、その利用者に対して新たな可能性を拓くものでは

あるが、その個人データ及びプライバシーに対して新たなリスクをもたらすものでもある。

(7) 公衆通信ネットワークの場合においては、自然人の基本的権利及び自由並びに法人の正当な利益を保護するために、特に、自動的な記録保存並びに加入者及び利用者に関するデータの処理の能力が増大しつつあることに関して、特別の法令、規則及び技術基準が提供されなければならない。

…

(11) 指令[95/46]と同様に、この指令は、[EU]の法律によって規律されていない行為に関する基本的な権利及び自由の保護の問題に対応していない。それゆえ、個人のプライバシーの権利と、公共の保安、防衛、構成国の国内保安(その活動が構成国の国内保安上の事柄と関連するときは、構成国の経済発展を含む。)及び刑事法の執行のために必要となるこの指令の第 15 条(1)に示す措置を構成国が遂行する可能性との間の既存のバランスに対しては何らの変更も加えられない。その結果として、この指令は、これらの目的のいずれかのために必要があり、かつ、欧州人権裁判所の判決によって解釈される[1950 年 11 月 4 日にローマで署名された]人権及び基本的自由の保護に関する欧州条約に従う場合には、電子通信の適法な傍受その他の措置を遂行するための構成国の権限に影響を与えることはない。そのような構成国の措置は、民主的な社会の中において、適切であり、その目的と厳格に比例するものであり、かつ、必要なものであることを要し、かつ、人権及び基本的自由の保護に関する欧州条約に従い、適切な安全性確保措置が講じられるべきである。

…

(22) 利用者以外の者によって、又は利用者の同意なくなされる通信及び関連するトラフィックデータの記録保存の禁止は、それが電子通信ネットワーク内での通信の遂行の目的によってのみなされるものである限り、その情報の自動的に中間的な処理としてなされる一時的な記録保存を禁止しようとするものではないが、ただし、その情報は、送受信及びトラフィック管理のために必要な期間を超えて記録保存されてはならず、かつ、記録保存されている期間内は、その機密性が保障され続けなければならない。公衆が利用可能な情報を、その受信者の求めに応じて、そのサービスの他の受信者に対して送信することをより効果的なものとする必要があるときは、この指令は、そのような情報がさらに記録保存されることを妨げるものではないが、ただし、その情報は、いかなる場合においても、制限なく公衆からアクセス可能であることを要し、かつ、そのような情報を求める個々の加入者又は利用者を示すデータは消去されなければならない。

…

(26) 電子通信ネットワーク内で接続を確立し、情報を送信するために処理される加入者と関連するデータには、自然人の私生活に関する情報が含まれ、その通信を尊重する権利に関連し、法人の正当な利益と関連する。そのようなデータは、課金もしくは相互接続料金支払請求の目的でのサービスの提供のために必要な範囲内で、かつ、時間を限定してなされる場合においてのみ、記録保存され得る。そのようなデータを別の目的で処理することは、…そのプロバイダが遂行しようとしている別の目的による処理のタイプ、そのような処理について加入者が同意を拒否する権利及び彼又は彼女の同意を撤回することのできる権利について、当該公衆が利用可能な電子通信サービスのプロバイダから、正確かつ完全な情報が加入者に対して提供されていることを前提とした上で、当該加入者がその処理について同意している場合においてのみ、認められる。電子通信サービスのマーケティング…のために用いられるトラフィックデータは、そのサービスの提供が終了した後は、消去され、又は、匿名化されなければならない…。

…

(30) 電子通信ネットワーク及びサービスの提供に用いられるシステムは、必要な個人データの処理を厳格にミニマムなものとして制限するように設計されなければならない。…」

15 「適用範囲及び目的」と題する指令 2002/58 第 1 条は、以下の通り規定する:

「1. この指令は、電子通信分野における個人データの処理と関連する基本的権利及び自由、とりわけプライバシーの権利の均一なレベルでの保護を確保し、かつ、[欧州連合]の中におけるそのようなデータの支障の無い移転及び電子通信機器類とサービスの支障の無い移転を確保すべきことが求められる構成国の法令を、整合性のとれたものとする。

2. この指令にある条項は、第 1 項で示した目的のために、指令[95/46] の特則を定め、これを補完する。更に、この指令にある条項は、法人である加入者の正当な利益の保護を提供する。

3. この指令は、欧州連合条約の第 5 款及び 6 款が適用されるような[TFEU]の適用範囲外の活動には適用されない。又、公共の保安、防衛、構成国の保安(その活動が構成国の保安上の事柄と関連するときは、構成国の経済発展を含む。)及び刑事法の分野に属する構成国の活動にも適用されない。」

16 「定義」と題する指令 2002/58 第 2 条によると:

「他に定めがある場合を除き、指令[95/46] 及び指令[2002/21]にある定義が適用される。

又、以下の定義も適用される:

(a) 「利用者」とは、私的な目的又は業務上の目的で、当該サービスへの加入を必要とせずに、公衆が利用可能な電子通信サービスを利用する自然人を意味する;

(b) 「トラフィックデータ」とは、電子通信ネットワークにおいて通信を搬送する目的で処理されるデータ、又は、その課金のために処理されるデータを意味する;

(c) 「位置データ」とは、電子通信ネットワークで処理され、公衆が利用可能な電子通信サービスの利用者の端末機器の地理的位置を示すデータを意味する;

(d) 「通信」とは、公衆が利用可能な電子通信サービスによって、一定数の当事者間で情報を交換し又はそれを搬送することを意味する。これは、その情報を受信する識別可能な加入者又は利用者と関連させることのできる情報である場合を除き、電子通信ネットワーク上で公衆に対して提供される放送サービスの一部として搬送される情報を含まない;

…」

17 「関連するサービス」と題する当該指令の第 3 条は、以下の通り規定する:

「この指令は、個人データの収集及び個人識別の仕組みを有する公衆通信ネットワークを含め、共同体の公衆通信ネットワーク内の公衆が利用可能な電子通信サービスの提供と関連する個人データの処理に適用される。」

18 「通信の機密性」と題する指令 2002/58 第 5 条上:

「1. 構成国は、自国の立法を通じて、公衆通信ネットワーク及び公衆が利用可能な電子通信サービス通信による通信及びトラフィックデータの機密性を確保しなければならない。構成国は、第 15 条(1)に従い適法な権限に基づいてなされるものを除き、とりわけ、利用者以外の者により利用者の同意なくなされる通信及び関連するトラフィックデータの聴取、盗聴、記録保存その他の傍受行為又は監視行為を禁止しなければならない。本項は、機密性の原則を妨げることなく、通信の搬送のために必要な技術上の記録保存を妨げるものではない。

…

3. 構成国は、関連する加入者及び利用者に対して、就中、処理の目的に関して、指令[95/46]に従い、明瞭で理解しやすい情報が提供された上で、関係する加入者又は利用者が彼もしくは彼女の同意を与えている場合においてのみ、当該加入者又は利用者の端末機器に情報を記録保存し、又は、そこに既に記録保存されている情報へアクセスすることができることを確保しなければならない。このことは、電子通信ネットワーク上での通信の送信を遂行する目的のみでなされる場合、又は、加入者又は利用者から明示で求められた情報社会サービスの

プロバイダがサービスを提供するために必須のものである場合には、技術的な記録保存又はアクセスを妨げるものではない。」

19 「トラフィックデータ」と題する指令 2002/58 第 6 条は以下の通り規定する:

1. 公衆通信ネットワーク又は公衆が利用可能な電子通信サービスのプロバイダによって処理もしくは記録保存された加入者及び利用者に関するトラフィックデータは、通信の送信の目的のために不必要となった場合には、本条の第 2 項、第 3 項及び第 5 項並びに第 15 条(1)を妨げることなく、消去され、又は、匿名化されなければならない。

2. 加入者への課金及び相互接続料金支払請求のために必要なトラフィックデータは、これを処理することができる。課金について適法に検討することのできる期間又は支払の請求がなされている期間の最終日までは、そのような処理をすることが許される。

3. マーケティングの電子通信サービスの目的又は付加価値サービスの提供の目的のためには、公衆が利用可能な電子通信サービスのプロバイダは、当該データと関連する加入者又は利用者が彼もしくは彼女の事前の同意を提供している限り、そのようなサービス又はマーケティングのために必要な範囲及び期間内で、第 1 項に示すデータを処理することができる。利用者又は加入者は、トラフィックデータの処理に対して与えた同意をいつでも撤回する可能性を与えられなければならない。

…

5. 第 1 項、第 2 項、第 3 項及び第 4 項に従ってなされるトラフィックデータの処理は、公衆通信ネットワーク及び公衆が利用可能な通信サービスのプロバイダの課金、トラフィック管理、顧客対応、詐欺の検出、通信サービスのマーケティング又は付加価値サービスの提供を取扱う権限に基づいて活動する者に限定されなければならず、又、そのような活動の目的のために必要な範囲内に限定されなければならない。」

…」

20 「トラフィックデータ以外の位置データ」と題する当該指令第 9 条はその第 1 項において以下の通り規定する:

「1. トラフィックデータ以外の位置データが処理され得る場合、そのようなデータは、それらが匿名化されている場合、又は付加価値サービスの提供のために必要な範囲内及びその期間内で、利用者又は加入者の同意がある場合に限り、これを処理することができる。そのサービスプロバイダは、利用者又は加入者に対し、その同意を得る以前に、処理されることになるトラフィックデータ以外の位置データのタイプ、処理の目的及び期間、並びに、付加価

値サービスの提供の目的のために当該データが第三者に移転されるか否かについて、通知しなければならない。…」

21 「指令[95/46]の条項の適用」と題する当該指令第 15 条は、以下の通り規定する:

「1. 構成国は、当該制限が、指令[95/46]の第 13 条(1)に示すような自国の保安の防護(すなわち EU 構成国の保安)、防衛、公共の保安、犯罪行為又は電子通信システムの無権限使用の防止、捜査、検知及び訴追のために必要、適切、かつ、民主的な社会の中において比例的な措置となる場合には、この指令の第 5 条、第 6 条、第 8 条(1)、(2)、(3)及び(4)並びに第 9 条に規定する権利及び義務の範囲を制限するための立法的措置を採択することができる。この目的のために、構成国は、就中、本項に定める根拠に基づき限定された期間内だけ正当化されるデータの保持について定める立法上の措置を講ずることができる。本項に示す全ての措置は、欧州連合条約第 6 条(1)及び(2)に示すものを含め、[EU]法の基本原則に従うものでなければならない。

…

2. 指令[95/46]の司法救済、責任及び制裁に関する第 3 章の条項は、この指令により採択される自国の法令との関連において、又、この指令から派生する個人の権利の尊重との関連において、適用されなければならない。

…」

規則/2016/679

22 規則 2016/679 前文 10 は以下の通り規定する:

「(10) 一貫性があり高いレベルの自然人の保護を確保するため、そして、欧州連合内における個人データの流れの障碍を除去するために、そのデータの処理と関連する自然人の権利及び自由の保護のレベルは、全ての構成国において均等でなければならない。欧州連合全域において、個人データ処理と関連する自然人の基本的な権利及び自由の保護のための法令の一貫性があり均質な適用が確保されなければならない。…」

23 規則 2016/679 第 2 条は以下の通り規定する:

「1. この規則は、その全部又は一部が自動的な手段による個人データの処理に対し、並びに、自動的な手段以外の方法による個人データの処理であって、ファイリングシステムの一部を構成するもの、又は、ファイリングシステムの一部として構成することが予定されているものに対し、適用される。

2. この規則は、以下の個人データの処理には適用されない:

(a) 欧州連合の法律の適用範囲外にある活動の過程で行われる場合;

(b) 構成国によって欧州連合条約第 5 款第 2 章の適用範囲内にある活動が行われる場合;

…

(d) 公共の保安に対する防護及びその脅威の防止を含め、職務権限を有する機関によって犯罪行為の防止、捜査、検知もしくは訴追又は刑罰の執行のために行われる場合。

…

4. 本規則は、指令[2000/31]の適用、とりわけ、同指令の第 12 条ないし第 15 条にある中間介在サービスプロバイダの法的責任に関する規定の適用を妨げない。」

24 当該規則第 4 条は以下の通り規定する:

「この規則の目的のために:

(1) 「個人データ」とは、識別された自然人又は識別可能な自然人(「データ主体」)に関する情報を意味し; 識別可能な自然人とは、とりわけ、氏名、識別番号、位置データ、オンライン識別子のような識別子を参照することによって、又は、当該自然人の肉体的、生理的、遺伝的、精神的、経済的、文化的又は社会的な同一性を示す又は複数の要素を参照することによって、直接的又は間接的に、識別され得る者のことであり;

(2) 「処理」とは、それが自動的な手段によって行われるか否かを問わず、収集、記録、編集、構成、記録保存、修正もしくは変更、検索、参照、使用、送信による開示、配布又は、それら以外に利用可能なものとすること、整列もしくは結合、制限、消去又は破壊のような、個人データもしくは一群の個人データに実施される業務又は一群の業務のことを意味する;

…」

25 規則 2016/679 第 5 条は以下の通り規定する:

「1. 個人データは:

(a) そのデータ主体との関係において、適法であり、公正であり、かつ、透明性のある態様で処理され(「適法性、公正性及び透明性」);

(b) 特定され、明示であり、かつ、正当な目的のために収集されるものとし、かつ、その目的に適合しない態様で別の目的のために処理してはならず;公共の利益におけるアーカ

イブの目的、科学調査もしくは歴史調査の目的又は統計の目的のために行われる別の目的による処理は、第 89 条第 1 項に従い、当初の目的と適合しないものとはみなされず(「目的の限定」);

(c) その個人データが処理される目的との関係において、十分であり、関連性があり、かつ、必要のあるものに限定され(「データのミニマム化」);

(d) 正確であり、かつ、それが必要な場合、最新の状態に維持され;その個人データが処理される目的を考慮した上で、遅滞なく、不正確な個人データが削除又は訂正されることを確保するための全ての手立てが講じられなければならず(「正確性」);

(e) その個人データが処理される目的のために必要な期間だけ、データ主体の識別を許容する方式が維持され;データ主体の権利及び自由の安全性を確保するために本規則によって求められる適切な技術上及び組織上の措置の実装の下で、第 89 条第 1 項に従い、公共の利益におけるアーカイブの目的、科学調査もしくは歴史調査の目的又は統計の目的のみのために処理される個人データである限り、その個人データをより長い期間で記録保存でき(「記録保存の制限」);

(f) 無権限による処理もしくは違法な処理に対して、並びに、事故による喪失、破壊又は加害に対して、適切な技術上又は組織上の措置を用いて行われる防護を含め、個人データの適切な安全性を確保する態様により、処理される(「完全性及び機密性」)。

…」

26 当該規則第 6 条は以下の通り規定する:

「1. 処理は、以下の少なくとも 1 又は複数が適用される場合においてのみ、その範囲内で、適法である:

…

(c) 管理者が服する法的義務を遵守するために処理が必要となる場合;

…

3. 第 1 項の(c)及び(e)に示す処理のための根拠は、以下によって定められる:

(a) 欧州連合法;又は、

(b) 管理者が服する構成国法。

処理の目的は、その法的根拠に従って決定され、…その法的根拠は、本規則の規定の適用を

調整するための特別の条項、就中:管理者による処理の適法性を規律する一般的な条件; 処理の対象となるデータの種類; 関係するデータ主体;個人データが開示され得る組織及びその目的;目的の限定;記録保存期間; 並びに、第 9 章中に定めるその他の特別の処理の状況のための措置のような適法かつ公正な処理を確保するための措置を含め、処理業務及び処理手続を含めることができる。欧州連合法又は構成国法は、公共の利益の目的に適合するものであり、かつ、その求める正当な目的と比例的なものとする。

…」

27 当該規則第 23 条は以下の通り規定する:

「1. データの管理者もしくは処理者が服する欧州連合の法律又は構成国の法律は、その制限が基本的な権利及び自由の本質的部分を尊重するものであり、かつ、以下の対象を防護するために民主主義社会において必要かつ比例的な措置である場合には、第 12 条ないし第 22 条に定める権利及び義務にそれらの法律の条項が対応する範囲内で、立法措置によって、第 12 条ないし第 22 条及び第 34 条並びに第 5 条に定める義務及び権利の適用範囲を制限することができる:

(a) 国家保安;

(b) 防衛;

(c) 公共の保安;

(d) 公共の保安への脅威に対する防護及びその防止を含め、犯罪行為の防止、捜査、検知もしくは訴追又は刑罰の執行;

(e) 欧州連合又は構成国の一般的な公共の利益の上記以外の重要な対象、とりわけ、出納、予算及び税務上の事項を含め、欧州連合又は構成国の重要な経済的な利益もしくは財政上の利益、公衆衛生及び社会保障;

(f) 司法権の独立の保護及び司法手続の保護;

(g) 規制を受ける職種における違背行為の防止、捜査、検知及び訴追;

(h) (a)ないし(e)及び(g)に示す場合において、一時的なものを含め、公的な権限の行使と関係する監視、監督及び規制の権能;

(i) データ主体の保護、又は、それ以外の者の権利及び自由の保護;

(j) 民事訴訟の執行確保。

2. とりわけ、第 1 項に示す立法措置は、それが適切なときは、以下の事項に関する特別の条項を含める:

(a) 処理の目的又は処理の類型;

(b) 個人データの類型;

(c) 導入される制限の適用範囲;

(d) 非違行為又は違法なアクセスもしくは違法な移転を防止するための安全性確保措置;

(e) 管理者又は管理者の類型の指定;

(f) 処理又は処理の類型の性質、範囲及び目的を考慮に入れた記録保存期間及び適用可能な安全性確保措置;

(g) データ主体の権利及び自由に対するリスク;並びに、

(h) その権利がその制限の目的を妨げ得るものでない限り、その制限に関する情報提供を受けるデータ主体の権利。」

28 当該規則第 79 条(1)上:

「第 77 条により監督機関に異議を申立てる権利を含め、利用可能な行政上の救済又は裁判外の救済を妨げることなく、個々のデータ主体は、彼もしくは彼女が、本規則を遵守せずに彼もしくは彼女の個人データ処理がなされた結果として本規則に基づく彼もしくは彼女の権利が侵害されたと判断するときは、効果的な司法救済の権利をもつ。」

29 規則 2016/679 第 94 条は以下の通り規定する:

「1. 指令[95/46] は、2018 年 5 月 25 日から効力を生ずるものとして、廃止される。

2. 廃止される指令への参照は、この規則への参照として解釈される。指令[95/46]の第 29 条によって設置された個人データ処理と関連する個人の保護に関する作業部会に対する参照は、本規則によって設置される欧州データ保護委員会への参照として解釈される。」

30 当該規則第 95 条は以下の通り規定する:

「本規則は、欧州連合内にある公衆通信ネットワークにおける公衆が利用可能な電子通信サービスの提供と関連する処理と関係する自然人又は法人に対し、指令[2002/58] の中で同じ目的で定められ、彼らが特別な義務として服する事柄に加え、付加的な義務を課すものではない。」

フランス法

国内保安法典

31 国内保安法典[25]（「CSI」）立法部第 8 巻では、L. 801-1 条から L. 898-1 条までの条文で、諜報に関する規則を規定している。

32 CSI 第 L. 811-3 条は以下の通り規定する:

「専門的諜報機関は、それぞれの任務を遂行することを唯一の目的として、以下の基本的な国家の利益の防護と促進に関連する諜報[26]を収集するために、本巻第 V 款に示されている技術を用いることができる:

1. 国家の独立、領土の保全、国防;
2. 主要な外交政策上の利益、フランスの欧州及び国際的な公約の遂行、及びあらゆる形態の外国からの干渉の防止:
3. フランスの主要な経済、産業、科学的利益;
4. テロリズムの防止;
5. 以下の防止:
   (a) 共和政体に対する攻撃;
   (b) 第 L. 212-1 条に従って解散した集団の維持又は再結成を目的とした行為;
   (c) 法と秩序の維持を著しく損なうおそれのある集団的な暴力;
6. 組織犯罪の防止;
7. 大量破壊兵器の拡散の防止。」

33 CSI 第 L. 811-4 条は以下の通り規定する:

「諜報技術監督委員会[27]の意見を受けて国務院により採択された布告[28]は、本巻第 V 款にい

[25] Code de la sécurité intérieure
[26] 仏語では renseignement
[27] Commission nationale de contrôle des techniques de renseignement
[28] décret en Conseil d'Etat. 国務院デクレ。

う技術を本巻に規定されている条件の下で使用することが許可される国防大臣、内務大臣、司法大臣、経済担当大臣、予算担当大臣、税関担当大臣の権限下にある専門的諜報機関以外の機関を指定する。それは機関毎に第 L. 811-3 条に記載されている目的と、許可され得る技術を特定する。」

34 CSI 第 L. 821-1 条[29]第 1 項は以下の通り規定する:

「本巻第 V 款第 I 章から第 IV 章までに記載されている諜報収集技術の国家領域内での実施は、諜報技術監督委員会の意見徴収を受けた後の首相による事前許可を条件とする。」

35 CSI の第 L. 821-2 条は以下の通り規定する。

「第 L. 821-1 条で言及された許可は、国防大臣、内務大臣、法務大臣、又は経済活動、予算若しくは関税を担当する大臣からの書面による理由のある申請に基づいて発行される。各大臣は、国防機密を取り扱う資格を持つ直属の部下にのみ、この権限を個別に委任することができる。

申請は以下を記さなければならない。

1. 実施する技術;
2. 申請対象となる職務;
3. 追求される目的;
4. 対策を講じる理由;
5. 許諾の有効期間;
6. 関係する人物、場所又は車両

第 6 号の適用については、身元がわからない人物は、その識別子又はその地位によって指定することができ、場所又は車両は、申請の対象者を参照して指定することができる。

…」

36 CSI 第 L. 821-3 条第 1 項上:

---

[29] LOI n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement (テロリズム行為の防止及び諜報に関する 2021 年 7 月 30 日の法律第 2021-998 号以下「法律第 2021-998 号」)第 18 条により改正

「申請は、諜報技術監督委員会議長に送付され、それができないときは、第 L. 831-1 条の第 2 号及び第 3 号に記載されている同委員会の委員の 1 人に送付され、議長又はその委員は 24 時間以内に首相に意見を述べる。申請が委員会の分科会又は全体会で審査される場合は、首相に遅滞なく報告され、72 時間以内に意見が出される。」

37 CSI 第 L. 821-4 条は以下の通り規定する:

「本巻第 V 款の第 I 章から第 IV 章までに言及されている技術を実施するための許可は、首相によって有効期間を最長 4 ヶ月として発行される。…許可には、第 L. 821-2 条の第 1 号から第 6 号に規定された理由及び記載内容が含まれなければならない。いかなる許可も、本章に規定された条件と同じ条件で更新可能である。

諜報技術監督委員会からの不賛成の意見の後に許可が発行された場合は、その意見に従わなかった理由を記載しなければならない。

…」

38 第 III 款第 III 章にある CSI 第 L. 833-4 条は、以下の通り規定する:

「委員会は、— 自らの発意により、あるいは諜報技術が彼又は彼女に対して違法に実施されていないことを確認したい者から苦情申立てを受けた場合には、— 本巻に従って、実施されているか、又はこれから実施されようとしているかどうかを認定する目的で、言及された技術又は技術群の検査を実施する。委員会は、必要な調査が行われたことを、その使用の有無を確認することも否定することもなく、苦情申立人に通知しなければならない。

39 CSI 第 L. 841-1 条の第 1 項及び第 2 項は以下の通り規定する:

「本法典第 L. 854-9 条の特別な規定に従うことを条件として、国務院は、行政裁判法典[30]第 7 巻第 VII 款第 III 章の 2 に規定された条件の下で、本巻第 V 款に記載された諜報技術の実施に関する訴訟を審理する管轄を有する。

以下の者は、国務院に対して訴訟を提起できる:

1. 彼又は彼女に対して諜報技術が違法に実施されていないことの確認を希望する者で、第 L. 833-4 条に規定されている手続きを事前に実施したことを証明できる者;

2. 第 L. 833-8 条に規定された条件の下、諜報技術監督委員会。」

40 「許可を要する諜報収集技術」に関する CSI 立法部第 8 巻第 V 款は、就中、CSI 第 L. 851-1

[30] code de justice administrative

条から第 L. 851-7 条が含まれる「接続データへの行政当局によるアクセス」と題された第 I 章が含まれる。

41 CSI 第 L. 851-1 条は以下の通り規定する:

「本巻第 II 款第 I 章に規定されている条件にしたがい、電子通信事業者及び[CPCE]の L. 34-1 条に記載されている者，及び、デジタル経済の信頼性に関する 2004 年 6 月 21 日の法律第 2004-575 号[31][(2004 年 6 月 22 日の JORF p. 11168)]の第 6 条(I)(1)及び(2)に示す者から，それらのネットワーク又は電子通信サービスによって処理又は保持された、電子通信サービスへの加入者番号若しくは接続番号、特定された者の加入者番号又は接続番号の全履歴、使用された端末機器の位置、並びに加入者の通信、すなわち起呼番号、着呼番号、通信時間及び日のリストの技術的データを含む情報又は文書の収集を行うことの許可を得ることができる。

第 L. 821-2 条の逸脱として、電子通信サービスへの加入識別子若しくは接続番号又は特定された者のすべての加入者番号若しくは接続番号の全履歴に関する技術的データに関する書面による理由のある申請は、第 L. 811-2 条及び第 L. 811-4 条に記載された諜報機関の個別に指定され授権された担当官によって、諜報技術監督委員会に直接送付される。委員会は、第 L. 821-3 条に規定された条件で意見を述べる。

首相の部局は、本条第 1 項に記載された事業者及び人物から情報又は文書を収集する責任を負う。諜報技術監督委員会は、収集された情報又は文書への恒久的で完全な直接かつ即時のアクセス権を持つ。

本条の適用の詳細な規則は、データ保護委員会[32]及び諜報技術監督委員会との協議を経て、国務院の採択する布告によって定められる。」

42 CSI 第 L. 851-2 条[33]は以下の通り規定する:

「I. 本巻第 II 款第 I 章に記載された条件の下で、テロを防止する目的に限って、第 L. 851-1 条に記載された事業者及び者のネットワーク上で、脅威への結びつきを有する可能性があるとして事前に特定された者に関する同条に記載された情報又は文書のリアルタイムによる収集が個別に許可され得る。許可に関係する者の人脈に属する 1 以上の者が、許可を受けた目的のために情報を提供する可能性があると信じる重大な理由がある場合、許可はこれらの人物にも、それぞれ個別に付与することもできる。

---

31 Loi n.° 2004-575 du 21 juin 2004 pour la confiance dans l’économie numérique

32 Commission nationale de l’informatique et des libertés

33 法律第 2021-998 号第 16 条及び第 18 条により改正。

I の 1. 本条に基づいて発行された許可のうち、一度に有効な最大数は、諜報技術監督委員会と協議の上、首相が決定する。この割当量を設定する決定と、第 L. 821-2 条第 1 項に記載された閣僚にどのように分配されるかは、発行された傍受許可の数とともに、委員会に送付される。

…」

43 CSI 第 L. 851-3 条[34]は以下の通り規定する:

「 I. - 本巻第 II 款第 I 章に記載されている条件の下で、テロリズムを防止することを唯一の目的として、第 L. 851-1 条に記載されている事業者及び者は、許可で指定されたパラメータに従って、テロリストの脅威を構成する可能性のある繋がりを検出するために設計された自動化されたデータ処理操作を、そのネットワーク上に実装することを命ぜられ得る。

このような自動化された処理は、第 L. 851-1 条に記載された情報又は文書を排他的に使用し、その設計されたパラメータを満たす以外のデータを収集せず、情報又は文書に関連する人物の特定識別を許容してはならない。

比例性の原則にしたがい、首相の許可は当該処理操作の実装の技術的範囲を特定するものとする。

II. 諜報技術監督委員会は、自動化された処理の許可申請と選択された検出用パラメータについて意見を出す。委員会はこのような処理操作や収集された情報及びデータに対して、恒久的かつ完全な直接アクセスを持つ。処理操作やパラメータへのいかなる変更も委員会に報告され、委員会は勧告を出せる。

本条第 I 項に規定された自動化された処理操作を実施するための最初の許可は、2 ヶ月間有効とする。この許可は、本巻第 II 款第 1 章に記載されている期間の条件の下で更新可能とする。更新申請には、自動化された処理によってフラグを立てられた識別子の数の記録と、これらのフラグ立ての関連性に関する分析結果を含める。

III. 第 L. 871-6 条に定められた条件は、第 L. 851-1 条に記載された事業者及び人物がそのような処理を実行する目的のために行う物理的操作に適用される。

IV. 本条第 I 項に記された処理操作により、テロリストの脅威の存在を指し示す可能性のあるデータが検出された場合、首相又はその委任を受けた者は、― 本巻第 II 款第 1 章に規定された条件の下で与えられた諜報技術監督委員会の意見を得た後 ― 関係者の特定及び関連

[34] 法律第 2021-998 号第 15 条(V)及び第 18 条により改正。

データの収集を行うことを許可できる。そのデータは、1 人又は複数の関係者に関連してテロの脅威が存在することを確認する実質的な理由がない限り、収集後 60 日以内に使用され、この期間が経過すると破棄される。

…」

44 CSI 第 L. 851-4 条は以下の通り規定する:

「本巻第 II 款第 1 章に記載された条件の下で、第 L. 851-1 条に記された使用される端末機器の位置に関する技術的データは、要求により、事業者がネットワークから収集し、リアルタイムで首相部局に送信され得る。」

45 本法典の規則部に掲載されている CSI 第 R. 851-5 条は、次のように規定する:

「I. 第 L. 851-1 条に記載された情報又は文書は、―交信又は照会された情報の内容を除いて― 以下のとおり:

1. [CPCE]第 R.10-13 条、第 R.10-14 条及び布告[第 2011-219 号]第 1 条に記載されているもの。

2. 第 1 号に記載されている以外の技術的データであって:

(a) 端末機器の位置を把握可能にするもの;

(b) オンライン公衆通信のネットワーク又はサービスへの端末機器のアクセスに関するもの;

(c) ネットワークによる電子通信の搬送[35]に関するもの;

(d) 利用者、接続、ネットワーク又はオンライン公衆通信サービスの識別及び認証に関するもの;

(e) 端末機器の特性及びそのソフトウェアの設定データに関するもの。

II. 第 I 項(1)に記載された情報及び文書のみ、第 L. 851-1 条に従って収集できる。この収集は非リアルタイムで行われる。

第 I 項(2)に記載された情報は、第 L. 851-2 条及び第 L. 851-3 条に基づき、これらの条文に規定された条件及び制限の下でのみ、第 R. 851-9 条が適用された上で、収集できる。

---

[35] 英文版 conveyance 仏文原文は l`acheminement

CPCE

46 CPCE の第 L. 34-1 条[36]は以下の通り規定する:

「I. 本条は、公衆への電子通信サービスの提供に際する個人データの処理に適用される; 特にデータの収集及び識別装置をサポートするネットワークに適用される。

II. 電子通信事業者、特にオンライン公衆通信サービスへのアクセスを提供する事業を行っている者は、第 III 項、第 IV 項、第 V 項及び第 VI 項の規定を停止条件として、トラフィックに関するいかなるデータも消去又は匿名化しなければならない。

公衆に電子通信サービスを提供する者は、前副項の規定を考慮した上で、職務権限を有する当局からの要求に応えるための内部手続きを確立しなければならない。

主たる又は補助的な事業活動の一環として、ネットワークへのアクセスを経由したオンライン通信を可能にする接続を、無料で提供される場合も含み、公衆に提供する者は、本条に基づき電子通信事業者に適用される規定を遵守する。

III. 犯罪若しくは知的財産法典[37]第 L. 336-3 条で定義された義務の違反を捜査、検知及び起訴するため、又は刑法典[38]第 323-1 条から第 323-3-1 条で規定され、処罰され得る自動化されたデータ処理システムの侵害を防止するため、並びに、必要に応じて法務当局若しくは知的財産法第 L. 331-12 条に記載されている高等機関、又は防衛法典[39]の L. 2321-1 条に記載されている情報システムセキュリティの国家機関への情報提供を可能にすることを唯一の目的として、特定のカテゴリーの技術データを削除又は匿名化するよう設計された作業は、最大 1 年間延期することができる。データ保護監督機関との協議の後に採択される国務院の布告は、第 VI 項に定められた制限の範囲内で、事業者の事業と通信の性質に応じて、これらの関連するデータのカテゴリーと保持期間、並びに国の要求に応じてこれらの目的で事業者が提供したサービスの識別可能かつ特定の追加費用に対する補償方法を決定[40]する。

---

36 法律第 2021-998 号第 17 条により改正されている。

37 code de la propriété intellectuelle

38 Code pénal

39 code de la défense

40 後掲 CPCE 第 R. 10-13 条が国務院布告により制定(Decree No. 2006-358 of March 24, 2006 on the retention of electronic communications data)され、改正(Decree No. 2012-436 of March 30, 2012 transposing the new European regulatory framework for electronic communications)されてい

…

VI. 第 III 項、第 IV 項、第 V 項に規定された条件で保持され処理されるデータは、専ら、事業者が提供するサービスを利用する者の識別特定、事業者が提供する通信の技術的特性及び端末機器の位置に関連する。

いかなる状況においても、そのようなデータを、これらの通信の一部として交信内容や照会された情報に、いかなる形態であろうとも、関連させてはならない。

当該データの保持及び処理は、情報処理装置、ファイル及び自由に関する 1978 年 1 月 6 日の法律第 78-17 号[41]の規定に従って行われる。

事業者は、当該データが本条に定める目的以外に使用されることを防止するためにあらゆる手段を講じる。」

47 CPCE 第 R. 10-13 条[42]は以下の通り規定する:

「I. 第 L. 34-1 条第 III 項に基づき、電子通信事業者は、刑事犯罪の捜査、検知、訴追を目的として、以下を保持する:

(a) 利用者を識別する情報;

(b) 使用する通信端末機器に関するデータ;

(c) 各通信の技術的特徴並びに日、時及び長さ;

(d) 要求又は使用された追加サービス及びその提供者に関するデータ;

(e) 通信の宛先を識別するデータ。

II. 電話事業については、事業者は、第 II[43]項で言及されたデータに加えて、通信の発信元及

る。

41 Loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

42 Décret n° 2021-1361 du 20 octobre 2021 relatif aux catégories de données conservées par les opérateurs de communications électroniques, pris en application de l'article L. 34-1 du code des postes et des communications électroniques（「布告第 2021-1361 号」）第 3 条及び第 4 条により改正されている。

43 本来第 I 項。判決フランス語原文も、legifrance(フランス法サイト)も II となっているが、前回改正時からの誤りと思われる。

び場所を識別特定できるデータを保持しなければならない。

III. 本条に記載されたデータは、記録された日から 1 年間保持される。

IV. 本条に記載されたカテゴリーのデータを提供するよう司法当局から要求された事業者が被った識別可能かつ具体的な追加費用は、刑事訴訟法典第 R.213-1 条に定められた手続きに従って補償される。」

48 CPCE 第 R.10-14 条[44]は、以下の通り規定する:

「I. 第 L. 34-1 条第 IV 項に従い、電子通信事業者は、課金・決済業務の目的で、利用者の識別を可能にする技術的データ及び第 R. 10-13 条(I)(b)、(c)及び (d)に記されたデータを保持することが許される。

II. 電話事業については、事業者は、I に記載されたデータに加えて、通信の場所及び通信の宛先の識別特定に関する技術的データ及び請求目的のデータを保持できる。

III. 本条の第 I 項及び第 II 項に記載されたデータは、提供されたサービスの請求及び決済に必要な場合にのみ保持できる。その保持は、この目的のために厳密に必要な期間に限定され、かつ 1 年を超えてはならない。

IV.- ネットワークや設備のセキュリティのために、事業者は 3 ヶ月を超えない期間、以下のデータを保持することができる。

(a) 通信の発信元を特定するデータ;

(b) 各通信の技術的特徴並びに日付、時間及び長さ;

(c) 通信の受信者を特定するための技術データ;

(d) 要求又は使用された追加サービス及びその提供者に関するデータ。」

デジタル経済の信頼性の促進に関する 2004 年 6 月 21 日の法律第 2004-575 号

49 デジタル経済の信頼性の促進に関する 2004 年 6 月 21 日の法律第 2004-575 号[45](2004 年 6 月

---

44 布告第 2021-1361 号により I 項が改正されている。

45 Loi no 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

22 日の JORF p.11168、以下「LCEN」)の第 6 条[46]は、以下の通り規定する:

「I. 1. その事業がオンライン公衆通信サービスへのアクセスを提供する者は、特定のサービスへのアクセスを制限したり、それらのサービスを選択したりする技術的手段の存在を加入者に知らせ、これらの手段のうち少なくとも 1 つを提供しなければならない。

…

2. 無償で提供されるものも含め、オンライン公衆通信サービスを経由した公衆への提供のために、サービスを受ける者から提供される様々な種類の信号、文章、画像音声、又はメッセージの記録保存をする自然人又は法人は、これらのサービスを受ける者の要求によりなされた行動又は記録保存された情報について、その違法な行動の性質又は問題の情報又はそれらの違法な性質を摘示する事実や状況の現実的認識を持っていなかった場合、又はそのような違法な性質に気付いた後すぐに問題のデータを削除するか、又はそれらへのアクセスをブロックするために迅速に行動した場合、民事上の責任を問われない。

…

II. 第 I 項(1)及び(2)に記載された者は、自らがプロバイダであるサービスのコンテンツの一部又は全部の作成に寄与した者[47]を識別特定できるデータを保管し、保持する。

彼らは、オンライン公衆通信サービスを公開する者[48]に対し、第 III 項で規定されている本人確認の条件を満たすことができる技術的手段を提供しなければならない。

司法当局は、第 I 項(1)及び(2)に記載されたサービスプロバイダに対して、第 1 パラグラフに記載されたデータの伝達を要求することができる。

このようなデータの処理には、刑法典第 226-17 条、第 226-21 条、第 226-22 条の規定が適用される。

データ保護監督官との協議を経て採択された国務院の布告は、第 1 副項に言及されたデータ

---

[46] 法律第 2021-998 号により改正されている。なお、さらに LOI n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République 等により改正されているが、本判決との関係はない。

[47] quiconque a contribué à la création du contenu ou de l'un des contenus. 日本のプロバイダ責任制限法の「発信者」相当の者。

[48] personnes qui éditent un service de communication au public.

を定義し、当該データが保持される期間及び方法を決定する。

…」

布告第 2011-219 号[49]

50 [LCEN]の第 6 条第 II 項最終副項に基づいて採択された布告第 2011-219 号第 I 章には、当該布告の第 1 条から第 4 条が含まれている。

51 布告 2011-219 号第 1 条は、以下の通り規定する:

「 [LCEN]第 6 条第 II 項に記載されており、当該規定の下、対象者が保持する義務があるデータは、以下のデータである:

1. 同条第 I 項(1)に記載されている者につき、かつ、その加入者の各接続に対して:

(a) 接続識別子;

(b) 対象者が加入者に割り当てた識別子;

(c) 接続に使用される端末の識別子で、対象者からアクセスできる場合;

(d) 接続の開始と終了の日付と時刻;

(e) 加入者回線の特徴。

2. 同条第 I 項(2)に記載されている者、及び各情報発信[50]につき:

(a) 通信を生じさせた接続の識別子;

(b) 情報システムが、情報発信対象となるコンテンツに割り当てる識別子;

(c) サービスへの接続やコンテンツの転送に使用されるプロトコルの種類;

(d) 情報発信の性質;

---

[49] 布告第 2011-219 号は、Décret n° 2021-1362 du 20 octobre 2021 relatif à la conservation des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, pris en application du II de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique(「布告第 2021-1362 号」) により全部廃止され、本布告が LCEN 第 6 条による委任立法として置き換わった。

[50] opération de création

(e) 情報発信を実行した日付と時刻;

(f) 情報発信者から提供された場合、情報発信者に用いられた識別子。

3. 同条第 I 項(1)及び(2)に記載された者については、利用者が契約を締結する際、又はアカウントを作成する際に提供される情報:

(a) アカウントの作成時の接続の識別子;

(b) 姓、名、又は会社名;

(c) 関連する郵便住所;

(d) 利用された仮名;

(e) 関連する電子メールやアカウントのアドレス;

(f) 電話番号;

(g) 最終更新のパスワード及びそれを確認・変更するためのデータ。

4. 同条第 I 項(1)及び(2)に記載された者については、契約又はアカウントへの加入が有償の場合、支払取引ごとに、支払に関する以下の情報:

(a) 使われている支払いの種類;

(b) 支払いの特定情報;

(c) 金額;

(d) 取引の日付と時刻。

第 3 号及び第 4 号に記載されたデータは、通常、人がそのようなデータを収集する範囲内でのみ保持される。」

52 当該布告第 2 条は以下の通り規定する:

「コンテンツ作成への寄与には、以下に関する行為が含まれる:

(a) コンテンツの初期作成;

(b) コンテンツ及びコンテンツに関連するデータの修正;

(c) コンテンツの削除。」

53 当該布告第 3 条は、以下の通り規定する:

「第 1 条に記載されたデータの保存期間は以下の日付から 1 年である:

(a) 第 1 項及び第 2 項に記載されたデータについては、第 2 条に定めるコンテンツの作成に寄与する各行為ごとにコンテンツの作成日;

(b) 第 3 項に記載されたデータについては、契約の終了又はアカウントの閉鎖の日;

(c) 第 4 項に記載のデータについては、請求又は支払取引ごとに、請求書発行日又は支払取引日」

ベルギー法

54 2016 年 5 月 29 日の法律は、とりわけ、電子通信に関する 2005 年 6 月 13 日の法律[51](2005 年 6 月 20 日のベルギー官報 28070 頁、「2005 年 6 月 13 日の法律」)、刑事訴訟法典[52]及び諜報及び保安機関に関する 1998 年 11 月 30 日の基本法[53](1998 年 12 月 18 日のベルギー官報 40312 頁、「1998 年 11 月 30 日の法律」)を改正した。

55 2016 年 5 月 29 日の法律により改正された 2005 年 6 月 13 日の法律の第 126 条は、以下の通り規定する:

「1. 個人データの処理に関するプライバシー保護に関する 1992 年 12 月 8 日の法律[54]を妨げることなく、インターネット経由を含む公衆への電話サービス、インターネットアクセス及びインターネット電子メールを提供するプロバイダ、公衆電子通信ネットワークを提供する事業者並びにこれらのサービスのいずれかを提供する事業者は、第 3 項に記載するデータを、関連する通信サービスの提供に際して当該データが彼らにより生成又は処理された場合、保持するものとする。

本条は、通信の内容については対象としない。

第 3 項で言及されたデータを保持する義務は、当該データが以下の場合、関連する当該通信

---

51 l loi du 13 juin 2005 relative aux communications électroniques

52 code d'instruction criminelle

53 loi du 30 novembre 1998 organique des services de renseignement et de sécurité

54 Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel

サービスの提供の際に、失敗した起呼にも適用される:

(1) 電話データに関する限り、公衆が利用可能な電子通信サービス又は公衆電子通信ネットワークの事業者によって生成又は処理されたものであること;

(2)インターネットデータに関しては、それらのプロバイダによって記録されたものであること。

2. 以下の当局のみが、簡易な要求により、本条に基づいて保持されたデータを、以下に示す目的及び条件で、第 1 項第 1 副項に記載されたプロバイダ及び事業者から入手することができる:

(1)犯罪の捜査、検知、訴追を目的として、刑事訴訟法典第 46 条の 2 及び第 88 条の 2 に記載されている措置を執行するために、かつこれらの条文で定められている条件の下で、法務当局;

(2) 諜報及び保安機関に関する 1998 年 11 月 30 日の基本法第 16/2 条、第 18/7 条及び第 18/8 条に記載されているデータ収集方法を用いて、本法に規定されている条件の下で、諜報任務を遂行するために、諜報及び保安機関;

(3) 第 114 条、第 124 条及び本条に反する犯罪の捜査、検知、訴追を目的とした、［ベルギー郵便・電気通信機関[55]］所属の法務警察員;

(4) 緊急通報を受けた際に、第 107 条(2)第 3 副項に記載されたデータベースを使用して、関係するプロバイダ又は事業者から緊急通報をした者を識別するデータが取得できなかった場合、又は不完全もしくは不正確なデータを取得した場合に、現場で支援を提供する緊急サービス。当該通報後 24 時間以内に、発信者を識別同定するデータのみを要求できる;

(5) 彼又は彼女が、危険にさらされている人物を支援するという任務に際して、失踪が心配される人を捜索しており、かつ行方不明者の身体的完全性が差し迫った危険にさらされているという重大な推定又は兆候がある場合の連邦警察の行方不明者ユニットの法務警察員。行方不明者に関する第 3 項第 1 副項及び第 2 副項に記載されたデータであって、データの要求に先立つ 48 時間の間に保持されたもののみを、国王が指定する警察機関を介して当該事業者又はプロバイダに要求できる;

(6) 特定の公共経済事業の改革に関する 1991 年 3 月 21 日の法律[56](「1991 年 3 月 21 日の法

[55] Institut belge des services postaux et des télécommunications
[56] loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques

律」)第 43 条の 2(3)(7)に規定された条件に従い、電子通信ネットワーク又はサービスを濫用した者を特定する目的での電気通信オンブズマン。本人識別同定データのみを要求できる。

第 1 項第 1 副項に記載されたプロバイダ及び事業者は、第 3 項に記載されたデータがベルギーから制限なくアクセス可能であること、及びこれらのデータ及びこれらのデータに関するその他の必要な情報が、本項に記載された当局にのみ遅滞なく送信可能であることを確保する。

他の法律の規定を妨げることなく、第 1 項第 1 副項に記載されたプロバイダ及び事業者は、第 3 項に従って保持されたデータを他の目的のために使用してはならない。

3. 利用者又は加入者及び通信手段を識別特定するために使用できるデータは、第 2 副項及び第 3 副項で特に規定されているデータを除き、使用されたサービスを用いて最後に通信が可能となった日から 12 ヶ月間保持される。

端末機器のネットワーク及びサービスへのアクセス及び接続、並びにネットワークの終点を含むその機器の位置に関するデータは、通信の日から 12 ヶ月間保持される。

発信元と発信先を含む内容以外の通信データは、通信が行われた日から 12 ヶ月間保存される。

国王は、法務大臣及び［電子通信に関する事項を所管する］大臣の提案に基づき、プライバシー保護委員会及び郵便・電気通信機関の意見を聴取した後に、閣僚会議で審議された布告により、第 1 副項から第 3 副項までに記載されたカテゴリーの種類別に保持されるデータ、及びこれらのデータが充足しなければならない要件を決定する。

…」

主手続の争点及び先決裁定のために照会された質問

Case C-511/18

56 La Quadrature du Net, French Data Network, the Fédération des fournisseurs d'accès à Internet associatifs 及び Igwan.net は、後に主手続で併合された 2015 年 11 月 30 日及び 2016 年 3 月 16 日に提出された申立てにより、国務院[57]に、布告第 2015-1185 号、第 2015-1211 号、第 2015-1639 号及

[57] Conseil d'État

び第 2016-67 号[58]が、就中、フランス憲法、人権の保護と基本的自由の欧州条約(「ECHR」)並びに、憲章第 7 条、第 8 条及び第 47 条に照らして読む指令 2000/31 及び指令 2002/58 に違反することを理由としてそれらの廃止を求める訴訟を提起した。

57 とりわけ、指令 2000/31 違反を主張する答弁については、照会元裁判所は、CSI 第 L. 851-3 条の条項は、電子通信事業者及び技術サービス提供者が「彼らのネットワークに、テロリストの脅威を構成するかも知れない繋がりを検出するために設計された、許可に規定されたパラメータの範囲内で、自動化されたデータ処理操作を実装すること」を義務づけると述べる。その技術はこの種の重大犯罪に関連するようなデータの、限定的な期間かつこれらの事業者やサービス提供者により処理されたすべての接続データからの、収集を促進することのみを意図している。そのような状況下で、そのような、能動的監視の網羅的義務を課さない条項は、照会元裁判所の考えでは、指令 2000/31 第 15 条に違反しない。

58 指令 2002/58 の違反を主張する答弁については、照会元裁判所は、就中、指令の条文及び 2016 年 12 月 21 日付 *Tele2 Sverige and Watson and Others* 判決(C-203/15 及び C-698/15 併合事件 EU:C:2016:970「*Tele2*」)からは、電子通信サービスのプロバイダに、当該指令第 15 条(1)に規定する、国家保安、防衛及び公共の保安の防護を含む目的で、彼らの利用者及び加入者のトラフィックデータ及び位置データの網羅的かつ無差別的な保持のような義務を課す構成国法は、これらのそれらのプロバイダの活動を統制するため、その指令の適用範囲に入ると考える。それは国内の当局によるデータへのアクセスとデータの利用を統制するルールについても適用される。

59 これから、照会元裁判所は CSI 第 L. 851-1 条によるデータを保持する義務並びにそのデータへの行政当局による及び第 L. 851-1 条、第 L. 851-2 条及び第 L. 851-4 条に規定する、リアルタイムアクセスを含むアクセスは、指令 2002/58 の適用範囲に入ると結論する。当該裁判所によると、網羅的な保持義務を関連する事業者に課すものではないものの、彼らに、彼らのネットワーク上、テロリストの脅威を構成するかも知れない繋がりを検出するために自動化された処理を実装することを義務づける CSI 第 851-3 条についても、同じことが言える。

60 一方、照会元裁判所は、指令 2002/58 の適用範囲は、構成国により直接適用された諜報収集技術に関するが、電子通信サービスのプロバイダの行動を、特定の義務を課すことによって規制しない、廃止申立てに言及された CSI の条項には拡張されないとの見解である。従って、それらの条項は EU 法を実装するものとして扱うことはできず、結果として、それらが指令

[58] 布告第 2015-1639 号及び第 2016-67 号は、主手続の 2021 年 4 月 21 日付判決 No. 393099 により、CSI の関連条項の実施に関して、独立した行政機関であってその決定に拘束力があるものまたは裁判所のいずれかによる、事前審査が無い限りにおいて廃止されている。

2002/58 に違反する旨を主張する答弁は、有効に依拠できない。

61 そこで、布告第 2015-1185 号, 第 2015-1211 号, 第 2015-1639 号及び第 2016-67 号が、CSI 第 L. 851-1 条から第 L. 851-4 条を実装するために採択された限りにおいて、それらの指令 2002/58 に照らした適法性に関する紛争を解決するためには、EU 法の解釈につき 3 つの疑問が生ずる。

62 第一に、指令 2002/58 第 15 条(1)の解釈については、照会元裁判所は、CSI 第 L. 851-1 条及び R. 851-5 条に基づき電子通信サービスのプロバイダに課された網羅的かつ無差別の保持義務が、就中、行政当局の接続データへのアクセス及びその利用が対象となる防護と確認措置に照らして、憲章第 6 条により保障された保安の権利、及び TEU 第 4 条により構成国にその責任が単独にある国家保安の要請により正当化される干渉であるとみなせるかどうか確信をえられない。

63 第二に、電子通信サービスのプロバイダに課され得るその他の義務については、照会元裁判所は、CSI 第 L. 851-2 条の条文は、テロリズムを防止する単一の目的で、当該法典第 L. 851-1 条に規定する情報又は文書の同じ者からの収集を許容すると述べる。そのような収集は、以前、テロリストの脅威との繋がりを潜在的に有すると特定された個人との関係においてのみ、リアルタイムで実行され得る。事業者からの、端末機器の位置に関連する技術的データに限定してリアルタイムの送信を許可する第 L. 851-4 条の条文についても、同じことが言える。それらの技術は CPCE 及び LCEN 上保持されたデータへの行政当局による様々な目的及び様々な手段によるリアルタイムアクセスも、しかしながら、関連するプロバイダに対して課金及び彼らのサービスの提供に必要な範囲を超える追加の保持義務を課すことなしに、規制する。同様に、サービスプロバイダに対して通信の分析のための自動化されたシステムをそのネットワーク上に実装することを義務づける CSI 第 L. 851-3 条の条文は、網羅的かつ無差別の保持を要しない。

64 照会元裁判所は、国家保安に対する重大かつ永続的な脅威、とりわけテロリストの脅威という背景において、網羅的かつ無差別の保持及び接続データに対するリアルタイムアクセスの双方は、比類の無い実務上の有用性を備えていると考える。網羅的かつ無差別の保持は、諜報機関が、関係する者が公共の保安、防衛又は構成国の保安への脅威をもたらすと信じる理由が特定される前に、通信データへのアクセスを得ることを可能にする。加えて、接続データへのリアルタイムアクセスにより公共の秩序に差迫った脅威をもたらす可能性のある個人の行動を、高レベルの即応性を伴い、監視することができるようになる、

65 さらには、CSI 第 L. 851-3 条に規定される技術により、その目的で特別に定義された基準に基づき、その行動が、彼らの通信の方法を考慮するとテロリストの脅威を構成するかもしれ

ない個人を検出することが可能になる。

66 第三に、職務権限を有する当局による保持されたデータへのアクセスについては、照会元裁判所は、憲章に照らし指令 2002/58 を読んだ場合に、接続データの収集手続の適法性には、データ主体が、通知されることによりもはや職務権限を有する当局により行われてきた捜査に支障を与える恐れがなくなり次第、知らされることが大前提であること、又はそのような手続は、その他すべての手続き的保障手段であって、そのような保障手段が救済を受ける権利が効果的であることを確保する場合に、それらを考慮すると適法として扱われることを意味すると解釈されるべきかどうか確信が持てない。

67 そのようなその他の手続的保障手段につき、照会元裁判所は、とりわけ、彼又は彼女に対して諜報技術が違法に利用されていないことを確認することを希望しているいかなる者も、―対審構造以外の手続により通知された情報に照らして ― 申立人が諜報技術の対象となってきたかどうか、及び当該技術が CSI 第 VIII 巻に従い利用されたかどうかを判断する責務を有する国務院の専門家委員会にその問題を申立てることができる、と述べる。当該委員会に授権された申立てを調査する権限は、それにより、同委員会による司法上の審査が効果的であることを確保する。従って、委員会は、申し立てを調査し、発見した不適法を職権で取り上げ、その不適法を是正するためのすべての適切な措置を高ずるよう当局に命じる管轄を有する。加えて、諜報収集技術が、国家領域内で、CSI の要件に従い、利用されたことを国家諜報技術監督委員会が検査する。したがって、主手続で問題となっている法律の条項が、関係する者に対する、彼らに適用された監視手段についての通知を規定していないという事実は、それ自体では、私的生活を尊重される権利に対する過度の干渉を構成しない。

68 これらに基づき、国務院は手続を中断すること及び先決裁定のために以下の質問を当裁判所に照会することを決定した:

「(1)[指令 2002/58]第 15 条(1)の実装条項に基づきプロバイダに課された網羅的かつ無差別の保持義務は、国家保安に対する重大かつ持続的な脅威、特にテロリストの脅威、という背景の下、[憲章]第 6 条において保障される保安への権利、及び[TEU]第 4 条に従い、構成国のみにその責任が課されている国家保安の義務により正当化される干渉として扱われるべきか？

(2) [憲章]に照らして読む[指令 2002/58]は、特定された個人のトラフィックデータ及び位置データのリアルタイム収集のための措置であって、電子通信サービスのプロバイダの権利及び義務に影響するものの、しかしながら、彼らに彼らのデータを保持する特定の義務を遵守することを義務づけないような立法措置を認めるものと解釈されるべきか？

(3) [憲章]に照らして読む[指令 2002/58]は、接続データの収集手続の適法性は、データ主体

が、通知されることによりもはや職務権限を有する当局により行われてきた捜査に支障を与える恐れがなくなり次第、知らされることが大前提である、又はそのような手続は、その他すべての既存の手続き的保障手段であって、そのような保障手段が救済を受ける権利が効果的であることを確保する場合に、それらを考慮すると適法とみなされる得ることを意味すると解釈されるべきか？」

Case C-512/18

69 French Data Network、La Quadrature du Net 及び the Fédération des fournisseurs d’accès à Internet associatifs は、2015 年 9 月 1 日付の訴状の提出により、CPCE 第 R.10-13 条及び布告第 2011－219 号の条文が憲章第 7 条、第 8 条及び第 11 条に照らして読む指令 2002/58 第 15 条(1)に違反することを理由として、それらの廃止を求める申立てに対して首相が応答しなかったことによる黙示の拒否決定の無効を求める訴訟を国務院に提起した。Privacy International と the Center for Democracy and Technology は、主手続に参加する申立てを認められた。

70 Cae C-511/18 におけるのと類似の検討を生ずる、CPCE 第 R. 10-13 条及び同条に規定された通信データの網羅的かつ無差別の保持義務につき、照会元裁判所は、そのような保持により法務当局は個人によりなされた通信に関係するデータへのアクセスを、犯罪を実行したとの嫌疑をうける前に許容し、その結果、犯罪の捜査、検知及び訴追のために比類の無い実務上の有用性を備えていると考える。

71 布告第 2011-219 号については、照会元裁判所は、コンテンツの生成に関係するデータのみを保管し保持する義務を課す LCEN 第 6 条(II)は、指令 2002/58 の適用範囲には、当該指令の適用範囲がその第 3 条(1)にしたがい、欧州連合の公衆通信ネットワーク上の公衆が利用可能な電子通信サービスの提供に限定されているため、入らないと考える。一方、その構成国法は、指令 2000/31 の適用範囲に入る。

72 照会元裁判所は、しかしながら、指令 2000/31 の第 15 条(1)及び(2)から、当該指令はコンテンツの生成に関係するデータの保持の原則的禁止であって、そこからの逸脱が、例外による場合にのみ可能であるものを確立していない、と考える。しかしながら、憲章第 6 条、第 7 条、第 8 条及び第 11 条並びに第 52 条(1)に照らして読む指令 2000/31 第 12 条、第 14 条及び第 15 条が、LCEN 第 6 条(II)のような構成国法であって、関係する者が、彼らが提供するサービスのコンテンツの全部又は一部の生成に寄与した者の特定を可能とするデータを保持する義務を、法務当局が適切な場合には、民事又は刑事の責任についてのルールの遵守を確保する目的で当該データの通知を要求することができるように、課すものを構成国が導入することを許容していると解釈すべきかどうか、という疑問が生ずる。

73 それらに基づき、国務院は手続を中断し、先決裁定のために以下の質問を照会することを決

定した:

「(1)[指令 2002/58]第 15 条(1)の実装条項に基づきプロバイダに課された網羅的かつ無差別の保持義務は、就中、そのような接続データの収集及び利用がその際に対象となる防護及び確認に照らし、[憲章]第 6 条において保障される保安への権利、及び[TEU]第 4 条に従い、構成国のみにその責任が課されている国家保安の義務により正当化される干渉とみなされるべきか?

(2) 憲章第 6 条、第 7 条、第 8 条及び第 11 条並びに第 52 条(1)に照らして読む[指令 2000/31]の条文は、その事業が、オンラインの公衆通信サービスへのアクセスの提供により成立している者及び、無償で提供する者もさえも含め、オンライン公衆通信サービスを経由した公衆への提供のために、サービスを受ける者が提供する様々な種類の信号、文章、画像、音声、又はメッセージの記録保存をする自然人又は法人は、これらのサービスを受ける者の要求によりなされた行動又は記録保存された情報について、構成国法であって、関係する者が、彼らが提供するサービスのコンテンツの全部又は一部の生成に寄与した者の特定を可能とするデータを、法務当局が適切な場合には、民事又は刑事の責任についてのルールの遵守を確保する目的で当該データの開示を要求することができるように、保持する義務を課すものを構成国が導入することを許容していると解釈すべきか?

Case C-520/18

74 主手続に併合された 2017 年 1 月 10 日、16 日、17 日及び 18 日に提出された申立書により、the Ordre des barreaux francophones et germanophone、the Académie Fiscale ASBL and UA、the Liga voor Mensenrechten ASBL、the Ligue des Droits de l'Homme ASBL、並びに VZ、WY 及び XX は、ベルギーの憲法裁判所[59]に、2016 年 5 月 29 日の法律が、ECHR 第 5 条、第 6 条から 11 条、第 14 条、第 15 条、第 17 条及び第 18 条、憲章第 7 条、第 8 条、第 11 条、第 47 条及び第 52 条(1)、国連総会により 1966 年 12 月 16 日に採択され 1976 年 5 月 23 日に発効した市民的及び政治的権利についての国際規約第 17 条、法的確実性、比例性及び情報に関する自己決定の一般的原則、並びに TEU 第 5 条(4)と相俟って読むベルギー憲法第 10 条及び第 11 条に違反することを理由として 2016 年 5 月 29 日の法律の廃止を求めて訴訟を提起した。

75 彼らの訴訟の根拠として、主手続の申立人は、要するに、2016 年 5 月 29 日の法律は、他の理由もあるが、厳格に必要な範囲を超えており、かつ、保護の十分な保障を規定していないため違法であると主張する。とりわけ、そのデータの保持に関する条項も、当局による保持

[59] Cour constitutionnelle

されたデータへのアクセスを統制するそれも、2014 年 4 月 8 日付 *Digital Rights Ireland and Others* (C-293/12 and C-594/12, EU:C:2014:238;「*Digital Rights*」) 判決及び 2016 年 12 月 21 日付 *Tele2*(C-203/15 and C-698/15, EU:C:2016:970) 判決から生じた要件を充足していない。これらの条項は、職務権限を有する当局に濫用されるかもしれない個人のプロフィールが集約されるというリスクを必然的に伴い、そして、保持されたデータの十分なレベルの安全性と保護を確立していない、と主張する。最後に、その法は、職業上の秘密保持義務に拘束される者及び守秘義務が課されている者も対象としており、機微な個人的通信のデータに、そのようなデータを保護する特別な防護を含めずに適用される。

76 照会元裁判所は、2016 年 5 月 29 日の法律により、インターネット経由を含む電話サービスのプロバイダ、インターネット接続及びインターネットベースの電子メール及び公衆電子通信ネットワークのプロバイダにより保持されなければならないデータは、公衆が利用可能な電子通信サービス又は公衆通信ネットワークサービスの提供に関係して生成又は処理されるデータの保持についての欧州議会及び理事会の 2006 年 3 月 15 日の指令 2006/24/EC (OJ 2006 L 105, p. 54) に列挙されているものと同一であり、関連する者について、又は追求される目的によって区別されることもない、と判断した。後者の点について、照会元裁判所は、当該法を手段として立法者により追求される目的は、テロリズム及び児童ポルノとの闘いだけではなく、保持されたデータの、刑事捜査の文脈における広汎な種類の状況における利用を可能にすることである。照会元裁判所は、当該法律の説明書から、国内の立法者が、追求される目的に照らして、標的を絞り、選択的なデータを保持する義務を課すことは不可能であると考えたこと、そして、立法者が、網羅的かつ無差別の保持義務に、保持されたデータ及び当該データへのアクセスの双方について、私的生活を尊重される権利への干渉を最小限にとどめるために、厳格な保障を適用することを選択したことが明らかであることも留意する。

77 照会元裁判所は、2016 年 5 月 29 日の法律により改正された 2005 年 6 月 13 日の法律第 126 条(2)第 1 副項及び第 2 副項は、法務当局並びに諜報及び保安機関が、それぞれ保持されたデータへのアクセスを得ることができる条件を規定しており、従って、EU 法の要件に照らした当該法律の適法性の審査は、そのようなアクセスに関して、当裁判所が、係属中の 2 つの先決裁定手続について判断するまで延期されるべき、とも述べる。

78 最後に、照会元裁判所は、2016 年 5 月 29 日の法律は、未成年者の性的虐待が関連する事件における効果的な刑事捜査及び効果的な罰則を確保し、そのような犯罪の加害者を識別することを、たとえ電子通信システムが用いられていても、可能にすることを追求する、と述べる。当該裁判所の手続においては、その点、ECHR 第 3 条及び第 8 条の積極的な義務に関しての注意が喚起された。それらの義務は、憲章の対応する条項上も生じるかも知れず、それ

は指令 2002/58 第 15 条(1)の解釈を左右するかもしれない。

79 それらに基づき、憲法裁判所は手続を中断することを決定し、先決裁定のために以下の質問を当裁判所に照会することを決定した:

「(1) [指令 2002/58]第 15 条(1)は、[憲章]第 6 条により保障される保安の権利、及び[憲章」第 7 条、第 8 条及び第 52 条(1)により保障される個人データを尊重される権利と相俟って読むと、本事件で問題となっているような、その目的を重大な刑事犯罪の捜査、検知及び訴追だけではなく、国家保安、領域の防衛及び公共の保安の防護、重大犯罪でない犯罪の捜査、検知及び訴追、電子通信システムの禁止された利用の防止、又は[規則 2016/679]第 23 条(1)に特定されたその他の目的の達成を目的とする構成国法であって、電子通信サービスの事業者及びプロバイダの、それらのサービスの提供の一貫として、彼らによって生成され処理される[指令 2002/58]の意味におけるトラフィック及び位置データを保持する一般的義務を規定するもの、さらには、当該データの保持及び当該データへのアクセスの観点から、当該法律の特別な防護措置を条件とするもの、を排除すると解釈されねばならないか？

(2) [指令 2002/58]第 15 条(1)は、[憲章]第 4 条、第 7 条、第 8 条、第 11 条及び第 52 条(1)と相俟って、本事件で問題となっているような、構成国法であって、電子通信サービスの運用者と提供者に対して、[指令 2000/58]の意味における、それらのサービスの提供の一環として彼らによって生成され処理されるトラフィックデータと位置データを保持する一般的な義務を規定するものを、当該法律の目的が、とりわけ、[憲章]第 4 条及び第 7 条上当局により果たされるべき積極的な義務を遵守することである場合であって、未成年者の性的虐待の効果的な刑事捜査及び効果的な罰則を可能とし、そのような犯罪の加害者を効果的に識別同定することを、たとえ電子通信システムが用いられていても、可能にする法的枠組みの条項により構成されるものを排除する、と解釈されねばならないか？

(3) 第一及び第二の質問の回答に基づき、もし憲法裁判所が、争われた法律はこれらの質問に言及された条項から生じた義務を充足していない、と判断した場合、法的不確実性を回避し、以前収集され保持されたデータがその法律の目的を追求するために継続して使用されるため、暫定的に[2016 年 5 月 29 日の法律]の効果を維持してよいか？

当法廷での手続

80 2018 年 9 月 25 日付裁判所長官決定により、C-511/18 事件及び C-512/18 事件は、書面及び口答の部分における手続と判決の目的で併合された。C-520/18 事件は、これらの事件に 2020 年 7 月 9 日付裁判所長官決定により、判決の目的で併合された。

照会された質問の検討

C-511/18 事件及びC-512/18 事件の質問1 並びにC-520/18 事件の質問1 及び質問2

81 まとめて検討されるべき C-511/18 事件及び C-512/18 事件の質問 1 並びに C-520/18 事件の質問 1 及び質問 2 により、照会元裁判所は、要するに指令 2002/58 第 15 条(1)が、電子通信サービスの提供者に対して、第 15 条(1)に規定する目的で、トラフィックデータ及び位置データの網羅的かつ無差別の保持を課す構成国法を排除すると解釈されねばならないかどうかを問う。

予備的所見

82 当裁判所が入手した書面からは、主手続で争点となっている法律が、区別や例外なしに、すべての電子通信システムを包含し、そのようなシステムのすべてのユーザに適用されることが明らかである。さらに、当該法律上、電子通信サービスのプロバイダにより保持されなければならないデータは、とりわけ、通信の発信元と通信の到達先を探知するため、通信の日時、長さ及び種類を判定するため、利用された通信機器を識別特定するため、並びに通信機器及び通信を探知するために必要なデータ、データのうち、就中、利用者の名称及び住所、起呼者及び相手方の電話番号を構成するもの、並びにインターネットサービスのための IP アドレスである。対照的に、そのデータは問題の通信の内容を包含しない。

83 したがって、主手続で争点となっている構成国法上、1 年間保持されなければならないとされているデータは、就中、電子通信システムの利用者が通信した相手先の者とどの手段で通信したかを識別し、通信及びインターネット接続の日時及び長さ、並びにそれらの通信及び接続がどの場所から行われたかを判定し、必ずしも通信が送信済みとは限らずに端末機器の位置を確定する。加えて、そのデータは、利用者が一定期間にある者とどの程度の頻度で通信が確立したかどうかの判定を可能にする。最後に、C-511/18 事件及び C-512/18 事件における構成国法については、ネットワークによる電子通信の搬送に関係するデータも包含する限りにおいて、オンラインで照会した情報の性質も識別することを可能にすると思われる。

84 追求される目的については、C-511/18 事件及び C-512/18 事件における構成国法は、その目的として、他の狙いのほか、犯罪の捜査、検知及び訴追一般; 国家の独立、領域の保全及び国家防衛; 主要な外交の利益; フランスの欧州及び国際的な約束の実施; フランスの主要な経済的、産業的及び科学的利益; 並びに、テロリズム、共和政体に対する攻撃、及び法と秩序の維持の深刻な破壊を引き起すおそれのある集団的暴力の防止を追求する。C-520/18 事件の争点となっている構成国法の目的は、就中、刑事犯罪の捜査、検知及び訴追並びに国家保安、領域の防衛及び公共保安の防護である。

85 照会元裁判所は、とりわけ、憲章第 6 条に謳われている保安への権利の指令 2002/58 第 15 条(1)の解釈についての影響の可能性につき確信が持てない。同様に、主手続で争点となっている法律に規定されているデータの保持から必然的に生じる憲章第 7 条及び第 8 条に謳われている基本権に対する干渉が、保持されたデータに対する国家当局によるアクセスを制限するルールの存在に照らして、正当化されたとみなされ得るかどうかを問う。加えて、国務院によると、その質問は国家保安に対する深刻かつ永続的な脅威と特徴付けられている文脈から生ずるため、TEU 第 4 条(2)に照らして評価されるべきとする。一方憲法裁判所は、C-520/18 事件において争点となっている構成国法は、未成年の性的虐待の効果的防止と処罰のための法的枠組みの確立を構成する、憲章第 4 条及び第 7 条から生じる積極的義務も実装していることを指摘する。

86 国務院及び憲法裁判所の双方が、主手続で争点となっている、トラフィックデータ及び位置データの、指令 2002/58 第 15 条(1)に規定する、国家保安の防護のような目的のための保持と国家当局によるそのデータのアクセスを統制するそれぞれの構成国法が、当該指令の適用範囲に包含されている、という前提から出発している一方、主手続の複数の当事者及び当裁判所に書面の意見を提出した構成国のいくつかは、その点、とりわけ当該指令第 1 条(3)の解釈に関して、不賛成である。したがって、まず、争点となっている法律が当該指令の適用範囲に包含されているかを検討する必要がある。

指令 2002/58 の適用範囲

87 La Quadrature du Net、the Fédération des fournisseurs d'accès à Internet associatifs、Igwan.net、Privacy International 及び the Center for Democracy and Technology は、指令 2002/58 の適用範囲についての当裁判所の判例法に依拠し、要するに、データの保持及び保持されたデータへのアクセスの双方が、当該アクセスが非リアルタイム又はリアルタイムで行われようが、当該適用範囲に入ると主張する。実際、国家保安の防護の目的が当該指令第 15 条(1)に明示的に言及されているため、当該目的の追求は、当該指令を不適用とすることにはならない、と主張する。彼らの考えでは、照会元裁判所により言及された TEU 第 4 条(2)は、当該分析に影響を与えない。

88 フランスの職務権限を有する当局により、電子通信サービスのプロバイダに対して特別な義務を課さずに彼らの行動を規制することなく、直接実施される諜報手段については、the Center for Democracy and Technology は、それらの手段が指令 2002/58 第 5 条により保障されている機密保持の原則への例外であるため、必然的に指令 2002/58 及び憲章の適用範囲に包含されると考える。それらの手段は、したがって、当該指令第 15 条(1)から生じる要件を遵守しなければならない。

89 一方、チェコ政府、エストニア政府、アイルランド、フランス政府、キプロス政府、ハンガリー政府、ポーランド政府、スウェーデン政府及び連合王国政府は、要するに、当該指令 2002/58 は、主手続におけるそれのような構成国法には、その法律の目的が国家保安を防護することであるから、適用されないと主張する。諜報機関の活動は、公共の秩序の維持並びに国内保安及び領域の保全の防護に関係する限り、構成国の不可欠な機能の一部であり、従って、とりわけ TEU 第 4 条(2)第 3 文により証明されるとおり、彼らの排他的な権限の範囲内である。

90 これらの政府とアイルランドは、指令 2002/58 の適用範囲から、指令 95/46 第 3 条(2)の最初の段落が過去そうしていたように、公共の保安、防衛及び構成国の保安の活動を除外する当該指令第 1 条(3)にも言及する。彼らはこの点、2006 年 5 月 30 日付 *Parliament v Council and Commission* 判決(C-317/04 及び C-318/04 併合事件 EU:C:2006:346)に記された後者の解釈に依拠する。

91 この点、指令 2002/58 は、その第 1 条(1)上、就中、電子通信分野における個人データの処理に関する均等なレベルの基本的権利及び自由の保護、とりわけプライバシーと機密性を守られる権利、を確保するために必要な構成国の法令の整合性がとれたものにすることを規定していることに留意すべきである。

92 当該指令第 1 条(3)はその適用範囲から、刑事法の分野並びに公共の保安、防衛、そして、その活動が構成国の保安上の事柄と関連するときは、構成国の経済発展を含む構成国の保安を含む、構成国の活動を含む、特定の分野における「構成国の活動」を除外している。このように例示により言及された活動は、いずれにせよ、構成国の活動又は構成国当局の活動であって、個人が活発な分野とは無関係である(2018 年 10 月 2 日付 *Ministerio Fiscal* 判決 C-207/16 事件 EU:C:2018:788 第 32 項及び引用された判例法)。

93 加えて、指令 2002/58 第 3 条は、当該指令が、個人データの収集及び個人識別の仕組みを有する公衆通信ネットワークを含め、欧州連合の公衆通信ネットワーク内の公衆が利用可能な電子通信サービス(「電子通信サービス」)の提供と関連する個人データの処理に適用されると規定する。したがって、当該指令は、そのようなサービスのプロバイダの活動を規制するものとみなされなければならない(2018 年 10 月 2 日付 *Ministerio Fiscal* 判決 C-207/16 事件 EU:C:2018:788 第 33 項及び引用された判例法)。

94 その文脈では、指令 2002/58 第 15 条(1)は、構成国が、規定された条件に服すかぎり、「[当該指令]第 5 条、第 6 条、第 8 条(1)、(2)、(3)及び(4)並びに第 9 条に規定する権利及び義務の範囲を制限するための立法的措置」を採択することができる、と規定する(2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 71 項)。

95 指令 2002/58 第 15 条(1)は、それが、当該指令が規定する条件を充足するときにのみ、構成国が立法的措置を採択することを明示的に許可しているため、言及されている構成国の立法的措置が当該指令の適用範囲内であることを必然的に前提としている。さらに、そのような措置は、当該条項に言及されている目的では、電子通信サービスのプロバイダの活動を規制する(2018 年 10 月 2 日付 *Ministerio Fiscal* 判決 C-207/16 事件 EU:C:2018:788 第 34 項及び引用された判例法)。

96 当裁判所が、指令 2002/58 第 15 条(1)は、その第 3 条と相俟って読むと、当該指令の適用範囲は、電子通信サービスのプロバイダにトラフィックデータ及び位置データを保持することを義務づける立法的措置だけではなく、彼らが当該データへの職務権限を有する当局のアクセスを許すことを義務づける立法的措置にも拡張することを意味すると解釈されねばならない、と判示してきたのは、就中、上述の考え方に照らしたものである。そのような立法的措置は、それらのプロバイダによるそのデータの処理を必然的に伴い、そしてそれらのプロバイダの活動を規制する限りにおいて、指令 2002/58 第 1 条(3)に規定する構成国に特徴的な活動であるとみなすことはできない(この点、2018 年 10 月 2 日付 *Ministerio Fiscal* 判決 C-207/16 事件 EU:C:2018:788 第 35 項及び 37 項並びに引用された判例法を参照)。

97 加えて、上記第 95 項に記した考え方及び指令 2002/58 の一般的な構造に鑑みると、当該措置が追求しなければならない目的が当該同じ指令の第 1 条(3)に言及される活動が追求する目的と相当重複しているためにその第 15 条(1)に言及される立法措置が当該指令の適用範囲から除外されるという当該指令の解釈は、その第 15 条(1)の実効を一切奪うことになる(この点、2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 72 項及び第 73 項参照)。

98 指令 2002/58 第 1 条(3)に示された「活動」の概念は、したがって、独立弁論官により、要するに、彼の *La Quadrature du Net and Others* (C-511/18 及び C-512/18 併合事件 EU:C:2020:6)の意見第 75 項において指摘されたとおり、当該指令第 15 条(1)に示された立法措置を包含するものと解釈することはできない。

99 本判決第 89 項に列挙した政府が参照する TEU 第 4 条(2)は、当該結論を無効にできない。実際、当裁判所の確立した判例法によると、構成国の不可欠な保安の利益を定義し、彼らの域内及び域外の保安を確保する適切な措置を採択するのは、構成国であるが、国家保安を防護する目的で各国の措置が講じられたという単なる事実により EU 法を不適用とすることはできず、構成国の EU 法を遵守する義務から構成国を免除することはできない(この点、2013 年 6 月 4 日付 *ZZ* 判決 C-300/11 事件 EU:C:2013:363 第 38 項; 2018 年 3 月 20 日付 *Commission v Austria (State printing office)*判決 C-187/16 事件 EU:C:2018:194 第 75 項及び第 76 項; 2020 年 4 月 20 日付 *Commission v Poland, Hungary and Czech Republic* (国際的庇護の申請者の移送に関する

暫定措置)判決 C-715/17、C-718/17 及び C-719/17 併合事件 EU:C:2020:257 第 143 項及び第 170 項参照)。

100 確かに、2006 年 5 月 30 日付 *Parliament v Council and Commission* 判決 (C-317/04 及び C-318/04 併合事件 EU:C:2006:346 第 56 項から第 59 項)において、当裁判所は、航空会社から第三国の公共当局へのテロリズム及び他の重大な犯罪を防止し、それらと闘う目的での個人データの移転は、指令 95/46 第 3 条(2)第 1 段落にしたがい、当該移転が公共の保安に関する公共当局により確立された枠組みに入るため、当該指令の適用範囲には入らない、と判示した。

101 しかしながら、本判決第 93 項、第 95 項及び第 96 項に記された考え方に鑑み、当該判例法は指令 2002/58 第 1 条(3)の解釈に類推適用できない。実際、独立弁論官が彼の *La Quadrature du Net and Others* (C-511/18 及び C-512/18 併合事件 EU:C:2020:6)の意見第 70 項から第 72 項において指摘したとおり、要するに、当該判例法が関係する指令 95/46 第 3 条(2)の第 1 段落は、一般的方法で、当該指令の適用範囲から「公共の保安、国防、[及び]構成国の保安に関する処理業務」を、だれが関連するデータ処理作業を実行したかによりいかなる区別もせず、除外している。対照的に、指令 2002/58 第 1 条(3)を解釈する文脈では、そのような区別をする必要がある。本判決第 94 項から第 97 項から明らかなとおり、電子通信サービスのプロバイダにより実行される個人データを処理するすべての業務は、公共当局によりそのようなプロバイダに課された義務によりなされる処理業務も含み、当該指令 2002/58 の適用範囲に入るが、そのような処理業務が、適切な場合には、反対に、指令 95/46 第 3 条(2)の第 1 段落に規定する、公共の保安、国防又は構成国の保安に関するすべての処理業務を含む例外の適用範囲に、当該条項の広汎な書きぶりのために、それらの業務が実行される者にかかわらず、入る可能性がある。

102 さらに、2006 年 5 月 30 日付 *Parliament v Council and Commission* (C-317/04 及び C-318/04 併合事件 EU:C:2006:346)判決をもたらして事件の争点となった指令 95/46 が、規則 2016/679 第 94 条(1)にしたがい、2018 年 5 月 25 日を発効日として廃止され、当該規則により置き換えられたことに留意すべきである。当該規則がその第 2 条(2)(d)において、「職務権限を有する当局により」就中、公共の保安に対する脅威の防護と防止を含む刑事犯罪の防止と検知の目的で、実行された処理作業には適用されないと規定するものの、当該規則第 23 条(1)(d)及び(h)からは、同じ目的で個人により実行された個人データの処理が、当該規定の適用範囲に入るのは明らかである。したがって、指令 2002/58 第 1 条(3)、第 3 条及び第 15 条(1)の上記解釈は、当該指令により補完され、指定された規則 2016/679 の適用範囲の定義と一貫性を有する。

103 対照的に、構成国が、電子通信サービスのプロバイダに処理義務を課すことなく電子通信を秘密として守るという定めから逸脱する措置を直接実装する場合、関係する者のデータの保護は指令 2002/58 ではなく、犯罪行為の防止、捜査、検知若しくは訴追のため、又は刑罰の

執行のために職務権限を有する当局によって処理される個人データについての自然人の保護及び個人データの支障の無い移転についての、かつ理事会枠組み決定 2008/977/JHA を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の指令(EU) 2016/680 (OJ 2016 L 119, p. 89) の適用を条件として、自国の法のみが適用され、その結果、当該問題となる措置は、就中、自国の憲法及び ECHR の諸要件を遵守しなければならない。

104 上述の検討の結果、国家保安の防護及び犯罪との闘いの目的でトラフィックデータ及び位置データの保持を電子通信サービスのプロバイダに義務づける、主手続の争点となっている法令のような国内法令は指令 2002/58 の適用範囲に入る。

指令 2002/58 第 15 条(1)の解釈

105 前提となる観点として、EU 法の条文を解釈する際には、その文言を参照するだけではなく、その文脈及びその当該条文をその構成要素とする法令の目的、及び、とりわけ、当該法令の期限を考慮することが必要である(この点、2018 年 4 月 17 日付 *Egenberger* 判決 C-414/16 事件 EU:C:2018:257 第 44 項参照)、とするのが確立した判例法であることを留意すべきである。

106 指令 2002/58 の目的は、就中、その前文第 6 項及び第 7 項から明らかなように、新技術、特にデータの自動化された記録保存と処理の能力の増大に起因する個人データとプライバシーへのリスクから電子通信サービスの利用者を保護することである。とりわけ、当該指令はその前文第 2 項に記載されているとおり、憲章第 7 条及び第 8 条に規定される権利が完全に尊重されることを確保することを追求している。この点、指令 2002/58 を生み出した電子通信分野における個人データの処理とプライバシーの保護に関する欧州議会と理事会の指令の提案(COM (2000) 385 final)の説明書からは、EU の立法者が「使用される技術にかかわらず、個人データとプライバシーの高レベルの保護がすべての電子通信サービスで継続して保証されることを確保する」ことを追求していることが明らかである。

107 そのために、指令 2002/58 第 5 条(1)は、電子通信及び関連するトラフィックデータの機密保持の原則を謳い、原則として、就中、利用者でない者が、それらの通信及びそのデータを記録保存することが禁止されることを義務付ける。

108 とりわけ、電子通信サービスのプロバイダによるトラフィックデータの処理及び記録保存については、そのような処理はマーケティング及び課金並びに付加価値サービスの提供に必要な範囲かつ必要な期間についてのみ許されることが、指令 2002/58 の第 6 条並びに前文第 22 項及び 26 項から明らかである。いったん当該期間が満了すれば、処理され記録保存されたデータは消去され、又は、匿名化されなければならない。トラフィックデータではない位置データについては、当該指令第 9 条(1)は、当該データは、匿名化されたか、又は利用者又は加入者の同意が既に得られた後に、一定の条件をみたす場合にのみ処理できると規定する(2016

年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 86 項及び引用された判例法)。

109 このように、当該指令を採択するにあたり、EU の立法者は、電子通信サービスの利用者が、原則として、彼らの通信及び、関連するデータが、匿名のままであって記録されてはならないことを、彼らが別段の合意をしない限り、期待する権利を有するように、憲章第 7 条及び第 8 条に謳われた権利について具体的な表現をした。

110 しかしながら、指令 2002/58 第 15 条(1)は、構成国が個人データの機密性を確保するための当該指令第 5 条(1)に規定する義務の原則及び就中、当該指令第 6 条及び第 9 条に示される関連する義務への例外を、そのような制限が、国家保安、防衛、公共の保安を防護するため、及び、犯罪行為又は電子通信システムの無権限使用の防止、捜査、検知及び訴追のために民主的な社会の中において必要、適切、かつ、比例的な措置となる場合には、導入できるようにしている。そのため、構成国は、就中、これらの理由のうち一つにより正当化される限定された期間のデータの保全を規定する立法措置を採択できる。

111 とはいえ、指令 2002/58 第 5 条、第 6 条及び第 9 条に規定する権利及び義務から逸脱する選択権は、電子通信及びそれに関連するデータの機密性を確保するための原則の義務、とりわけ、当該指令第 5 条に明示的に規定されている当該データの記録保存の禁止に対する例外が規範となることまでは許容できない(この点、2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 89 段落及び第 104 段落参照)。

112 指令 2002/58 のとりわけ第 5 条、第 6 条及び第 9 条に規定される権利と義務の制限を正当化することができる目的については、当裁判所は、当該指令第 15 条(1)の第 1 文に規定される列挙された目的は限定列挙されたものであり、その結果、当該条文の下採択された立法措置は、それらの目的に、真に、かつ厳密に、呼応しなければならない(この点、2018 年 10 月 2 日付 *Ministerio Fiscal* 判決 C-207/16 事件 EU:C:2018:788 第 52 項及び引用された判例法参照)。

113 加えて、指令 2002/58 第 15 条(1)第 3 文から、当該指令第 5 条、第 6 条及び第 9 条に規定された権利と義務の適用範囲を制限する立法措置を採択することを、比例性の原則を含む EU 法の一般原則及び憲章により保障された基本的権利にしたがわない限り、構成国が許されていないことが明らかである。この点、当裁判所は、構成国により構成国法令によって、必要な場合、職務権限を有する当局により利用可能とする目的で、電子通信サービスのプロバイダに課されたトラフィックデータを保持する義務が、プライバシーの保護及び個人データの保護にそれぞれ関係する憲章第 7 条及び第 8 条だけではなく、表現の自由に関係する憲章 11 条への適合性の問題を生じることを以前から判示している(この点、2014 年 4 月 8 日付 *Digital Rights Ireland and Others* 判決 C-293/12 及び C-594/12 併合事件 EU:C:2014:238 第 25 項及び第

70 項、2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 91 項及び第 92 項並びに引用された判例法参照)。

114 したがって、指令 2002/58 第 15 条(1)の解釈には、当裁判所の判例法から生じたとおり、憲章第 7 条により保障されるプライバシーへの権利及びその第 8 条により保障される個人データを保護される権利の重要性と並んで、表現の自由への権利の重要性も、憲章第 11 条で保障される当該基本権が、多元的な民主的社会の不可欠の土台を構成し、かつ TEU 第 2 条上、欧州連合がその上に築かれた価値観の一つであることを踏まえ、考慮に入れなければならない(この点、2001 年 3 月 6 日付 *Connolly v Commission* 判決 C-274/99 P 事件 EU:C:2001:127 第 39 条及び 2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 93 項参照)。

115 この点、トラフィックデータ及び位置データの保持は、それ自体、一方では、利用者以外の何者も当該データを記録保存することを禁ずる、指令 2002/58 第 5 条(1)に規定する禁止事項からの逸脱であり、及び、他方では、憲章第 7 条及び第 8 条に謳われている私的生活の尊重を受け、個人データを保護される基本権への干渉であり、それが、私的生活に関係する問題の情報が機微であるかどうか、又は、対象となる者が当該干渉のために不便を被ったかどうかに係わらないことを明確にしておきたい(この点、この点、2017 年 7 月 26 日付意見 1/15 (*EU-Canada PNR Agreement*) EU:C:2017:592 第 124 項及び第 126 項並びに引用された判例法参照;ECHR 第 8 条について、ECtHR の 2020 年 1 月 30 日付 *Breyer v. Germany* 判決 CE:ECHR:2020:0130JUD005000112 第 81 項を類推して参照)。

116 保持されたデータがその後利用されたかどうかも、当該データへのアクセスは、その後の利用にかかわらず、前項に言及された基本権人権への別個の干渉行為(この点、2017 年 7 月 26 日付意見 1/15 (*EU-Canada PNR Agreement*) EU:C:2017:592 第 124 項及び第 126 項を参照)であるから、関係が無い(ECHR8 条につき EctHR の 2000 年 2 月 16 日付 *Amann v. Switzerland* 判決 CE:ECHR:2000:0216JUD002779895 第 69 項及び 2020 年 2 月 13 日付 *Trajkovski and Chipovski v. North Macedonia* 判決 CE:ECHR:2020:0213JUD005320513 第 51 項を類推して参照)。

117 その結論は、トラフィックデータ及び位置データが、関係する者の私的生活の、性的指向、政治的意見、宗教的、哲学的、社会的又はその他の信念及び健康状態のような機微な情報を含む、多数の側面についての情報をあらわにするかもしれないため、そのようなデータが EU 法の下でさらに特別な保護を受けていることを考えると、なおさら正当化される。全体として、当該データは、そのデータを保持された者の、たとえば日常生活の習慣、恒久的又は一時的な居住地、日常的又はその他の移動、実行される活動、それらの人々の社交、及び彼らが頻繁に訪れる社会的環境などの私的生活に関して非常に正確な結論を引き出すことを可能にする。とりわけ、当該データは関連する者のプライバシーへの権利の観点からは実際の

通信の内容に勝るとも劣らない機微な情報である、プロフィールを確証する手段を提供する(この点、2014 年 4 月 8 日付 *Digital Rights* 判決 C-293/12 及び C-594/12 併合事件 EU:C:2014:238 第 27 項及び 2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 99 項参照)。

118 したがって、第一に、警察目的でのトラフィックデータ及び位置データの保持は、それ自体、憲章第 7 条に謳われている通信を尊重される権利を侵害し、電子通信システムの利用者が、憲章第 11 条において保障されている彼らの表現の自由を行使することを萎縮させるおそれがある(この点、2014 年 4 月 8 日付 *Digital Rights* 判決 C-293/12 及び C-594/12 併合事件 EU:C:2014:238 第 28 項及び 2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 101 項参照)。そのような萎縮は、とりわけ自己の通信が、職業上の機密保持義務にかかる者及びその行為が連合法違反を通報した者の保護に関する欧州議会及び理事会の 2019 年 10 月 23 日の指令(EU) 2097/1937 (OJ 2019 L 305, p. 17)によって保護される公益通報者に影響を与え得る。その上、当該萎縮効果は、保持されたデータの数量や広範さを考えると、さらに深刻である。

119 第二に、継続的に、網羅的かつ無差別の保持措置の下保持されるトラフィックデータ及び位置データの多大な数量並びに当該データから推測される情報の機微な性質を考えると、電子通信サービスのプロバイダによる単なる保持は、非違行為及び違法なアクセスのリスクが必然的に生ずる。

120 とはいえ、指令第 15 条(1)が、構成国が上記第 110 条に言及される逸脱を導入することを許容している限りにおいて、当該条文は、憲章第 7 条、第 8 条及び第 11 条に謳われている権利が絶対的権利ではなく、それらの社会における機能との関係で検討されなければならない、という事実を反映している(この点、2020 年 7 月 16 日付 *Facebook Ireland and Schrems* 判決 C-311/18 事件 EU:C:2020:559 第 172 項及び引用された判例法参照)。

121 実際、憲章第 52 条(1)に見て取れるとおり、当該条文はそれらの権利の行使に制限をかけることを、当該制限が、法律に規定され、それらの権利の本質を尊重し、比例性の原則を遵守して、それらが必要であり、かつ欧州連合によって認められた一般的利益の目的又は他者の権利及び自由を保護するための必要に真に適合している場合に、許容している。

122 したがって、指令 2002/58 第 15 条(1)を憲章に照らし解釈するためには、憲章第 3 条、第 4 条、第 6 条及び第 7 条に謳われている権利の重要性並びに他者の権利及び自由の保護に寄与する国家保安防護及び重大犯罪との闘いの目的の重要性も考慮しなければならない。

123 この点、フランス国務院及びベルギー憲法裁判所が言及する憲章第 6 条は、すべての個人の自由への権利だけではなく、保安への権利を規定し、ECHR 第 5 条により保障されている権

利に呼応する権利を保障している(この点、2016 年 2 月 15 日付 *N.*判決 C-601/15 PPU 事件 EU:C:2016:84 第 47 項; 2016 年 7 月 28 日付 *JZ* 判決 C-294/16 PPU 事件 EU:C:2016:610 第 48 項; 及び 2019 年 9 月 19 日付 *Rayonna prokuratura Lom* 判決 C-467/18 事件 EU:C:2019:765 第 42 項, paragraph 42 並びに引用された判例法参照)。

124 加えて、憲章第 52 条(3)が、憲章に含まれている権利と、ECHR で保障されている呼応する権利との間の必要な一貫性を、EU 法の自律性及び欧州連合司法裁判所のそれに悪影響を与えない範囲で、確保することを意図していることを思い起こすべきである。したがって、憲章を解釈する目的においては、ECHR の呼応する権利を、保護の最小限の範囲として、考慮にいれなければならない(この点、2019 年 2 月 12 日付 *TC* 判決 C-492/18 PPU 事件 EU:C:2019:108 第 57 項及び 2019 年 5 月 21 日付 *Commission v Hungary (Rights of usufruct over agricultural land)*判決 C-235/17 事件 EU:C:2019:432 第 72 項並びに引用された判例法参照)。

125 「自由への権利」及び「安全への権利」を謳う ECHR 第 5 条は、欧州人権裁判所の判例により、個人が、恣意的又は不当な自由の剥奪から保護されることを確保することを意図している(この点、EctHR の 2008 年 5 月 18 日付 *Ladent v. Poland* 判決 CE:ECHR:2008:0318JUD001103603 第 45 項及び第 46 項; 2010 年 3 月 29 日付 *Medvedyev and Others v. France* 判決 CE:ECHR:2010:0329JUD000339403 第 76 項及び第 77 項; 及び 2012 年 12 月 13 日付 *El-Masri v. 'The former Yugoslav Republic of Macedonia'* 判決 CE:ECHR:2012:1213JUD003963009 第 239 項参照)。しかしながら、当該条項は、公共の当局による自由の剥奪に適用されるため、憲章第 6 条が、公共の当局に一定の犯罪行為を防止し、処罰する特定の措置を講じる義務を課すものであると解釈することはできない。

126 他方、ベルギー憲法裁判所により言及された、とりわけ未成年者及びその他の脆弱な者に対し行われた犯罪行為と闘うための効果的行動については、公共の当局の能動的義務が私的及び家族の生活を保護するための法的措置を採用することを求める憲章第 7 条から生じ得ることを指摘すべきである(この点、2020 年 6 月 18 日付 *Commission v Hungary (Transparency of associations)*判決 C-78/18 事件 EU:C:2020:476 第 123 項及び引用された欧州人権裁判所の判例法を参照)。そのような義務は、個人の住居及び通信の保護に関する第 7 条並びに個人の身体的及び精神的完全性並びに拷問並びに非人間的及び人間的尊厳を損なう扱いの禁止に関する第 3 条及び第 4 条からも生じ得る。

127 当裁判所が問題となっているさまざまな利益と権利の間で均衡を取らなければならないのは、これらの異なる能動的義務を背景にしている。

128 憲章第 4 条及び第 7 条に対応する防護措置が規定されている ECHR 第 3 条及び第 8 条から生じる能動的義務は、特に、実体的及び手続き的条項並びに、効果的捜査及び訴追を通じて人

に対する犯罪と闘うための効果的行動を可能にする実務的手段の採択を要求しており、当該義務は、こどもの身体的及び倫理的健康がリスクにさらされている場合になおそら重要である、と欧州人権裁判所は判示してきた。しかしながら、職務権限を有する当局が講じる措置は、犯罪捜査権限の範囲を制限する適正手続き及びその他の保護措置、並びにその他の自由及び権利を完全に尊重する必要がある。とりわけ、当該裁判所によると、保護されるべきさまざまな利益と権利の間で均衡を取ることを可能とする法的枠組みが確立されるべきである (EctHR の 1998 年 10 月 28 日付 *Osman v. United Kingdom* 判決 CE:ECHR:1998:1028JUD002345294 第 115 項及び第 116 条; 2004 年 3 月 4 日付 *M.C. v. Bulgaria* 判決 CE:ECHR:2003:1204JUD003927298 第 151 項; 2004 年 6 月 24 日付 *Von Hannover v. Germany* 判決 CE:ECHR:2004:0624JUD005932000 第 57 項及び第 58 条; 及び 2008 年 12 月 2 日付 *K.U. v. Finland* 判決 CE:ECHR:2008:1202JUD000287202 第 46 項、第 48 項 及び第 49 項)。

129 比例性の原則の遵守については、指令 2002/58 第 15 条(1)第 1 文は、構成国が、通信及び関連するトラフィックデータが機密として保たれるという原則から逸脱する措置を、そのような措置が、当該条項に規定する目的の見地から「民主的社会において…必要、適切かつ比例的」である場合、採択できると規定する。当該指令前文第 11 項は、そのような性質の措置は、企図された目的に「厳格に」比例しなければならない、と規定する。

130 この点、当裁判所の確立した判例法によれば、プライバシーへの基本権の保護は、個人データの保護についての逸脱及び制限が、厳格に必要な場合にのみ適用しなければならないことを要求していることに留意すべきである。加えて、一般的利益の目的は、当該一般的利益の目的を問題となっている基本的権利と適切に均衡を取ることにより、その措置から影響を受ける基本的権利との整合をとらなければならない、という事実を鑑みずに追求してはならない(この点、2008 年 12 月 16 日付 *Satakunnan Markkinapörssi and Satamedia* 判決 C-73/07 事件 EU:C:2008:727 第 56 項; 2010 年 11 月 9 日付 *Volker und Markus Schecke and Eifert* 判決 C-92/09 及び C-93/09 併合事件 EU:C:2010:662 第 76 項、第 77 項及び第 86 項; 並びに 2014 年 4 月 8 日付 *Digital Rights* 判決 C-293/12 及び C-594/12 併合事件 EU:C:2014:238 第 52 項; 2017 年 7 月 26 日付意見 1/15 *(EU-Canada PNR Agreement)*EU:C:2017:592 第 140 項参照)。

131 特に、当裁判所の判例法からは、構成国が、就中、指令 2002/58 第 5 条、第 6 条及び第 9 条に規定された権利及び義務についての制限を正当化できるかどうかは、当該制限から不可避的に生じる干渉の深刻度を測り、当該制限により追求される公共の利益の目的の重要性が、当該深刻度に比例していることを検証することにより評価されなければならない(この点、2018 年 10 月 2 日付 *Ministerio Fiscal* 判決 C-207/16 事件 EU:C:2018:788 第 55 項及び引用された判例法参照)。

132 比例性の要件を満たすためには、法令は問題の措置の適用範囲及び実装を統制し、最小限の

防護措置を課す明瞭で精緻な規則を、その個人データが影響を受ける者が、当該データが非違行為のリスクから効果的に保護されることの十分な保障を有するよう、規定しなければならない。当該法令は国内法上、法的拘束力を有し、とりわけ、どの状況で、かつどの条件の下そのようなデータの処理を規定する措置が採択できるかを示さなければならず、それにより干渉が厳格に必要な範囲に限定されていることを確保する。そのような防護措置の必要性は、個人データが自動化された処理の対象となる場合、とりわけ当該データへの違法なアクセスの多大なリスクがある場合、さらに大きい。これらの考え方は、特に、機微なデータである特定の種類の個人データの保護が問題となっている場合、適用される(この点、2014 年 4 月 8 日付 *Digital Rights Ireland and Others* 判決 C-293/12 及び C-594/12 併合事件 EU:C:2014:238 第 54 項及び第 55 項、2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 事件 EU:C:2016:970 第 117 項; 2017 年 7 月 26 日付意見 1/15 *(EU-Canada PNR Agreement)* EU:C:2017:592 第 141 項を参照のこと)。

133 したがって、個人データの保持を義務づける法令は、常に、保持されることになるデータと追求される目的との間の連関を確立する客観的基準を満たさなければならない(この点、2017 年 7 月 26 日付意見 1/15 *(EU-Canada PNR Agreement)* EU:C:2017:592 事件第 191 項及び引用された判例法、及び 2019 年 10 月 3 日付 *A and Others* 判決 C-70/18 事件 EU:C:2019:823 第 63 項参照)。

－ 国家保安を防護する目的でのトラフィック及び位置データの予防的保持を規定する立法措置

134 照会元裁判所及び意見陳述書を提出した政府により言及された国家保安を防護する目的は、指令 2002/58 を解釈する判決において、未だ特別に審査されたことがないと考えるべきである。

135 この点、まず、TEU 第 4 条(2)が国家保安は、各構成国の単独の責任として残されると規定していることに留意すべきである。その責任は、構成国の不可欠な機能と社会の基本的な利益を保護するという主たる利益に対応するものであり、一国の憲法上、政治的、経済的、又は社会的な基本的構造を著しく不安定にする、そして、特にテロリストの活動のような社会、住民、構成国自体を直接脅かす可能性がある活動の予防及び処罰を含む。

136 TEU 第 4 条(2)に照らして読むと、国家保安の防護の目的の重要性は、指令 2002/58 第 15 条(1)に言及される他の目的、就中、一般的な犯罪との闘い、それどころか重大犯罪との闘い及び公共の保安の防護の目的の重要性を超える。前項に言及されているような脅威は、その性質及び特別な深刻度から、公共の保安に影響する緊張又は混乱が生じる、たとえそれが深刻な性質であるとしても、一般的なリスクと区別できる。憲章第 52 条(1)に規定するその他の

要件の充足を条件に、国家保安の防護の目的は、従って、基本権へのより深刻な干渉を必然的に伴う措置を、それら他の目的により正当化できるかもしれない措置よりも、正当化できる。

137 したがって、本判決第135項及び136項に描写されたもののような状況において、指令2002/58第15条(1)は、憲章第7条、第8条、第11条及び第52条(1)に照らして読むと、原則として、職務権限を有する当局が電子通信サービスのプロバイダに電子通信システムのすべての利用者のトラフィックデータ及び位置データの保持を、限定した長さの期間命じることを、関係する構成国が、本判決第135項及び第136項に言及され、真であり、現存するか又は予見可能であることが示された国家保安に対する深刻な脅威に直面していると考える十分確実な理由がある限り、許容する立法措置を排除しない。たとえそのような措置が電子通信システムのすべての利用者に無差別に適用され、一見、本判決第133項に引用された判例法の意味におけるその構成国の国家保安への脅威とのいかなる連関もそこになくとも、それにもかかわらず、当該脅威の存在そのものが、それ自体、当該連関を確立することができる、と考えなければならない。

138 電子通信システムのすべての利用者のデータの予防的保持のための命令は、しかしながら、厳格に必要な範囲で期間を限定していなければならない。電子通信サービスのプロバイダにデータを保持することを要求する命令が、そのような脅威の継続的性質により、更新可能であることも考えられるが、各命令の期間は、予見可能な期間を超えることはできない。それだけではなく、そのようなデータ保持は、制限に服さなければならず、関連する者の個人データを非違行為のリスクから効果的に保護することを可能にする厳格な保護措置により範囲を限定されなければならない。したがって、当該保持は、本質的に機械的性質であってはならない。

139 網羅的かつ無差別のデータの保持を伴う措置から生じる憲章第7条及び第8条に謳われている基本権への干渉の深刻度を考えると、そのような措置への依拠は、実際には、本判決第135項及び第136項に言及された国家保安への深刻な脅威がある状況に限定されるよう確保しなければならない。当該目的では、電子通信サービスのプロバイダに対して、そのようなデータ保持を実行させる命令を発出する決定が、裁判所又は独立した行政機関であってその決定に拘束力があるもののいずれかによる、効果的な審査であって、当該審査の目的が、それらの状況の一つが存在すること並びに法令に規定されなければならない当該条件及び防護措置が遵守されていることを検証することにあるものに服すことが不可欠である。

ー 犯罪との闘い及び公共の保安の防護の目的でのトラフィック及び位置データの予防的保

持を規定する立法措置

140 犯罪行為を防止し、捜査し、検知し、及び訴追する目的については、比例性の原則にしたがい、重大犯罪と闘う行為及び公共の保安への深刻な脅威を防止するための措置のみが、トラフィックデータ及び位置データの保持により不可避的に生じる干渉のような憲章第 7 条及び第 8 条に謳われている基本権への深刻な干渉を正当化できる。したがって、それらの基本権への深刻でない干渉のみが、一般的に犯罪行為を防止し、捜査し、検知し、及び訴追する目的により正当化される(この点、2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 102 項、2018 年 10 月 2 日付 *Ministerio Fiscal* 判決 C-207/16 事件 EU:C:2018:788 第 56 項及び第 57 項、2017 年 7 月 26 日付意見 1/15 *(EU-Canada PNR Agreement)* EU:C:2017:592 第 149 項参照)。

141 重大な犯罪との闘いの目的で網羅的かつ無差別のデータの保持を規定する構成国法は、厳格に必要な範囲の限界を超えており、憲章第 7 条、第 8 条、第 11 条及び第 52 条(1)に照らして読む指令 2002/58 第 15 条(1)により要求されるとおり民主的社会において正当化されるとは考えられない(この点、2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 107 項参照)。

142 トラフィックデータ及び位置データが示す可能性のある情報の機微な性質を考えると、そのデータの機密性は私的生活を尊重される権利に不可欠である。したがって、第一に、当該データの保持に起因する、上記第 118 項に述べた憲章第 7 条及び第 11 条に謳われている基本権の行使への萎縮効果、第二にそのような保持から不可避的に生じる干渉の深刻度に鑑みると、民主的な社会においては、指令 2002/58 により確立されたシステムにより規定されるとおり、当該保持は例外とし、規範としないこと、そしてデータが機械的かつ継続的に保持されないことが必要である。当該結論は、重大犯罪との闘い公共の保安への深刻な脅威を防止する目的及びそれらに付随する重要性を鑑みても適用される。

143 加えて、当裁判所は、網羅的かつ無差別のトラフィックデータ及び位置データの保持を規定する法令が、事実上全人口の電子通信を、目的に照らしたいかなる区別、限定及び例外もなく対象とすることを強調してきた。そのような法令は、上記第 133 項に言及した要件と対照的に、それが電子通信サービスを利用するすべての者に、それらの者が間接的でさえ刑事手続を生ずるようなおそれがある状況になくても、影響する点において包括的である。それはしたがって、彼らの行動と、たとえ間接的又は遠いものでさえも、重大犯罪との闘いの目的との関係性があるかもしれないことを示唆することができる証拠がない者、及び、とりわけ、その者の保持が規定されたデータ及び公共の安全への脅威との関係が無い場合にも適用される(この点、2014 年 4 月 8 日付 *Digital Rights* 判決 C-293/12 及び C-594/12 併合事件 EU:C:2014:238 第 57 項及び第 58 項、2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15

併合事件 EU:C:2016:970 第 105 項参照)。

144 とりわけ、当裁判所が以前判示したとおり、そのような法令は(i) 何らかの形で重大犯罪に関与するおそれのある期間及び／又は、地理的範囲及び／又は、人々の集団に関係するデータ、又は(ii)その他の理由で、彼らのデータの保持により重大犯罪との闘いに寄与するかもしれない人々、に関係する保持に限定されていない(この点、2014 年 4 月 8 日付 *Digital Rights* 判決 C-293/12 及び C-594/12 併合事件 EU:C:2014:238 第 59 項、2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 106 項参照)。

145 状況に応じて、憲章第 3 条、第 4 条及び第 7 条から生じるかもしれない構成国の能動的義務であって、本判決第 126 項及び第 128 項で指摘したとおり、犯罪行為との闘いへの効果的行動を促進する規範の定立に関係するものであっても、関連する者のデータと追求される目的の間に、少なくとも間接的な関係もなく、事実上全人口のトラフィックデータ及び位置データの保持を規定する法令から不可避的に生じる、憲章第 7 条及び第 8 条に謳われている基本権への干渉のような深刻な干渉を正当化する効果を持ち得ない。

146 対照的に、本判決第 142 条から第 144 条に記したものにしたがい、かつ問題となる権利と利益の間で取らねばならない均衡に鑑み、重大犯罪との闘い、公共の保安に対する深刻な攻撃の防止、及び、特に国家保安の防護の目的は、―就中、前項で述べた能動的義務であって、ベルギー憲法裁判所が言及したそれらの重要性を考えると―トラフィックデータ及び位置データの標的を絞った保持から生じる特に深刻な干渉を正当化できる。

147 したがって、当裁判所が以前から判示してきたとおり、憲章第 7 条、第 8 条、第 11 条及び第 52 条(1)に照らして読む指令 2002/58 第 15 条(1)は、構成国が、トラフィックデータ及び位置データの標的を絞った保持を、重大犯罪と闘い、公共の保安への深刻な脅威を防止し、及び等しく国家保安を防護する目的で、防止措置として許容する法令の採択を、そのような保持が、保持されるデータの種類、影響する通信の手段、関連する者及び定められた保持期間について、厳格に必要な範囲に限定されている限り、禁止しない(この点、2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 108 項参照)。

148 そのようなデータ保持措置が服しなければならない限界については、それらは、指令 2002/58 第 15 条(1)が、そのトラフィックデータ及び位置データが、何らかの形で重大な犯罪との闘い又は公共の安全への深刻なリスクもしくは国家保安のリスクを防止することに寄与するため、少なくとも間接的な、重大な犯罪行為との繋がりを示すおそれがある者を、絞り込むことを可能とする客観的証拠に基づく立法を排除していないため、とりわけ、関連する者の種別にもとづき決定できる(この点、2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 111 項参照)。

149 この点、そのように絞り込まれた人々は、とりわけ、適用される国内手続の途上で、かつ客観的証拠に基づき、関連する構成国において、公共の保安又は国家保安への脅威を呈するとして、事前に識別特定された人々であるかもしれないことを明らかにしなければならない。

150 トラフィックデータ及び位置データの保持を規定する手段の限界は、職務権限を有する国内の当局が、客観的かつ非差別的な要素に基づき、一又はそれ以上の地理的範囲において、重大な犯罪行為の準備又は実行の高度のリスクにより特徴付けられる状況にあると考える場合には、地理的な基準を利用することによっても設定できる(この点、2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 111 項参照)。これらの範囲には、重大犯罪の高い発生率のある場所、日常的に非常に大量の訪問者を受け入れている場所又は施設のような重大な犯罪行為の実行に対して特に脆弱な場所又は空港、駅若しくは料金所エリアのような戦略的場所を含みうる。

151 本判決第 147 項から 150 項に描写された標的を絞った保持措置により不可避的に生ずる干渉が比例性の原則を遵守することを確保するためには、それらの期間は、追求された目的及びそれを正当化する状況に照らして厳格に必要な範囲を、そのような保持が継続して必要な場合にはそれらの措置の延長の可能性を妨げることなく、超えてはならない。

ー 犯罪との闘い及び公共の保安の防護の目的での IP アドレス及び市民識別同定に関するデータの予防的保持を規定する立法措置

152 IP アドレスはトラフィックデータの一部であるが、それらは特定の通信とは独立して生成され、電子通信サービスのプロバイダを通じて、インターネット通信がなされた端末機器を所有する自然人を識別するために主に用いられることに留意すべきである。したがって、電子メール及びインターネット電話との関係では、通信の発信元の IP アドレスのみが保持され、その受信者の通信の IP アドレスが保持されていなければ、それらのアドレスは、そのように、通信を行った者と連絡を取った第三者についていかなる情報も、開示しない。その種類のデータについてはしたがって、他のトラフィックデータよりも機微度が低い。

153 しかしながら、IP アドレスは、とりわけ、インターネット利用者の完全なクリック履歴、したがって彼又は彼女のオンライン活動のすべてを追跡するために利用できるので、そのデータは利用者の詳細なプロフィールが生成されるのを可能にする。したがって、そのような追跡に必要な、それらの IP アドレスの保持及び分析は、インターネット利用者の憲章第 7 条及び第 8 条に謳われた基本権への深刻な干渉を構成し、それは本判決第 118 項に言及された萎縮効果を有する。

154 本判決第 130 条に引用された判例法により要求される問題となる権利と利益の均衡を取るためには、オンラインで犯罪行為が行われた場合、IP アドレスは、犯罪行為が行われた時点で

そのアドレスが割り当てられた者を識別するために唯一の操作手段かもしれない、という事実を考慮しなければならない。その考慮事項に、電子通信サービスのプロバイダによる IP アドレスの当該データが割り当てられた期間を超える保持は、原則として問題のサービスの課金の目的に必要ではなく、その結果、オンラインでなされた犯罪行為の検知はしたがって、指令 2002/58 第 15 条(1)にもとづく立法措置への依拠無しには、立証するのが不可能であるという、いくつかの政府が、かれらの当裁判所への意見陳述書中に述べたような、事実を加えなければならない。それらの政府が主張するとおり、それは、就中、児童の性的虐待及び性的搾取並びに児童ポルノとの闘いについての、並びに理事会枠組み決定 2004/68/JHA を置き換える欧州議会及び理事会の 2011 年 12 月 13 日の指令 2011/93/EU (OJ 2011 L 335, p. 1)第 2 条(c)の意味におけるとりわけ深刻な児童ポルノの取得、頒布、送信又はオンラインでの利用可能化のような児童ポルノ犯罪を伴う事件において起き得る。

155 これらの状況において、確かに、すべてのインターネットへのアクセスができる端末機器を所有する自然人の IP アドレスの保持を規定する立法措置により、一見して、追求された目的と、本判決第 133 項に引用された判例法の意味における、何の連関のない者を把握してしまうかもしれないし、又、インターネットユーザは、本判決第 109 項に記された内容にしたがい、憲章第 7 条及び第 8 条の下、彼らの素性が、原則として開示されないことを期待する権利を有していることも確かである一方、接続元に割り当てられたＩＰアドレスのみの網羅的かつ無差別の保持を規定する立法措置は、原則として、当該可能性が、当該データの利用を規制する実体的及び手続き的条件への厳格な遵守を条件とする限り、憲章第 7 条、第 8 条、第 11 条及び第 52 条(1)に照らして読む指令 2002/58 第 15 条(1)に反してはいないと思える。

156 当該保持により不可避的に生じる、憲章第 7 条及び第 8 条に謳われている基本権への干渉の深刻さに照らし、重大犯罪と闘うための行動、公共の安全への深刻な脅威の防止、及び国家保安の防護のみが、当該干渉を正当化することができる。さらに、保持期間は、追求された目的に照らし厳格に必要な範囲を超えてはならない。最後に、その性質の措置は、当該データの、特に追跡による、関連する者によりなされた通信及びオンラインで実行された行為についての利用に関する、厳格な条件と防護手段を確立しなければならない。

157 最後に、電子通信システムの利用者の市民としての識別同定に関係するデータに関して、当該データはそれ自体が、行われた通信の日にち、時刻、期間及び受信者、又はそれらの通信がなされた場所、又はそれらの通信が、ある期間中に特定の者となされた頻度を確定することを可能にしないので、その結果、それら利用者の、住所のような連絡先の詳細を除き、送信された通信に関する情報を提供せず、結果として利用者の私的生活に関する情報も提供しない。したがって、当該データの保持により不可避的に生じる干渉は、原則として深刻なものと分類できない(この点、2018 年 10 月 2 日付 *Ministerio Fiscal* 判決 C-207/16 事件

EU:C:2018:788 第 59 項及び第 60 項参照)。

158 したがって、本判決第 140 項に述べられたものにしたがい、関連する利用者を識別する単独の目的での当該データの保持と当該データへのアクセスであって、そのデータをなされた通信に関するデータと関連付けることが可能では無いものを含むそのような当該データの処理に関する立法措置は、指令 20002/58 第 15 条(1)が言及する、犯罪行為一般の防止、捜査、検知及び訴追の目的により正当化できる(この点、2018 年 10 月 2 日付 *Ministerio Fiscal* 判決 C-207/16 事件 EU:C:2018:788 第 62 項参照)。

159 これらの状況において、問題となっている権利及び利益の間で取られなければならない均衡に鑑み、本判決第 131 項及び第 158 項に記した理由により、たとえ、電子通信システムのすべての利用者と追求された目的の間になんら連関がないとしても、憲章第 7 条、第 8 条第 11 条及び第 52 条(1)に照らして読む指令 2002/58 は、電子通信サービスのプロバイダに、特定の期間の制限なしに、すべての電子通信システムの利用者の市民識別同定に関係するデータの保持を、犯罪行為一般を防止し、捜査し、検知し及び訴追する目的並びに公共の保安を防護する目的で義務づける立法措置を、犯罪行為又は公共の保安について悪影響をもたらす脅威若しくは行為が深刻である必要もなく、排除しないと判示しなければならない。

ー 重大犯罪と闘う目的でのトラフィック及び位置データの迅速な保持を規定する立法措置

160 指令 2002/58 第 5 条、第 6 条及び第 9 条に基づき、又は本判決第 134 項から第 159 項までに描写されたとおり、当該指令第 15 条(1)の下講じられた立法措置に基づき電子通信サービスにより処理され記録保存されたトラフィックデータ及び位置データについては、当該データが、状況に応じて、当該指令を移植した構成国法の条項にしたがい処理され記録保存されなければならない法定の期間の終了時に、原則として、消去されるか、又は匿名化されなければならないことが留意されるべきである。

161 しかしながら、当該処理及び記録保存の期間中、重大犯罪又は国家保安に悪影響を与える行為を注視するため、当該機関が修了した後も当該データを保持することが必要となる状況が生じるかも知れない; これは、これらの犯罪又は悪影響を与える行為が既に確立されている場合、及び、すべての関連する状況の客観的な分析の後、そのような犯罪又は悪影響を与える行為が、合理的に疑われる場合の双方の状況にあてはまる。

162 この点、27 の構成国により署名され、うち 25 カ国により批准された 2001 年 11 月 23 日の欧州評議会のサイバー犯罪に関する条約(European Treaty Series – No. 185)は、その目的としてコンピュータネットワークを用いて行われた犯罪行為との闘いを促進することを有するが、その第 14 条において、その条約の締約国が、特定の刑事捜査又は刑事手続の目的で、既に記録保存されたトラフィックデータに関する当該データの迅速な保全のような一定の措置を採

択すべきことを規定する。とりわけ、当該条約第 16 条(1)は当該条約の締約国が、特に、自国の職務権限を有する当局が、コンピュータシステムによって記録保存されたトラフィックデータが、特に滅失しやすく又は改変されやすいと信ずるに足りる理由がある場合には、当該データについて迅速な保全を命令すること又はこれに類する方法によって迅速な保全を確保することを可能にするため、必要な立法措置をとるべきことを規定する。

163 本判決第 161 項に描写された状況において、問題の権利と利益との間で取られなければならない均衡に照らし、構成国が、指令 2002/58 第 15 条(1)にしたがい採択された立法において、職務権限を有する当局による決定であって、効果的な法務上の審査に服するものにより、電子通信サービスのプロバイダに対して彼らが処分権限を有するトラフィックデータ及び位置データの指定された期間の保持を命令する可能性を規定することは許容できる。

164 そのような迅速な保持の目的がもはやデータが当初収集され保持された目的と呼応しなくなった限りにおいて、かつ、いかなるデータの処理も、憲章第 8 条(2)の下、指定された目的と一貫性を有しなければならないため、構成国は、彼らの法令において、データの迅速な保持が何の目的で行われてよいかを明らかにしなければならない。そのような保持から生ずる憲章第 7 条及び第 8 条に謳われた基本権への干渉の深刻な性質に照らし、重大犯罪と闘う行動、及び、さらには、国家保安の防護のようなもののみが、そのような干渉を正当化できる。さらには、その主の措置により不可避的に生じる干渉が厳格に必要な範囲に限定されることを確保するためには、第一に、その保持義務は、問題の重大犯罪又は国家保安に悪影響を与える行動の解明に役立つトラフィックデータ及び位置データのみに関係しなければならない。第二に、そのようなデータが保持される期間は、状況及びその措置により追求される目的が、延長することを正当化する場合は延長できるが、厳格に必要な範囲に限定されなければならない。

165 この点、そのような迅速な保持は、問題の重大犯罪又は国家保安に悪影響を与える行動をしたことが具体的に疑われる者のデータに限定される必要は無い。憲章第 7 条、第 8 条、第 11 条及び第 52 条(1)に照らして読む指令 2002/58 第 15 条(1)により確立された枠組みを遵守し、上記第 133 項における事実を考慮に入れる一方、そのような措置は、立法者の選択により、厳格に必要な範囲の限界に服しつつ、問題の重大犯罪又は国家保安に悪影響を与える計画をし、又は行動したことが疑われる者以外の者に関係するトラフィックデータ及び位置データに、当該データが、客観的かつ非差別的な要素により、そのような犯罪又は国家保安に悪影響を与える行動の解明に役立つ場合に限り、たとえばその被害者に関するデータ、彼若しくは彼女の社会的若しくは職業的サークル、又は、犯罪又は国家保安に悪影響を与える行動が実行されたか準備された、特定された地理的範囲である場合でさえも、拡張できる。加えて、職務権限を有する当局はそのように保持されたデータへのアクセス権を、いかに指令 2002/58

が解釈されるべきかについての判例法から生じた条件を遵守して、供与されなければならない(この点、2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 118 項から第 121 項及び引用された判例法参照)。

166 とりわけ、上記第 115 項及び第 133 項から明らかなとおり、指令 20002/58 第 15 条(1)の下講じられた措置にしたがいプロバイダにより保持されたトラフィックデータ及び位置データへのアクセスは、原則として、それらのプロバイダが当該データを保持するよう命令された公共の利益の目的によってのみ正当化されることも追加されるべきである。したがって、とりわけ、そのようなデータへの通常の犯罪を訴追し処罰する目的での当該アクセスは、そのようなデータの保持が、重大犯罪との闘いの目的、さらには、国家保安を防護する目的により正当化されたいかなる場合にも許可されてはならない。しかしながら、比例性の原則にしたがい、上記第 131 項に言及されたとおり、重大な犯罪との闘いの目的で保持されたデータへのアクセスは、前項に言及されたそのようなアクセスに関係する実体的及び手続き的条件が遵守される場合には、国家保安を防護する目的により正当化できる。

167 この点、構成国が彼らの法令において、トラフィックデータ及び位置データへのアクセスが、当該データが指令 2002/58 第 5 条、第 6 条、第 9 条、又は第 15 条(1)と一貫性を有する方法でプロバイダにより保持された場合には、それらの同じ実体的及び手続き的条件に服することにより、重大な犯罪との闘い又は国家保安の防護の目的で許容される、と規定することは許容される。

168 上記検討結果のすべてに照らし、C-511/18 事件及び C-512/18 事件の質問 1 並びに C-520/18 事件の質問 1 及び質問 2 への回答は、憲章第 7 条、第 8 条、第 11 条及び第 52 条(1)に照らして読む指令 2002/58 第 15 条(1)は、第 15 条(1)に規定する目的で、予防措置として、網羅的かつ無差別のトラフィックデータ及び位置データの保持を規定する立法措置を排除するものであると解釈されなければならない。対照的に、第 15 条(1)は、憲章第 7 条、第 8 条、第 11 条及び第 52 条(1)に照らして読むと:

- 国家保安を防護する目的で、電子通信サービスのプロバイダに網羅的かつ無差別にトラフィックデータ及び位置データの保持を要求する命令への依拠を、関連する構成国が、真であり、かつ現存するか又は予見可能であることが示された国家保安に対する深刻な脅威に直面している場合で、そのような命令を課す決定が、裁判所又は独立したその決定が法的拘束力を有する行政機関による効果的な審査に服し、当該審査の目的がそれらの状況の一つが存在し、規定されなければならない状況及び防護手段が遵守されていることを検証することである場合であり、そして当該命令が厳格に必要な範囲に限定された期間にのみ出され、ただし当該期間は、脅威が持続すれば延長できる場合である状況において、許容する;

- 国家保安を防護し、重大犯罪と闘い、公共の保安への深刻な脅威を防止する目的で、トラフィックデータ及び位置データの標的を絞った保持であって、客観的かつ無差別の要素に基づき、関連する者の区別にしたがい、又は地理的基準を用いて、厳格に必要な範囲の長さに限定された、ただし延長可能な期間、に限定されたものを規定する;
- 国家保安を防護し、重大犯罪と闘い、公共の保安への深刻な脅威を防護する目的で、インターネット接続の接続元に割り当てられた IP アドレスの網羅的かつ無差別の、厳格に必要な範囲の長さに限定された保持を規定する;
- 国家保安を防護し、犯罪と闘い、公共の保安を防護する目的で、電子通信システムの利用者の市民識別同定に関係するデータの網羅的かつ無差別の保持を規定する;
- 重大犯罪と闘い、さらには、国家保安を防護する目的で、電子通信サービスのプロバイダに、その保有するトラフィックデータ及び位置データの迅速な保持を、指定された期間、要求する職務権限を有する当局の決定による命令であって、そのような命令を課す決定が、効果的な法務上の審査に服するものへの依拠を許容する、

立法措置を排除しないが、ただし、それらの措置は、明瞭で精緻な規則により、問題のデータの保持が、適用できる実体的及び手続き的条件の遵守を条件としており、問題の者が非違行為のリスクに対して効果的な防護手段を有していることを確保していることを条件とする。

C-511/18 事件の質問2 及び質問3

169 C-511/18 事件の質問 2 及び質問 3 において、照会元裁判所は、要するに、憲章第 7 条、憲章第 8 条、憲章第 11 条及び憲章第 52 条(1)に照らして読む指令 20002/58 第 15 条(1)が、電子通信サービスが、彼らのネットワーク上に、第一に、トラフィック及び位置データの自動化された分析及びリアルタイム収集、並びに、第二に、利用された端末機器の位置に関する技術的データのリアルタイム収集を許容する措置を実装することを義務づけるが、当該処理及び当該収集に関連する者に、それが通知される規定がない構成国法を排除するものと解釈されなければならないかどうかを問う。

170 照会元裁判所は、CSI 第 L. 851-2 条から L. 851-4 条に規定される諜報収集技術は、電子通信サービスのプロバイダに対してトラフィックデータ及び位置データを保持する特別な義務を課さないことを留意する。とりわけ、CSI 第 L. 851-3 条にいう自動化された分析については、照会元裁判所は当該処理の目的は、当該目的で確立された基準にしたがい、テロリストの脅威を構成するかもしれない繋がりを検出することであると理解する。CSI 第 L. 851-2 条にいうリアルタイム収集については、当該裁判所は、そのような収集が、テロリストの脅威

への繋がりを潜在的に有することが事前に識別された 1 人以上の者に排他的に関連することに留意する。同じ裁判所によると、それらの 2 つの技術は、テロリズムを防止する目的のみで実装でき、CSI 第 L. 8151-1 条及び第 L. 851-5 条にいうデータを包含できる。

171 予備的な点として、CSI 第 L. 851-3 条にしたがい、その規定する自動化された分析は、そのデータが分析される利用者が、識別されることを可能にしないという事実は、そのようなデータが「個人データ」として分類されることを排除しないことが留意されるべきである。当該条項の第 IV 項に規定する手続は、データの自動化された分析がテロリストの脅威があるかもしれないことを示した場合、そのデータにより懸念された者が、その後識別同定されることを可能とするので、自動化された分析の対象となったすべての者は、いまだ当該データから識別同定され得る。規則 2016/679 第 4 条(1)の個人データの定義にしたがい、就中、識別可能な者に関連する情報は、個人データを構成する。

トラフィック及び位置データの自動化された分析

172 CSI 第 L. 851-3 条からは、それが規定する自動化された分析は、要するに、電子通信サービスのプロバイダにより保持されたすべてのトラフィックデータ及び位置データであって、職務権限を有する国内当局の要請により、それらのプロバイダにより実施された、その当局の指定したパラメータを適用した絞り込み作業に呼応することが明らかである。そして、電子通信システムの利用者のすべてのデータは、もしそれがそれらのパラメータに合致すれば検証される。したがって、そのような自動化された分析は、関連する電子通信サービスのプロバイダにとっては、職務権限を有する当局を代理して行う、当該データの利用の様式で、自動化された運用の助力を得て、電子通信システムのすべてのユーサのトラフィックデータ及び位置データを対象とする、網羅的かつ無差別の、規則 2016/679 第 4 条(2)の意味における処理の作業を伴うと考えられなければならない。当該処理は、当該自動化された分析に引き続く、識別された者に関するデータのその後の収集であって、CSI 第 L. 851-3 条第 IV 項に基づき許可されたものとは別個のものである。

173 トラフィックデータ及び位置データのそのような自動化された分析を許可する構成国法は、指令 2002/58 第 5 条により確立された通信及び関連するデータの機密性を確保するという原則の義務から逸脱する。そのような法令は、その後そのようなデータがいかに利用されたかにかかわらず、憲章第 7 条及び第 8 条に謳われた基本権への干渉も構成する。最後に、本判決第 118 項に引用された判例法で述べられたとおり、そのような法令は憲章第 11 条で謳われた表現の自由の行使に対する萎縮効果を有するおそれがある。

174 さらには、主手続において問題となっているようなトラフィックデータ及び位置データの自動化された分析から生じる干渉は、それが、網羅的かつ無差別的に、電子通信システムを利

用している者のデータを対象とするので、とりわけ深刻である。この判断は、主手続で問題となっている構成国法から明らかなとおり、自動化された分析の対象となっているデータがオンラインで照会された情報の性質をあらわにすることを考えると、より正当化される。加えて、そのような自動化された分析は、網羅的に電子通信システムを利用したすべての者に適用され、結果として、その行為が、テロリストの行動との間接的あるいは遠い繋がりでさえもあることを示唆することができる証拠のない者についても適用される。

175 そのような干渉の正当化については、憲章第 52 条(1)により確立された、基本権の行使についてのいかなる制限も法に規定されなければならない、とする要件が、それらの権利への干渉を許容する法的根拠が、それ自体、関連する権利の行使についての制限の提供範囲を定義しなければならないことを、含意する(この点、2020 年 7 月 16 日付 *Facebook Ireland and Schrems* 判決 C-311/18 事件 EU:C:2020:559 第 175 項及び引用された判例法参照)。

176 加えて、本判決第 130 項及び第 131 項で喚起した比例性の要件、すなわちそれにしたがい個人データの保護からの逸脱及びそれの制限が厳格に必要な範囲でのみ適用されなければならない、とするものを満たすためには、保持されたトラフィックデータ及び位置データへの職務権限を有する当局によるアクセスを統制する国内法は、本判決第 132 項に引用された判例法から生じた要件を遵守しなければならない。とりわけ、そのような法令は、当局のそのようなデータへのアクセスが当該法令により追求される目的に合致することを要求することに限定され得ず、当該利用を統制する実体的及び手続き的条件を規定しなければならない(この点、2017 年 7 月 26 日付意見 1/15 *(EU-Canada PNR Agreement)*EU:C:2017:592 第 192 項及び引用された判例法を類推して参照)。

177 この点、本判決第 134 項から 139 項の判示にいう、網羅的かつ無差別のトラフィックデータ及び位置データの保持により構成されるとりわけ深刻な干渉及び当該データの自動化された分析により構成されるとりわけ深刻な干渉は、構成国が、真であり、かつ現存するかまたは予見可能であることが示された国家保安への深刻な脅威に直面している状況においてのみ、ただし、当該保持の期間が厳格に必要な範囲に限定されている場合に、比例性の要件を満たせることに留意すべきである。

178 前項にいうような状況において、電子通信システムのすべての利用者のトラフィックデータ及び位置データの自動化された分析の厳格に限定された期間の実装は、憲章第 7 条、第 8 条、第 11 条及び第 52 条(1)に照らして読む、指令 2002/58 第 15 条(1)から生じた要件に照らし正当化されると考えることができる。

179 そうはいっても、そのような措置が、国家保安を防護する、より具体的にはテロを防止するために現実に厳格に必要な範囲に限定されていることを本判決第 139 項に判示したとおりに

保障するためには、自動化された分析を許可する決定は、裁判所によるか又はその決定が拘束力を持つ独立した行政機関による効果的な審査に服し、当該審査の目的が、当該措置を正当化する状況が存在すること並びに規定しなければならない条件及び防護措置が遵守されているかどうかを検証するものであることが不可欠である。

180 この点、その種のデータ処理が基づく事前に確立されたモデル及び基準が、第一に、特定され、かつ信頼性が有り、テロリスト犯罪への参加の合理的な疑いがある個人を識別同定する成果を達成することを可能としており、第二に、非差別的であるべきことに留意すべきである(この点、2017 年 7 月 26 日付意見 1/15 *(EU-Canada PNR Agreement)*EU:C:2017:5 第 172 項参照)。

181 加えて、人種もしくは民族的な出自、政治的意見、宗教もしくは信条、労働組合員であること、又は健康または性生活に関する情報が、それら自体、かつその者の個別の行動にかかわらずテロリズムを防止するために関係することを前提とするモデル及び基準に基づき実施されたいかなる自動化された分析も、憲章第 21 条と相俟って読む憲章第 7 条及び第 8 条で保障された権利を侵害することになることに留意しなければならない。したがって、自動化された分析の目的で事前設定されたモデル及び基準であって国家保安への深刻な脅威を構成するテロリスト活動の防止を目的とするものは、当該機微なデータに単独で基づくことはできない。(この点、2017 年 7 月 26 日付意見 1/15 *(EU-Canada PNR Agreement)*EU:C:2017:5 第 165 項参照)。

182 さらには、トラフィックデータ及び位置データの自動化された分析は、一定の誤差の範囲を必然的に伴うため、自動化された処理に従って得られた陽性の結果は、関連する者に悪影響を与える、引き続くトラフィックデータ及び位置データのリアルタイム収集のような個別の措置が講じられる前に、そしてそのような措置は、自動化された措置による結果に単独でかつ決定的に基づくことはできないため、自動化されていない手段により個別の再審査に服さなければならない。同様に、事前設定されたモデル及び基準、それによる利用、そして利用されるデータベースが差別的ではなく、国家保安への深刻な脅威を構成するテロリスト活動を防止する目的に照らして厳格に必要な範囲に限定されていることを確保するため、これらの事前設定されたモデル及び基準並びに利用されたデータベースが信頼でき、最新版となっていることを確保するために、定期的な再審査が行われるべきである(この点、2017 年 7 月 26 日付意見 1/15 *(EU-Canada PNR Agreement)*EU:C:2017:5 第 173 項及び第 174 項参照)。

トラフィック及び位置データのリアルタイム収集

183 CSI 第 L. 851-2 条にいうトラフィックデータ及び位置データのリアルタイム収集は、「[テロリスト]の脅威に潜在的に繋がりを有すると事前に特定された者」に関して、個別に許可され

得る。さらに、その描写によると、かつ「許可に関係する者の人脈に属する 1 以上の者が、許可を受けた目的のために情報を提供する可能性があると信じる重大な理由がある場合、許可はこれらの人物それぞれに個別に付与することもできる」。

184 そのような措置の対象であるデータは、各国の職務権限を有する当局による、許可の期間中、継続してかつリアルタイムで、それらの者が通信をする相手方である者、彼らが利用する手段、彼らの通信の期間及び彼らの居住地移動の監視を可能にする。それは、オンラインで照会した情報の種類も明らかにする。全体としてみると、本判決第 117 項から明らかなとおり、当該データは、関連する者の私的生活に関して大変精緻な結論を引き出すことを可能にし、関連する個人のプロフィールを確立する手段を提供し、プライバシーへの権利の観点からは実際の通信の内容に勝るとも劣らない機微な情報である。

185 CSI 第 L. 851-4 条にいうデータのリアルタイム収集については、当該条項は、端末機器の位置に関する位置データが収集されリアルタイムで首相直轄部門に転送されることを許可する。そのようなデータにより、責任を有するその部門が、当該許可の期間中いつでも、利用された移動電話のような端末機器の位置を継続的かつリアルタイムで探知することを可能にすると思われる。

186 データの自動化された分析を許可する構成国法のように、そのようなリアルタイム収集を許可する構成国法は、指令 2002/58 第 5 条により確立された、電子通信及び関係するデータの機密保持を確保するための原則の義務から逸脱する。それは、したがって、憲章第 7 条及び第 8 条に謳われた基本権への干渉を構成し、憲章第 11 条で保障されている表現の自由の行使に対する萎縮効果をもたらすおそれがある。

187 端末機器の位置を探知することを可能にするデータのリアルタイム収集により構成される干渉は、当該データが職務権限を有する各国の当局に移動電話の利用者の移動を正確かつ永久に追跡できる手段を提供するため、特に深刻であると思われることを強調されなければならない。当該データが、したがって、とりわけ機微であると考えられる限り、そのようなデータへの職務権限を有する当局によるリアルタイムのアクセスと、当該データへの非リアルタイムのアクセスとは、前者がそれら利用者の事実上全体の監視を可能とする点においてより侵襲的であるので、区別されねばならない(2018 年 2 月 8 日付 ECtHR *Ben Faiza v. France* 判決 CE:ECHR:2018:0208JUD003144612 第 74 項を類推して参照)。当該干渉の深刻度は、関連する者のトラフィックデータにも拡張されると、さらに悪化する。

188 主手続で問題となっている構成国法により追求されるテロリズムの防止の目的は、その重要性を考えると、トラフィックデータ及び位置データのリアルタイム収集の形式での干渉を正当化する可能性があるが、そのような措置は、そのとりわけ侵襲的な性質を考慮に入れ、何

らかの形でテロリストの活動に関与していることを疑う有効な理由がある者についてのみ実装できる。その分類の外側の者については、当裁判所の判例法にしたがい、テロリストの活動のような特別な状況においてのみ、かつ、当該データが、個別の案件において、テロリズムとの闘いに対して効果的な寄与をするかもしれないことが推論できる客観的証拠がある場合に実行できる非リアルタイムのアクセスの対象者にのみなり得る(2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 119 項及び引用された判例法参照)。

189 加えて、トラフィックデータ及び位置データのリアルタイム収集を許可する決定は、構成国法に規定された客観的基準に基づかなければならない。とりわけ、当該法令は、本判決第 176 項に引用された判例法にしたがい、そのような収集が許可されうる状況及び条件を定義しなければならず、かつ、前項で指摘したとおり、テロリズムを防止する目的につながりを持つ者のみが、その収集の対象となることを規定しなければならない。加えて、トラフィックデータ及び位置データのリアルタイム収集を許可する決定は、構成国法に規定された客観的かつ非差別的な基準に基づかなければならない。実際に、それらの条件が遵守されることを確保するため、リアルタイム収集を許可する措置の実装は、裁判所又はその決定が拘束力を有する独立した行政機関のいずれかによる事前審査に服し、その裁判所又は機関が、就中、そのようなリアルタイム収集が厳格に必要な範囲の制限内のみで許可されることに納得しなければならないことが不可欠である(この点、2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 120 項参照)。十分に正当化される緊急時には、その審査は短時間で行われなければならない。

そのデータが収集又は分析された者への通知

190 トラフィックデータ及び位置データのリアルタイム収集を行う職務権限を有する構成国の当局は、適用される国内手続にしたがい、当該通知によりこれらの当局が責任を有する任務を危険にさらすおそれがなくなった限りで直ちに、関連する者に通知しなければならない。当該通知は、実際、影響のあった者が、憲章第 7 条及び第 8 条の下、それらの措置の対象となった彼らの個人データへのアクセスを請求し、かつ、適切な場合には、その個人データが正しく修正され、又は消去されることを得る権利、並びに憲章第 47 条第 1 項にしたがい、裁判所において効果的な救済を得る権利であって、当該権利が実際、規則 2016/679 第 79 条(1)と相俟って読む指令 2002/58 第 15 条(2)により明示的に保障されているものを行使することを可能にするために必要である(この点、2016 年 12 月 21 日付 *Tele2* 判決 C-203/15 及び C-698/15 併合事件 EU:C:2016:970 第 121 項及び引用された判例法、及び 2017 年 7 月 26 日付意見 1/15 *(EU-Canada PNR Agreement)*EU:C:2017:592 第 219 項及び第 220 項を類推して参照)。

191 トラフィックデータ及び位置データの自動化された分析の文脈において必要な通知につい

ては、職務権限を有する各国の当局は、関連する者個々人への通知をする必要はないものの、その分析に関係する一般的な性質の情報を公表する義務がある。しかしながら、自動化された分析を許可する措置に指定されたパラメータにデータが合致し、当該当局が関連する者を、彼又は彼女に関するデータをより深く分析するために、特定した場合、その者に個別に通知する必要がある。当該通知は、しかしながら、当該通知によりこれらの当局が責任を有する任務を危険にさらすおそれがなくなった限りで直ちになされなければならない(2017 年 7 月 26 日付意見 1/15 *(EU-Canada PNR Agreement)*EU:C:2017:592 第 222 項及び第 224 項を類推して参照)。

192 上記すべてに照らし、C-511/18 事件の質問 2 及び質問 3 の回答は、憲章第 7 条、第 8 条、第 11 条及び第 52 条(1)に照らして読む指令 2002/58 第 15 条(1)は、電子通信サービスのプロバイダが、第一に、就中、トラフィックデータ及び位置データの自動化された分析及びリアルタイム収集に依拠する手段を有し、第二に、端末機器が利用された位置に関する技術データのリアルタイム収集に依拠する手段を有することを義務づける構成国の規則を排除しないものと解釈されなければならず、その場合:

- 自動化された分析への依拠が、構成国が、それが真であり、かつ現存するか又は予見可能であることが示されている国家保安への深刻な脅威に直面しており、そして、そのような分析への依拠が裁判所又は、その決定が拘束力を有する独立した行政機関のいずれかによる効果的な審査に服す可能性があり、当該審査の目的が、当該措置を正当化する状況が存在しかつ、規定されなければならない条件及び防護手段が遵守されていることを検証するものである状況に限定され; かつその場合

- トラフィックデータ及び位置データのリアルタイム収集への依拠が、そのようなリアルタイム収集が厳格に必要な範囲内のみで許可されることを確保するために、何らかの形でテロリスト活動に関与していることを疑う有効な理由がある者に限定され、裁判所又は、その決定が拘束力を有する独立した行政機関のいずれかにより行われる事前審査に服す。十分に正当化される緊急時には、その審査は短時間で行われなければならない。

C-512/18 事件の質問 2

193 C-512/18 事件の質問 2 により、照会元裁判所は、指令 2000/31 の条項が、憲章第 6 条、第 7 条、8 条、第 11 条及び第 52 条(1)に照らして読むと、オンライン公衆通信サービスへのアクセスプロバイダ及びホスティングサービスプロバイダに対して、網羅的かつ無差別的な、就中、これらのサービスに関係する個人データを保持する義務を課す構成国法を排除するものと解釈されなければならないかどうかの確信を得ようとしている。

194 照会元裁判所は、そのようなサービスが、指令 2002/58 ではなく、指令 2000/31 の適用範囲に

入るとの見解を維持している一方、指令 2000/31 第 15 条(1)及び(2)は、その第 12 条及び第 14 条と相俟って読むと、それ自体、保持されるコンテントの生成に関係するデータについて、例外的な場合のみ逸脱できる、原則的禁止を確立していない、との考えである。しかしながら、当該裁判所は、憲章第 6 条、第 7 条、第 8 条及び第 11 条に謳われている基本権が必要的に遵守されなければならないことから、その考えが成り立つかどうか確信が持てない。

195 加えて、照会元裁判所は、その質問が、布告第 2011-219 号と相俟って読む LCEN 第 6 条に規定された保持する義務に関して投げかけられたことを指摘する。その下で関連するサービスプロバイダにより保持されなければならないデータは、就中、人の姓、名、関連する郵便番号、関連する電子メール又はアカウントのアドレス、パスワード、及び、契約又はアカウントへの継続利用料金が支払わなければならない場合、利用された支払いの種類、支払い参照番号、取引の金額及び日時のようなそれらのサービスを利用した者の市民識別同定に関するデータを含む。

196 さらに、保持する義務の対象であるデータは、加入者、接続、及び利用された端末機器の識別子、コンテンツに割り当てられた識別子、接続及び操作の開始と終了の日時並びにそのサービスに接続し、コンテンツを転送するために用いられたプロトコルを包含する。1 年間保持されなければならない当該データへのアクセスは、民事及び刑事の責任を統制する規定の遵守を確保するために、刑事及び民事手続の文脈において、並びに、CSI 第 L. 851-1 条が適用される諜報収集措置の文脈において要求できる。

197 この点、指令 2000/31 第 1 条(2)にしたがい、当該指令が、当該指令第 2 条(a)にいう情報社会サービスについての構成国法を近接させることに留意すべきである。

198 そのようなサービスが、たとえばインターネット若しくは通信ネットワークへのアクセスを提供するサービス又はホスティングサービスのような、隔地において、データの処理及び記録保存の電子機器により、サービスを受ける者の個別の要求に応じてかつ通常は対価を得るために提供されるそれを含むことは確かである(この点、2011 年 11 月 24 日付 *Scarlet Extended* 判決 C-70/10, EU:C:2011:771 事件第 40 項; 2012 年 2 月 16 日付 *SABAM* 判決 C-360/10 事件 EU:C:2012:85 第 34 項; 2016 年 9 月 15 日付 *Mc Fadden* 判決 C-484/14 事件 EU:C:2016:689 第 55 項;及び 2018 年 8 月 7 日付 *SNB-REACT* 判決 C-521/17 事件 EU:C:2018:639 第 42 項並びに引用された判例法参照)。

199 しかしながら、指令 2000/31 第 1 条(5)は、当該指令が指令 95/46 及び 97/66 の対象となる情報社会サービスに関連する問題には適用されないと規定する。この点、指令 2000/31 の前文第 14 項及び第 15 項から、情報社会サービスの文脈における通信の機密性及び個人データの処理に関する自然人の保護は指令 95/46 及び指令 97/66 のみにより統制されていることが明ら

かであり、後者は、その第 5 条において、機密性を保護するために、すべての様式の通信の傍受又は監視を禁じている。

200 通信の機密性及び個人データの保護に関係する質問は、指令 97/66 及び指令 95/46 をそれぞれ置き換える指令 2002/58 及び規則 2016/679 に基づき評価されなければならず、その指令 2000/31 が確保しようと意図した保護は、いかなる場合も指令 2002/58 及び規則 2016/679 上の要件を弱めることはできないことが留意されるべきである(この点、2008 年 1 月 29 日付 *Promusicae* 判決 C-275/06 事件 EU:C:2008:54 第 57 項参照)。

201 本判決第 195 項に言及された構成国法によりオンライン公衆通信サービスへのアクセスプロバイダ及びホスティングサービスプロバイダに課されたこれらのプロバイダに関係する個人データを保持することを命じる義務は、したがって、ー 独立弁論官が、彼の *La Quadrature du Net and Others* (C-511/18 及び C-512/18 併合事件 EU:C:2020:6)意見第 141 項において提案するとおり ー 指令 2002/58 又は規則 2016/679 に基づき評価されなければならない。

202 したがって、当該構成国法で包含されるサービスの提供が指令 2002/58 の適用範囲に入るかどうかにより、憲章第 7 条、第 8 条、第 11 条及び第 52 条(1)に照らして読む当該指令、特にその第 15 条(1)、又は、憲章の同じ条項に照らして読む規則 2016/679、特にその規則第 23 条(1)のいずれかにより、それは統制される。

203 今回の場合、欧州委員会がその書面による意見により表明するとおり、本判決第 195 項に言及される構成国法が適用されるサービスのうちいくつかは指令 2002/58 の意味における電子通信サービスを構成することが考えられるが、それは照会元裁判所が検証すべきである。

204 この点、指令 2002/58 は、指令 2002/58 第 2 条が言及し、電子通信サービスを「通常は対価を得るために提供され、放送に用いられる電気通信サービス及びネットワーク上の伝送サービスを含む、その全部又は主要部分が電子通信ネットワーク上の信号の搬送により構成されるサービス」と定義する指令 2002/21 第 2 条(c)に規定する条件を充足する電子通信サービスを対象にする。本判決第 197 項及び第 198 項に言及され、指令 2000/31 が対象とするような情報社会サービスについては、それらが、全部が、又は主として電子通信ネットワーク上の信号の搬送により構成される限り、それらは電子通信サービスである(この点、2019 年 6 月 5 日付 *Skype Communications* 判決 C-142/18 事件 EU:C:2019:460 第 47 項及び第 48 項参照)。

205 したがって、本判決第 195 項に言及された構成国法により対象となっていると思われるインターネット接続サービスプロバイダは、指令 2002/21 前文第 10 項において確認されているとおり、当該指令の意味における電子通信サービスである(この点、2019 年 6 月 5 日付 *Skype Communications* 判決 C-142/18 事件 EU:C:2019:460 第 37 項参照)。それは、ウェブベースの電子メールサービスにも、技術的レベルにおいて、電子通信ネットワーク上の信号の搬送を全

体として又は主として扱うので、当てはまり、それは、当該構成国法の対象にも入ると思われる(この点、2019 年 6 月 13 日付 *Google* 判決 C-193/18 事件 EU:C:2019:498 第 35 項及び第 38 項参照)。

206 憲章第 7 条、第 8 条、第 11 条及び第 52 条(1)に照らして読む指令 2002/58 第 15 条(1)から帰結する要件については、C-511/18 事件及び C-512/18 事件の質問 1 並びに C-520/18 事件の質問 1 及び質問 2 への回答の文脈においてなされた判示と評価のすべてに戻って参照するのが適切である。

207 規則 2016/679 から帰結する要件については、当該規則の目的が、就中、その前文第 10 項から明らかなとおり、欧州連合内における個人データの高いレベルの自然人の保護を確保するため、そして、そのために、一貫性があり、均質な、個人データの処理に関連するそのような自然人の基本的権利及び自由の保護のための規則の適用を欧州連合全域で確保することであることに留意すべきである(この点、2020 年 7 月 16 日付 *Facebook Ireland and Schrems* 判決 C-311/18 事件 EU:C:2020:559 第 101 項参照)。

208 この目的で、いかなる個人データの処理も、規則 2016/679 第 23 条において許容されている逸脱を停止条件として、当該規則第 II 章及び第 III 章にそれぞれ規定する個人データの処理及び関連する者の権利を統制する原則を遵守しなければならない。とりわけ、いかなる個人データの処理も、第一に当該規則第 5 条の原則にしたがい、そして第二に、当該規則第 6 条に列挙される適法性の条件を満たさなければならない(指令 95/46 に関する 2013 年 5 月 30 日付 *Worten* 判決 C-342/12 事件 EU:C:2013:355 第 33 項及び引用された判例法を類推して参照)。

209 より具体的に、規則 2016/679 第 23 条(1)については、当該条項は、指令 2002/58 第 15 条(1)と同様に、構成国が、自国の規定する目的のため、かつ立法措置により、同条項中で言及されている義務と権利を「その制限が基本的な権利及び自由の本質的部分を尊重するものであり、かつ、」追求される目的を「防護するために民主主義社会において必要かつ比例的な措置である場合には、」制限することを許容する。それに基づき採択されたいかなる立法措置も、とりわけ、当該規則第 23 条(2)に規定された特別な要件を遵守しなければならない。

210 したがって、規則 2016/679 第 23 条(1)及び(2)は、構成国に憲章第 7 条又はその他そこに謳われている保障を無視して、私的生活への尊重を低下させる権限を供与することができるものと解釈してはならない(指令 95/46 に関する 2003 年 5 月 20 日付 *Österreichischer Rundfunk and Others* 判決 C-465/00、C-138/01 及び C-139/01 併合事件 EU:C:2003:294 第 91 項を類推して参照)。とりわけ、指令 2002/58 第 15 条(1)の場合と同様、規則 2016/679 第 23 条(1)により構成国に供与された権限は、比例性の要件にしたがう場合にのみ行使でき、それによると個人データの保護に関する逸脱及び制限は、厳格に必要な場合にのみ適用されなければならない(指

令 95/46 に関する 2013 年 11 月 7 日付 *IPI* 判決 C-473/12 事件 EU:C:2013:715 第 39 項及び引用された判例法を類推して参照)。

211 したがって、C-511/18 事件及び C-512/18 事件の質問 1 並びに C-520/18 事件の質問 1 及び質問 2 への回答の文脈においてなされた判示と評価が、必要な変更を加えて、規則 2016/679 第 23 条に適用される。

212 上記に照らし、C-512/18 事件の質問 2 への回答は、指令 2000/31 は、情報社会サービスの文脈における通信の機密性及び個人データの処理に関する自然人の保護の分野には適用されず、そのような保護は、指令 20002/58 又は規則 2016/679 のいずれか適切な方により統制されると解釈されなければならない。憲章第 7 条、第 8 条、第 11 条及び第 52 条(1)に照らして読む規則 2016/679 第 23 条(1)は、オンライン公衆通信サービスへのアクセスプロバイダ及びホスティングサービスプロバイダに対し、就中、それらのサービスに関係する個人データの保持を網羅的かつ無差別に義務づける構成国法を排除するものであると解釈されなければならない

C-520/18 事件の質問3

213 C-520/18 事件の質問 3 により、照会元裁判所は、要するに、構成国の裁判所に、構成国法の下宣言するよう拘束されている違法性の宣言の時間的効力を制限する権限を与える当該構成国法の条項を、電子通信サービスのプロバイダに、－ 就中、国家保安の防護及び犯罪との闘いの目的を追求するために、－ 網羅的かつ無差別のトラフィックデータ及び位置データの保持を課す構成国法令に関して、当該法令が憲章第 7 条、第 8 条、第 11 条及び第 52 条(1)に不適合であるという事実のため、構成国の裁判所が、適用してよいかどうか確信を得ようとしている。

214 EU 法優越の原則は、構成国の法律に対する EU 法の優位性を確立する。当該原則は、したがって、構成国のすべての機関に対して、様々な EU の法律条項に完全な効力を与えることを義務づけ、構成国の法は、それら構成国の領域内でそれらの様々な条項により与えられた効果を弱めてはならない(1964 年 7 月 15 日付 *Costa* 判決 6/64 事件 EU:C:1964:66 593 頁及び 594 頁、2019 年 11 月 19 日付 *A. K. and Others (Independence of the Disciplinary Chamber of the Supreme Court)* 判決 C-585/18、C-624/18 及び C-625/18 併合事件 EU:C:2019:982 第 157 項及び第 158 項並びに引用された判例法)。

215 優越性原則に照らし、EU 法の要件を遵守するよう構成国法を解釈することができない場合、その管轄権の行使において EU 法の条項を適用することを求められた構成国の裁判所は、必要な場合、抵触する構成国の法令の条項の適用を、仮に事後に採択されたとしても、自らの意思で拒絶して、EU 法の条項に完全な効力を付与する義務に服し、当該裁判所が、そのよう

な構成国法の条項の法令又はその他の憲法的手段による事前の取消しを請求又は待機する必要はない(2010 年 10 月 22 日付 *Melki and Abdeli* 判決 C-188/10 及び C-189/10 併合事件 EU:C:2010:363 第 43 項並びに引用された判例法; 2019 年 6 月 24 日付 *Popławski* 判決 C-573/17 事件 EU:C:2019:530 第 58 項; 2019 年 11 月 19 日付 *A. K. and Others (Independence of the Disciplinary Chamber of the Supreme Court)*判決 C-585/18、C-624/18 及び C-625/18 併合事件 EU:C:2019:982 第 160 項)。

216 例外的な場合のみ、当裁判所は、法的確実性を最優先とする考え方に基づき、EU 法の規則の、それに反する構成国法についての先占効力の暫定的な停止を許容する。当裁判所によりなされる当該 EU 法の解釈の時間的効力へのそのような制限は、要求された解釈に対する具体的な判決についてのみ、認容される(この点、2012 年 10 月 23 日付 *Nelson and Others* 判決 C-581/10 及び C-629/10 併合判決 EU:C:2012:657 第 89 項及び第 91 項; 2020 年 4 月 23 日付 *Herst* 判決 C-401/18 事件 EU:C:2020:295 第 56 項及び第 57 項;及び 2020 年 6 月 25 日付 *A and Others (Wind turbines at Aalter and Nevele)*判決 C-24/19 事件 EU:C:2020:503 第 84 項並びに引用された判例法参照)。

217 EU 法の優越及び統一的な適用は、暫定的であったとしても、もし構成国の裁判所が、構成国の法の条項に対して、それらの条項が違反する EU 法との関係で、優越性を与える権限を有するとすれば、弱体化する(この点、2019 年 7 月 29 日付 *Inter-Environnement Wallonie and Bond Beter Leefmilieu Vlaanderen* 判決 C-411/17 事件 EU:C:2019:622 第 177 項及び用する判例法参照)。

218 しかしながら、当裁判所は、環境及び保護された場所についてのプロジェクトの事前の影響評価を行う EU 法上の義務に違反して採択された措置の適法性に関する事件において、もし国内法がそれを許容すれば、構成国の裁判所は、例外的に、そのような措置の維持が、真にかつ深刻な構成国内の電力供給における途絶の脅威であって、他の方法又は代替手段により、とりわけ域内市場の文脈で、救えないものを無効化する必要が上回るという考え方により正当化される場合で、その違反を是正するために厳格に必要な期間のみ継続する場合に限り、そのような措置の効果を維持できると判示した(この点、2019 年 7 月 29 日付 *Inter-Environnement Wallonie and Bond Beter Leefmilieu Vlaanderen* 判決 C-411/17 事件 EU:C:2019:622 第 175 項、第 176 項、第 179 項及び第 181 項参照)。

219 しかしながら、環境保護の特定分野におけるプロジェクトの事前影響評価のような手続的義務の違反と異なり、憲章第 7 条、第 8 条、第 11 条及び第 52 条(1)に照らして読む指令 2002/58 第 15 条(1)の不遵守は、前項で言及されている手続きと比較可能な手続により是正できない。主手続において問題となっている構成国法の効果の維持は、その法令が電子通信サービスのプロバイダに、EU 法に反し、かつそのデータが保持された者の基本的権利に深刻に干渉する義務を課し続けることを意味することになる。

220 したがって、照会元裁判所は、構成国法の下、行うよう拘束される、主手続で問題となっている構成国法に関する不適法宣言の時間的効力を制限する権限を自身に与えるその構成国法の条項を適用してはならない。

221 一方、当裁判所に提出された意見陳述書において、VZ、WY 及び XX は、質問 3 は暗示的にしかし必然的に、EU 法に反してトラフィックデータ及び位置データの網羅的かつ無差別な保持の結果得られた情報及び証拠の刑事手続における利用を EU 法が排除しているかどうかを問うものであると主張する。

222 この点、照会元裁判所に対する役に立つ回答を出すため、EU 法の現在の状態では、原則として、重大犯罪行為の嫌疑をかけられた者に対する刑事手続における、EU 法に反するそのような保持により得られた情報及び証拠の許容性及び評価に関係する規則を決定するのは、各構成国法のみであることを思い起こすべきである。

223 当裁判所は、問題に関する EU 法が欠缺している場合、手続き的自律性の原則にしたがい、EU 法から生じる個人の権利を防護することを意図する訴訟の手続き的規則を確立するのは、各構成国の自国の法秩序であるが、ただし、それらの規則は同様の国内訴訟を統制する規則よりも不利ではなく(均等の原則)、かつ EU 法により付与された権利の行使を事実上不可能にし、又は過剰に困難にするものではない(有効性の原則)ことを一貫して判示してきた(この点、2015 年 10 月 6 日付 *Târşia* 判決 C-69/14 事件 EU:C:2015:662 第 26 項及び第 27 項;2018 年 10 月 24 日付 *XC and Others* 判決 C-234/17 事件 EU:C:2018:853 第 21 項及び第 22 項並びに引用された判例法;及び 2019 年 12 月 19 日付 *Deutsche Umwelthilfe* 判決 C-752/18 事件 EU:C:2019:1114 第 33 項参照)。

224 均等の原則については、指令 2002/58 から帰結する要件に反して得られた情報及び証拠に基づき刑事手続の公判を行う場合、それらの手続を統制する構成国の法が、そのような情報及び証拠の許容性及び利用に関して、国内法に違反して得られた情報及び証拠を統制するそれよりも不利な規則を規定しているかどうかを決定するのは、当該公判を行う構成国の裁判所である。

225 有効性の原則については、情報及び証拠の許容性及び利用についての各国の規範の目的が、各国の法によりなされた選択にしたがい、違法に得られた情報及び証拠が、犯罪を実行したとの嫌疑を受けた者を不当に不利にすることを禁止することであることを留意すべきである。当該目的は、各国の法の下、そのような情報及び証拠の利用を禁止するだけではなく、そのような資料の評価及び重み付けを統制する各国の規則及び実務、又はそのような資料が違法かどうかを、量刑するために酌量することによっても達成できる。

226 とはいえ、当裁判所の判例法からは、EU 法の要件に反して得られた情報及び証拠を排除す

るかどうかを決定するに際し、とりわけ、当事者主義の違反のリスク、したがって、それらの情報及び証拠の許容性から必然的に生ずる公正な裁判を受ける権利を考慮しなければならないのが明らかである(この点、2003 年 4 月 10 日付 *Steffensen* 判決 C-276/01 事件 EU:C:2003:228 第 76 項及び第 77 項参照)。もし裁判所が、一方当事者が、裁判体が知識を有しない分野に関するが、事実認定に圧倒的影響を持つおそれがある証拠に効果的に意見を述べる立場にないと判断すれば、公正な裁判を受ける権利の侵害があると認定し、そのような侵害を回避するため当該証拠を排除しなければならない(この点、2003 年 4 月 10 日付 *Steffensen* 判決 C-276/01 事件 EU:C:2003:228 第 78 項及び第 79 項参照)。

227 したがって、有効性の原則は、構成国の刑事裁判所に対して、網羅的かつ無差別のトラフィック及び位置データの保持という手段により、EU 法に違反して得られた情報と証拠を、犯罪を実行したとの嫌疑を受けた者に対する刑事手続の文脈で、それらの者が当該情報及び当該証拠について効果的に意見を述べる立場になく、それらが、裁判体が知識を有しない分野に関係し、事実認定に圧倒的影響を持つおそれがあるものである場合、無視することを要求する。

228 上記に照らし、C-520/18 事件の質問 3 への回答は、構成国の裁判所は、電子通信サービスのプロバイダに、― 就中、国家保安を防護し、犯罪と闘うために ― トラフィックデータ及び位置データの網羅的かつ無差別の保持義務を課す構成国の法律であって、基本権憲章第 7 条、第 8 条、第 11 条及び第 52 条(1)に照らして読む指令 2002/58 第 15 条(1)に不適合であるものについて、構成国の法律の下そうするよう拘束されている不適法宣言の時間的効力を制限する権限を裁判所に付与する当該法律の条項を適用してはならない、ということになる。第 15 条(1)は、有効性の原則に照らして読むと、構成国の刑事裁判所が網羅的かつ無差別のトラフィックデータ及び位置データという手段により、EU 法に違反して得られた情報と証拠を、犯罪を実行したとの嫌疑を受けた者に対する刑事手続の文脈で、それらの者が当該情報及び当該証拠について効果的に意見を述べる立場になく、それらが、裁判体が知識を有しない分野に関係し、事実認定に圧倒的影響を持つおそれがあるものである場合、無視することを要求する。

費用

229 これらの手続は、主手続の当事者にとって、構成国の裁判所において中断している訴訟の途中段階であるので、費用についての決定は、それらの裁判所の問題である。当裁判所に意見陳述書を提出するための費用は、それらの当事者の費用を除き、回復不能である。

これらの理由により、当裁判所(大法廷)は以下の通り判決する:

1. 欧州連合の基本権憲章第 7 条、第 8 条、第 11 条及び第 52 条(1)に照らして読む欧州議会

及び理事会の 2009 年 11 月 25 日の指令 2009/136/EC により改正された電子通信分野における個人データの処理及びプライバシーの保護に関する欧州議会及び理事会の 2002 年 7 月 12 日の指令 2002/58/EC(プライバシー及び電子通信に関する指令)第 15 条(1)は、第 15 条(1)に規定する目的で、予防措置として、網羅的かつ無差別のトラフィックデータ及び位置データの保持を規定する立法措置を排除するものであると解釈されなければならない。対照的に、指令 2009/136 により改正された指令 2002/58 第 15 条(1)は、基本権憲章第 7 条、第 8 条、第 11 条及び第 52 条(1)に照らして読むと、以下の:

- 国家保安を防護する目的で、電子通信サービスのプロバイダに網羅的かつ無差別にトラフィックデータ及び位置データの保持を要求する命令への依拠を、関連する構成国が、真であり、かつ現存又は予見可能であることが示された国家保安に対する深刻な脅威に直面している場合で、そのような命令を課す決定が、裁判所又はその決定が法的拘束力を有する独立した行政機関による効果的な審査に服し、当該審査の目的がそれらの状況の一つが存在し、規定されなければならない状況及び防護手段が遵守されていることを検証することである場合であり、そして当該命令が厳格に必要な範囲に限定された期間にのみ出され、ただし当該期間は、脅威が持続すれば延長できる場合である状況において、許容する;

- 国家保安を防護し、重大犯罪と闘い、及び公共の保安への深刻な脅威を防止する目的での、トラフィックデータ及び位置データの標的を絞った保持であって、客観的かつ非差別的な要素に基づき、関連する者の区別にしたがい、又は地理的基準を用いて、厳格に必要な範囲の長さに限定された、ただし延長可能な期間、に限定されたものを規定する;

- 国家保安を防護し、重大犯罪と闘い、及び公共の保安への深刻な脅威を防護する目的で、インターネット接続の接続元に割り当てられた IP アドレスの網羅的かつ無差別の、厳格に必要な範囲の長さの期間に限定された保持を規定する;

- 国家保安を防護し、犯罪と闘い、及び公共の保安を防護する目的で、電子通信システムの利用者の市民識別同定に関係するデータの網羅的かつ無差別の保持を規定する;

- 重大犯罪と闘い、及び、さらに国家保安を防護する目的で、電子通信サービスのプロバイダに、その保有するトラフィックデータ及び位置データの迅速な保持を、指定された期間、要求する職務権限を有する当局の決定による命令であって、そのような命令を課す決定が、効果的な法務上の審査に服するものへの依拠を許容する、

立法措置を排除しないが、ただし、それらの措置は、明瞭で精緻な規則により、問題の

データの保持が、適用できる実体的及び手続き的条件の遵守を条件としており、関連する者が非違行為のリスクに対して効果的な防護手段を有していることを確保していることを条件とする。

2. 基本権憲章第 **7** 条、第 **8** 条、第 **11** 条及び第 **52** 条**(1)**に照らして読む指令 **2009/136** により改正された指令 **2002/58** 第 **15** 条**(1)**は、電子通信サービスのプロバイダが、第一に、就中、トラフィックデータ及び位置データの自動化された分析及びリアルタイム収集に、第二に、端末機器が利用された位置に関する技術データのリアルタイム収集に依拠できる手段を有することを義務づける構成国の規則を排除しないものと解釈されなければならず、その場合**:**

- 自動化された分析への依拠が、構成国が、真であり、かつ現存するか又は予見可能であることが示されている国家保安への深刻な脅威に直面しており、そして、そのような分析の依拠が、裁判所又はその決定が拘束力を有する独立した行政機関のいずれかによる効果的な審査の対象となる可能性があり、当該審査の目的が、当該措置を正当化する状況が存在し、かつ規定されなければならない条件及び防護手段が遵守されていることを検証するものである状況に限定され**;** かつその場合

- トラフィックデータ及び位置データのリアルタイム収集への依拠が、そのようなリアルタイム収集が厳格に必要な範囲内のみで許可されることを確保するために、何らかの形でテロリスト活動に関与していることを疑う有効な理由がある者に限定され、裁判所、又はその決定が拘束力を有する独立した行政機関のいずれかにより行われる事前審査に服す。十分に正当化される緊急時には、その審査は短時間で行われなければならない。

3. 域内市場における情報社会サービス、特に電子商取引の特定の法的側面に関する欧州議会及び理事会の **2000** 年 **6** 月 **8** 日の指令 **2000/31/EC(**「電子商取引に関する指令」**)**は、情報社会サービスの文脈における通信の機密性及び個人データの処理に関する自然人の保護の分野には適用されず、そのような保護は、指令 **2009/136** により改正された指令 **2002/58**、又は個人データの処理と関連する自然人の保護に関する、及び、そのデータの支障の無い移転に関する、並びに、指令 **95/46/EC** を廃止する欧州議会及び理事会の **2016** 年 **4** 月 **27** 日の規則**(EU)2016/679** のいずれか適切な方により統制されると解釈されなければならない。基本権憲章第 **7** 条、第 **8** 条、第 **11** 条及び第 **52** 条**(1)**に照らして読む規則 **2016/679** 第 **23** 条**(1)**は、オンライン公衆通信サービスへのアクセスプロバイダ及びホスティングサービスプロバイダに対し、それらのサービスに関係する個人データの保持を網羅的かつ無差別に義務づける構成国法を排除するものであると解釈されなければならない

4. 構成国の裁判所は、電子通信サービスのプロバイダに、－ 就中、国家保安を防護し、犯罪と闘うために － トラフィックデータ及び位置データの網羅的かつ無差別の保持義務を課す構成国の法律であって、基本権憲章第 **7** 条、第 **8** 条、第 **11** 条及び第 **52** 条**(1)** に照らして読む指令 **2002/58** 第 **15** 条**(1)**に不適合であるものについて、当該法律の下そうするよう拘束されている不適法宣言の時間的効力を制限する権限を裁判所に付与する当該法律の条項を適用してはならない。第 **15** 条**(1)**は、有効性の原則に照らして読むと、構成国の刑事裁判所が網羅的かつ無差別のトラフィック及び位置データという手段により、**EU** 法に違反して得られた情報と証拠を、犯罪を実行したとの嫌疑を受けた者に対する刑事手続の文脈で、それらの者が当該情報及び当該証拠について効果的に意見を述べる立場になく、それらが、裁判体が知識を有しない分野に関係し、事実認定に圧倒的影響を持つおそれがあるものである場合、無視することを要求する。

[署名]

2022 Printed in Japan
ISSN 2432-6089
法と情報雑誌　第 7 巻第 1 号（通巻第 47 号）（第 3 分冊）
The Law and Information Magazine vol.7 no.1 (consecutive no.47) part 3

2022 年 1 月 10 日発行
発行者　夏井高人
発行所　法と情報研究会（代表 夏井高人）
東京都千代田区神田駿河台 1－1
学校法人明治大学研究棟
（非売品）