EU刑事司法指令（LED）における個人情報保護

――「適法性」・「目的特定」・「目的拘束」原則を中心に――

韓　　修　玭

一　はじめに
　㈠　日本法の現況
　㈡　EU個人データ保護法制と筆者の関心
二　「適法性」原則――法律上の根拠と法律の質
　㈠　LEDにおける「適法性」の意味
　㈡　法的根拠の質的要件
　㈢　小　括
三　「目的特定」の原則――法執行目的の具体的特定
　㈠　LED第1条第1項の目的列挙と「特定された」目的の区別
　㈡　「明確にされた」目的の実現態様
　㈢　小　括
四　「目的拘束」の原則――目的変更の統制
　㈠　GDPRとLEDにおける目的変更の統制の相違
　㈡　「捜査」目的と「訴追」目的の分離：*Inspektor*判決①
　㈢　LEDからGDPRへの目的変更：*Inspektor*判決②
　㈣　GDPRからLEDへの目的変更
　㈤　小　括
五　おわりに

一　はじめに

現代社会において、国家による個人情報の取得・利用等は、もはや例外的事態ではなく、不可欠な要素となっている。なかでも警察は、犯罪の予防・捜査・訴追という国家の責務を根拠として、一般市民に関する膨大な

情報を恒常的に取得・保有する立場に置かれている。このような警察による情報の取得・利用等は、国家権力と個人の自由とが最も鋭く交差する領域のひとつであり、いかなる法的根拠のもとで取得され、いかなる目的に供され、いかなる統制に服するのかという問いは、個人情報保護法制の核心に位置する問題である。しかしながら、日本の現行法制においては、この問いに対する答えが十分に整備されているとは言い難い。

㈠　日本法の現況

日本における警察による個人情報の利用等は、原則として一般行政部門と同様に個人情報保護法の下に置かれている[1)]。現行法は、行政機関等が個人情報を保有するにあたって、法令上の事務遂行に必要な場合に限りこれを保有することができ、その目的を可能な限り特定しなければならず、目的達成のために必要な範囲を超えて保有してはならない旨を規定する（第61条）。また、保有個人情報は、法令に基づく場合を除き、目的外に利用・提供されてはならない（第69条第１項）。さらに、情報主体には原則として開示・訂正・利用停止請求権が認められており（第76条、第90条、第98条）、行政機関が個人情報ファイルを新たに保有し、又は変更する際には個人情報保護委員会への事前通知が義務づけられ（第74条）、開示請求に対して行政機関の長等が応じる義務も定められている（第78条）。

法執行活動に対しても、保有等の制限・正確性の確保・安全管理措置・利用および提供の制限・漏えいに対する罰則といった一般規定は、原則として適用されると解される[2)]。しかし、法執行活動における個人情報の取得・利用等は、個人情報保護法の枠内で完結するものではない。警察による個人情報の取得は、具体的な犯罪捜査の場面では刑事訴訟法に従って行われる。一方で、犯罪予防や危険防止といった行政警察活動の一環として行われる場面では、取得後の保存・分析・共有の段階においては、警察内

1)　田村正博『全訂 警察行政法解説［第三版補訂版］』（東京法令出版、2026年１月）329-330頁。
2)　同上。

部の規則および実務運用に大きく依存している。田村の整理によれば、日本の法執行分野における個人情報の取得・利用等は、個人情報保護法、刑事訴訟法、一般行政法およびアーキテクチャによる統制が併存しているとされる[3)]。

このうち、個人情報保護法は法執行活動に対して多くの例外規定を設けている。まず、犯罪の捜査、公訴の提起若しくは維持のために作成し、又は取得する個人情報ファイルについては、行政機関による個人情報保護委員会への事前通知義務が適用されない（第74条第 2 項第 2 号）。また、仮に開示請求がなされた場合であっても、犯罪の予防・捜査、公訴の維持、刑の執行その他公共の安全と秩序の維持に支障を及ぼすおそれがある情報については、不開示情報として開示を拒否することができる（第78条第 5 項）。さらに、刑事事件若しくは少年の保護事件に係る裁判、司法警察職員が行う処分、刑若しくは保護処分の執行等に係る保有個人情報については、情報主体の開示・訂正・利用停止請求に関する規定を含む第 5 章第 4 節の規定が一括して適用されない（第124条第 1 項第 1 号）。警察の法執行活動において保有する個人情報に関しては、情報主体による諸請求は広範に排除されている[4)]。

このような構造の下で、外部監督がいかなる程度においてかかる規律の空白を補完し得るかが問題となる。個人情報保護委員会が行政機関等に対して行使し得る権限は、第156条から第159条に規定される資料提出・説明要求および実地調査、指導・助言、勧告、ならびに勧告に基づく措置報告要求にとどまる。民間事業者に対して認められている一般的命令権に相当する権限は、行政機関等に対しては付与されていない。では、国家公安委員会などによる監督が実効的に機能しているかというと、必ずしもそうではない。国家公安委員会は、市民的統制を担う機関として位置づけられているが、警察DNA型データベースに関しては、小山が指摘するとおり、

3） 田村正博「警察における情報の取得及び管理に対する行政法的統制」産大法学50巻 1 ・ 2 号（2017年 1 月）70–77頁。なお、同論文は個人情報保護法2022年改正前のものである。

4） 田村・前掲注 1 ）325、330頁。

国家公安委員会は監視機関としての機能を果たしていないとされる。警察が保有する個人情報の利用等について、国家公安委員会において審議・報告がなされた形跡は乏しく、実質的な監視が及んでいるとは言い難い[5]。名古屋高裁判決も、「国家公安委員会等による監視も到底十全であるとはいえない」[6]と指摘するところである。結局のところ、いずれの機関による統制も実効性を欠いており、十分な保護を提供し得ていない。

㈡　EU個人データ保護法制と筆者の関心

法執行分野は、民間部門および一般行政部門とは異なり、個人の権利保障と公共の安全・秩序の維持という、衝突する二つの要請が存在する。その分野の特殊性ゆえに個人情報保護が弱まらざるを得ない側面があることは確かである。そのため、問題の本質は、法執行という分野の特殊性ゆえに権利保障を断念するか否かにあるのではなく、特殊性を理由とした一般的権利保障の修正の後に、その空白を埋めるべき仕組みをどのように構想できるのかにある。

かかる問題に対し、EUの法制はひとつの制度的回答を示している。EUはまさにこの点に着目し、一般データ保護規則（以下、「GDPR」という。）[7]とは別個にEU刑事司法指令（以下、「LED」という。）[8]を制定することで、

5）　小山剛「憲法上の個人情報保護についての基本的な考え方・補論」意見書（2022年 8 月10日） 8 頁（名古屋共同法律事務所、https://nagoya-kyodo.com/media/20220810_Prof.koyama.pdf）。

6）　名古屋高判令和 6 年 8 月30日法教531号111頁。

7）　Regulation（EU）2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC（General Data Protection Regulation）

8）　Directive（EU）2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

法執行の特殊性を前提としつつも権利保護の実質を確保するための、刑事司法に特化した規律体系を構築した。一般規律の適用範囲から法執行分野を除外させ、「犯罪捜査の特殊性に鑑み、別の特別法によって規律」[9] している。この点はLEDの前文規定から明らかである。LED前文第12項[10] は、かかる規律は、これらの活動の特殊な性質を尊重するものでなければならないと述べる。EUの法制は、日本のように法執行活動の「特殊性」を理由に保護を後退させるのではなく、当該特殊性を織り込んだうえで別建ての保護設計を与えるという制度構造を採用する点に特徴がある。この並列構造は、刑事司法領域の個人情報保護を「一般法の例外」として位置づけるのではなく、独自の規範構造として把握するための視角を与えるものといえる。

LEDに関する日本の先行研究では、LEDそれ自体が独立の分析対象として検討されるのではなく、EUの個人データ保護法令群を体系化した上で他の関連立法との法適用関係を明確化する文脈において取り上げられている[11) 12) 13)]。とりわけGDPRの制度説明の文脈で、法執行目的の取得・利用等がGDPRの適用除外であることを示す参照点として位置づけられる傾向が強く、さらに、LEDはプラットフォームによる情報提供[14] や顔認識[15]、

9） 夏井高人「EUの個人データ保護法令と他の関連立法との関係に関する検討」法律論叢第91巻第 4 ・ 5 合併号（2019年 1 月）168頁。

10） LED, recital 11. “... respecting the specific nature of those activities.”

11） 夏井・前掲注 9 ）165頁以下。

12） 石井夏生利『EUデータ保護法』（勁草書房、2020年 1 月）。

13） 宍戸常寿「安全・安心とプライバシー」論ジュリ第18号（2016年）56頁以下。

14） 小向太郎「捜査機関による第三者保有の個人情報に対するアクセスと本人保護」情報通信政策研究第 4 巻第 1 号（2020年）63頁以下。

15） 水野陽一「刑事手続におけるAI実装と個人情報保護に関する諸問題――刑事捜査・訴追機関の情報収集・処理に関するものを中心に――」北九州市立大学法政論集第47巻第 1 ・ 2 号併合（2019年12月）75頁以下。

第三国移転・刑事司法共助[16) 17)]等とのかかわりで必要に応じて言及される。

日本の先行研究においてLEDは、主にGDPR体系説明の付属軸として、又は特定争点とのかかわりから必要に応じて呼び出される傾向を示している。これに対して、筆者の関心は、法執行分野における国家による個人情報の取得・利用等において、いかなる最低限の基準が憲法上要請されるのか、という点にある。

ところで、EUにおける個人データの取得・利用等の規律に関する憲法的基盤の一つは、EU基本権憲章第 8 条第 2 項である。同項前段は、個人データは、特定された目的のために、当事者の同意又は法律に定めるその他の適法な根拠に基づいて、公正に取得・利用等をされなければならないと規定し、取得・利用等の法的根拠の存在と目的の特定を憲章次元において要請している。この要請は二次法であるGDPRやLEDにおいても明示されている。そこで本稿では、まず、第二章において、そのような共通の基盤の上に立つLEDの基本原則のうち、諸原則の根底にある「適法性」原則に着目し、法執行分野における個人データの取得・利用等がいかなる法的根拠によって正当化されるのか、またその法的根拠に対していかなる質的要請が課されるのかを検討する。そして、第三章および第四章では、これを受けて「目的特定」・「目的拘束」原則を取り上げ、目的の具体化がいかなる意味で必要性・比例性審査および事後的統制の出発点となるのかを明らかにするとともに、目的変更の統制の構造を検討する。なお、LEDはEU加盟国に国内法化を求める指令（Directive）であるが、本稿は、各加盟国の実施法制を網羅的に整理したり、個別加盟国の実施差それ自体を比較対象としたりするものではない。検討の対象は、あくまでLEDの文

16）星周一郎「GDPRと刑事司法指令、PNR指令の相関」ジュリ第1521号（2018年）20頁以下；星周一郎「テロ防止のための捜査法」前田雅英編集代表『現代危機管理論：現代の危機の諸相と対策』（立花書房、2017年）116頁以下；星周一郎「外国機関との情報共有」山本龍彦＝横大道聡＝大林啓吾＝新井誠編集『入門・安全と情報』（成文堂、2015年）43頁以下。

17）横田明美「EU刑事司法指令のドイツにおける国内法化と十分性認定：監督機関に着目して」情報法制研究第 9 号（2021年）92頁以下。

言・構造およびその解釈を通じて把握される、EU法制上の共通した考え方にある。

二 「適法性」原則――法律上の根拠と法律の質

LEDは、GDPRとは異なり、個人データの取得・利用等[18]が何らかの一般的な正当化根拠によって広く許容されると考えるのではなく、法執行領域における取得・利用等を、「適法性」原則、すなわち、EU法又は加盟国法上の根拠に結び付けて正当化する。LEDは、同意、契約、正当な利益など複数の法的根拠を並列的に認めるGDPRとは異なり、所管官庁による個人データの取得・利用等が、同指令第1条第1項に掲げられた目的のために遂行される任務に必要であり、かつEU法又は加盟国法に基づく場合に限って適法とするのである。

㈠ LEDにおける「適法性」の意味

先述のとおり、個人データの取得・利用等に法的根拠を要求することは、一次法（憲章第8条第2項）からの要請である。この要請は、GDPRおよびLEDにおいて「適法性」原則[19]として具体化されている。同原則は「公

18） LED第3条第2号は、「processing」を、個人データ又は個人データの集合に対して行われるあらゆる作業又は一連の作業をいうものと定義し、その例として、取得、記録、編成、構造化、保存、修正・変更、検索、参照、利用、送信による開示、頒布その他の提供、照合・結合、制限、消去又は破棄を挙げている。本稿では、区別する必要がない限り、叙述の便宜上、これらを包括して「取得・利用等」とする。

19） GDPR第5条第1項およびLED第4条第1項のいずれにおいても、諸原則の冒頭には、「適法性」を求める要請が置かれている。GDPRにおける基本原則を定める第5条は、第1項において、各原則を「適法性」（“lawfulness”）、「公正性」（“fairness”）、「透明性」（“transparency”）、「目的拘束」（“purpose limitation”）、「データの最小化」（“data minimisation”）、「正確性」（“accuracy”）、「記録保存の制限」（“storage limitation”）、「完全性および機密性」（“integrity and confidentiality”）を、さらに第2項において「責任性」（“accountability”）を括弧書きにより掲げている。これに対し、LED第4条はGDPRのように各原

正性」原則と並んで、LED第 4 条およびこれに対応するGDPR第 5 条が掲げるデータ保護原則の一つを構成し、他の個人データ保護原則を基礎づける基本的原則として位置づけられる。両原則は、他のあらゆる個人データ取得・利用等に関する原則を「包摂し、生成する」基本的な原則として位置づけられている[20]。EUデータ保護法制における「適法性」原則は、一般的な適法性ないし法治主義の原理から導かれると理解される。これは、広義には、個人データの取得・利用等はすべて法に基づき正当化されるべきであり、そのことは同時に、個人データ保護原則一般の遵守を要請するものと説明される[21]。

「適法性」原則に含まれる要請の具体的内容は、LED第 8 条において定められている。同条第 1 項によれば、個人データの取得・利用等が適法とされるのは、①所管官庁が第 1 条第 1 項所定の目的（法執行目的）を遂行するために必要な場合に限り、かつその必要性の範囲内であること、②当該取得・利用等がEU法又は加盟国法に基づいて行われること、という要件を充足する場合である。これは、法執行目的による個人データの取得・利用等が、私生活および個人データ保護に関する基本権への介入を構成し得る以上、当該取得・利用等が法律に基づき、正当な目的を追求し、その達成のために必要かつ比例的な範囲に限定されなければならないからである[22]。すなわち、LEDにおける適法な取得・利用等とは、抽象的な公的利益の存在を意味するのではなく、法により任務を付与された機関が、その任務の範囲内で、権限行使として個人データを取得・利用等することを前提とする。もっとも、LEDは、加盟国の憲法秩序に由来する要請を害しない限りで、法的根拠が常に議会制定法の形式を要するものではない

則を括弧書きで命名する形式を採っていない。

20）Maria Tzanou, “Article 8 Lawfulness of processing” in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (OUP 2024, ebook edn), pp. 347-348.

21）Ibid.

22）Tzanou (n 20) 355.

としている[23)]。

これに対して、GDPRにおける法的根拠は、データ主体の同意、契約、法的義務、公的業務、生命に関する重大な利益、正当な利益が挙げられる。たしかに憲章第 8 条第 2 項はデータ主体の同意による個人データの取得・利用等を認めている。しかし、LEDでは、GDPRで定義される同意を法的根拠として挙げていない。LEDは、その前文規定からして、この意味でのデータ主体の同意が所管官庁の個人データの取得・利用等に対する法的根拠を提供してはならないことを明示する[24)]。LED上想定される活動には、捜査・起訴はもちろん、事案が犯罪に該当するか否かですら事前に確定しない局面での警察活動、デモ・大規模スポーツイベント・暴動等の状況下で行使される強制権限、公共の安全や社会の基本的利益に対する脅威を防止するための秩序維持活動などが含まれ得る[25)]。これらの任務が法令により所管官庁に制度的に付与されている場合、当該官庁は、自然人

23） LED前文33項は、同指令が加盟国法、法的根拠又は立法措置に言及する場合であっても、それが必ずしも議会によって採択された法律を要するものではないとする。このような理解はGDPRにも共通しており、GDPR第 6 条第 2 項および前文41項にも類似の規定がみられる。これは、加盟国ごとの憲法秩序および法源形式の多様性に配慮したものと解される。アイルランドデータ保護委員会によれば、GDPR前文第41項の存在は、GDPRが加盟国の多様な憲法秩序を認めているためであると説明する。したがって、GDPR上の適法性根拠の一つである「法的義務」は、法律、委任立法・下位法令、又は慣習法上の要件に基づくことができると説明する。Data Protection Commission, “Guidance Note: Legal Bases for Processing Personal Data”, p. 14, “What Constitutes a Legal Obligations?”.

24） LED, recital 35. “... . The performance of the tasks of preventing, investigating, detecting or prosecuting criminal offences institutionally conferred by law to the competent authorities allows them to require or order natural persons to comply with requests made. In such a case, the consent of the data subject, as defined in Regulation（EU）2016/679, should not provide a legal ground for processing personal data by competent authorities. Where the data subject is required to comply with a legal obligation, the data subject has no genuine and free choice, so that the reaction of the data subject could not be considered to be a freely given indication of his or her wishes. ... .”

25） Tzanou（n 20）358.

に対し、自らが行った要請に従い、又は命令に服するよう求め、あるいは命ずることができる[26]。このような状況の下では、データ主体は真に自由な選択を行い難く、応答を求められる強制的状況に置かれ得るため、その「同意」（より厳密には所管官庁への応答）を自由意思に基づく意思表示として評価することは困難である[27][28]。

さらに、このような理解は、LEDの内部構造のみによって支えられるものではない。そもそも、EUにおいても、法の支配の一要請として、公的機関の行為は法の下で、かつ法の範囲内で行われなければならない。すなわち、公的機関の行為には法的根拠が必要であり、当該機関は付与された権限の範囲内で行為しなければならず、権限逸脱（ultra vires）は許されない。また、当該行為は、個別の法的根拠が定める手続規則に従い、基本権およびEU法上の一般原則を含む上位規範にも適合するものでなければならない[29]。このような法的根拠の要求は、個人に対して国家作用の予見可能性を保障するとともに、裁判所が当該行為の適法性を審査するための基準を提供するという意義を有する[30]。公的機関による個人データ取得・利用等も、法により付与された任務の遂行およびそれに伴う権限行使として行われる限り、以上の意味における公権力作用として理解されるべきである。この点はGDPRにおいても、公的機関による取得・利用等について同様の方向性を見て取ることができる。すなわち、GDPR第6条第1項(f)でいう「正当な利益」は、公的機関がその任務を遂行する場合には適用されない。また、同項(c)「法的義務」及び(e)「公益又は公的権限行使に基づく職務遂行」に基づく取得・利用等については、同条第3項が、

26）LED, recital 35（n 24）.

27）Ibid.

28）Tzanou（n 20）345.

29）Herwig C. H. Hofmann, “General Principles of EU Law and EU Administrative Law” in Catherine Barnard and Steve Peers（eds）, *European Union Law*（3rd edn, OUP 2020）, p. 223.

30）Paul Craig, “The Rule of Law” in *Rule of Law in Europe: Perspectives from Practitioners and Academics*（European Judicial Training Network, 2020）pp. 10–11.

その根拠をEU法又は加盟国法に求めている。このような方向性は、*Schrems II*判決[31]にも見て取ることができる。すなわち、同判決は、個人データ保護権に対する制限が許容されるためには、その法的根拠自体が権利制約の範囲を具体的に定めることを要求している。

以上のように、LEDは、所管官庁による個人データ取得・利用等の適法性について、GDPRのように同意・契約・正当な利益等の複数の法的根拠を併置するのではなく、EU法又は加盟国法に基づくことを唯一の取得・利用等の根拠として位置づけている。

㈡　法的根拠の質的要件

1　「法律の質」

とはいえ、国内法上の根拠が形式的に存在するというだけでは、当該データ取得・利用等が直ちに正当化されるわけではない。先述のとおり、LED第 8 条第 1 項は、取得・利用等が法執行目的の遂行に「必要な場合」に限り、かつその「必要性の範囲内」で行われることを要求している。さらに、加盟国法が備えるべき最低限の要件を定める同条第 2 項は、単に「所管官庁が行為に法的根拠を有する」という形式的要請にとどまらず、加盟国法が少なくとも、取得・利用等の目標および目的、取得・利用等される個人データの範囲を具体的に特定することを求める。したがって、第三章で扱う抽象的な「治安維持」という目的の掲示のみでは足りない[32]。この点、単に所管官庁が行為するに当たって法的根拠を有していなければならないという意味にとどまるものではなく、法律それ自体の質（quality of law、以下「法律の質」という）に関する要件をも設定するものとして理解される[33]。

31）　CJEU, *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*（*Schrems II*）（C-311/18）, Judgment of 16 July 2020, ECLI: EU: C: 2020: 559, paras. 174-175.

32）　Tzanou（n 20）356-357.

33）　Bart van der Sloot, “Article 4 Principles relating to processing of personal data” in Eleni Kosta and Franziska Boehm（eds）, *The EU Law Enforcement*

LEDの「法律の質」に関する欧州司法裁判所（CJEU）の判例は、現時点では、主として目的原則、厳格必要性および比例性の問題を中心に展開されている。一例として*Ministerstvo na vatreshnite raboti*判決[34]がある。同判決は、故意の公訴対象犯罪について被疑者又は被告人とされたすべての者から、写真、指紋およびDNAを取得するブルガリア法制が問題となった事案である。CJEUは、まず、生体データおよび遺伝データ等の特別な種類の個人データの取得・利用等について、厳格必要性および適切な保障措置のもと、EU法又は加盟国法によって認められている場合に限り許されると定めるLED第10条(a)を、基本権の制約が法律によって定められ、かつ比例性原則に従わなければならないとする憲章第52条第１項に照らして解釈した。すなわち、犯罪対策や法秩序の維持を目的とする捜査活動のために所管官庁が生体データおよび遺伝データを取得・利用等することは、加盟国法が当該取得・利用等を認める、十分に明瞭であり、かつ権限行使の対象・条件・範囲を画定する法的根拠を含む限り、同号の意味において「加盟国法によって認められる」（authorised by Member State law）ものに当たると判示した。さらに、LED第10条を、第４条第１項(a)から(c)までおよび第８条第１項・第２項と併せて解釈し、生体データおよび遺伝データの体系的取得を定める国内法は、所管官庁が、当該取得が具体的目的の達成のために厳格に必要であること、また、その目的がデータ主体の権利及び自由に対してより侵害性の少ない方法によっては達成し得ないことを確認し、かつ示す義務を課していない限り、LED第10条に反すると判示した。このように、同判決は、特別な種類の個人データの取得・利用等を可能にする加盟国法について、単に形式的な根拠の存在にとどまらず、当該取得・利用等を認める法的根拠の意味内容が明瞭であり、かつ権限行使の対象・条件・範囲が十分に画定されていること、および厳格必要性の判断を可能にする規律内容を要求するものとして位置づけることができる。

Directive (*LED*)*: A Commentary* (OUP 2024, ebook edn), p. 289.

34）CJEU, *Ministerstvo na vatreshnite raboti*, C-205/21, Judgment of 26 January 2023, ECLI: EU: C: 2023: 49, paras. 76, 118, 124-127, 130-135.

2　EUにおける「法律の質」の内容

このような要請は、EUが、「法律の質」に関する一連の要件を展開してきた欧州人権裁判所（ECtHR）の判例法理を踏襲しているものと説明される[35]。憲章制定前の、欧州人権条約（以下、「条約」という）第 8 条[36] 第 2 項の定める「法律に従って」要件の解釈を通じてECtHRが形成してきた判例理論――明確性・予見可能性・アクセス可能性、および濫用を防止する制度的保障を要請する枠組み――に基づいたと解される[37]。以下では、EU法における「法律の質」要件の前提をなすものとして、ECtHRの判例法理を概観する。

⑴　まず、法執行領域に関するものではないが、欧州人権条約上の「法律の質」を示す典型例として、「サンデー・タイムズ判決」[38] がある。同判決は、表現の自由に対する介入が「法律によって定められている」といえるためには、成文法・不文法を問わず、法律が接近可能（accessible）であり、その効果が予見可能（foreseeable）であることを要するとした[39]。

⑵　しかし、「接近可能性」および「予見可能性」を法執行領域においてそのまま貫徹することは必ずしも容易ではない。とりわけ秘匿的監視措

35）　van der Sloot（n 33）289-290.

36）　欧州人権条約第 8 条（私生活および家族生活の尊重を受ける権利）
「1　すべての者は、その私的および家族生活、住居ならびに通信の尊重を受ける権利を有する。
2　この権利の行使に対しては、法律に基づき、かつ、国の安全、公共の安全もしくは国の経済的福利のため、また、無秩序もしくは犯罪の防止のため、健康もしくは道徳の保護のため、または他の者の権利および自由の保護のため、民主的社会において必要なもの以外のいかなる公の機関による介入もあってはならない。」（欧州評議会「ヨーロッパにおける人権および基本的自由の保護のための条約」）

37）　van der Sloot（n 33）289-290; Tzanou（n 20）353.

38）　ECtHR, *The Sunday Times v. the United Kingdom*（*No. 1*）, no. 6538/74, Judgment of 26 April 1979, Series A no. 30.

39）　江島晶子「表現の自由と民主的社会：裁判所侮辱法に基づく新聞記事差止命令：サンデー・タイムズ判決（The Sunday Times v. the United Kingdom）［1979、全員法廷］」戸波江二ほか編『ヨーロッパ人権裁判所の判例Ⅰ』（信山社、2008年）354-356頁参照。

置は、その実効性を確保するために、秘密性および被監視者にとって予見不可能であることを不可欠とするからである[40]。それゆえ、実効的な権利保障のためには、当該措置を根拠づける法は、法治主義に適合する「法律の質」を備えなければならない。

法執行領域における「接近可能性」および「予見可能性」について判示したのが、「マローン判決」[41] である。本件は、イギリス警察が捜査の一環として申立人の電話を盗聴し、あわせてメータリングを行ったことが、条約 8 条の保障する私生活および通信の秘密に対する介入として適法か否かが争われた事案である。ECtHR は、「法律に従って」という要件について、単に国内法上の根拠の存在のみならず、接近可能性および秘密監視の文脈に即した予見可能性を含むものであり、法の支配と両立しうる「法律の質」を要求するものとした。そして、秘密裡に行使される権限については濫用の危険が高い以上、国内法は、市民に対し、公権力がいかなる状況において、いかなる条件の下で当該措置をとり得るのかについて十分な指示を与えなければならず、また、裁量権を付与する法律は、その裁量の範囲および行使の方法を合理的な明確さをもって示していなければならないとした。そのうえでECtHR は、イギリス法について、警察目的での通信傍受をめぐる権限行使の範囲および方法を合理的な明確さをもって示しておらず、現状ではなお曖昧であって異なる解釈を許すものであるとして、申立人に対する介入は条約第 8 条第 2 項のいう「法律に従って」行われたものとはいえないと判示した[42]。その後、この判断枠組みは、秘密監視措置に関する事案において継承・具体化され、当該措置を規律する国内法の「質」を審査する基準として展開されていった。

40）　van der Sloot（n 33）289-290.

41）　ECtHR, *Malone v. the United Kingdom*, no. 8691/79, Judgment of 2 August 1984, Series A no. 82.

42）　倉持孝司「通信の秘密：警察による電話盗聴および「メータリング」（マローン判決）［1984、全員法廷］」戸波江二ほか編『ヨーロッパ人権裁判所の判例Ⅰ』（信山社、2008年）342-344頁参照。

⑶ 「クリュスラン判決」[43] は、マローン判決で示された法理を承継しつつ、フランスの電話盗聴は条約第 8 条第 2 項に反するとした。ECtHR は、電話盗聴のような措置が私生活および通信の尊重に対する重大な介入を構成する以上、条約 8 条 2 項のいう「法律に基づいて」という要件は、単に国内法上の根拠が存在することによって満たされるものではないとした。すなわち、ここで要求されるのは、法の支配に適合するだけの「法律の質」であり、そのためには、法が権限ある当局に付与した裁量の範囲を十分に明確に示し、恣意的な干渉に対して個人に十分な保護を与えるものでなければならないとされた。とりわけ、電話による会話の傍受は重大な権利制約であり、しかもこの分野の技術的手段は不断に高度化し得ることから、当該措置を規律する法には、明確かつ詳細な準則が不可欠であると判示された。そのうえで裁判所は、当時のフランス法制について、盗聴の対象となり得る者の範囲、対象犯罪の性質、措置の期間、記録作成および保存の方法、録音テープの消去・廃棄の条件などに関する明確な定めを欠いており、実務上の運用が存在するとしても、それは成文法又は判例法ではない以上、濫用防止のための十分な保護とはいえないとした[44]。

⑷ さらに、審査の焦点は、個別の通信傍受措置の適法性そのものにとどまらず、通信傍受又は信号情報取得を可能にする法制度それ自体が、条

43） ECtHR, *Kruslin v. France*, no. 11801/85, Judgment of 24 April 1990, Series A no. 176-A. なお、これと同日・同趣旨の並行判決として、ECtHR, *Huvig v. France*, no. 11105/84, Judgment of 24 April 1990, Series A no. 176-B がある。両判決は、いずれもフランスの電話盗聴法制につき、条約 8 条 2 項の「法律に基づいて」という要件の下で、「法律の質」、すなわち予見可能性および恣意的干渉に対する保護が問題とされた点で、実質的に同一の法理を示す。事実関係には差異があり、前者は申立人自身の電話回線に対する盗聴、後者は刑事捜査の過程で行われた申立人の電話盗聴に関するものであるが、いずれも電話盗聴のような重大な介入を規律する法には特別の明確性が必要であり、当時のフランス法制は、盗聴対象者、対象犯罪、措置期間、記録作成・保存、録音の消去・廃棄等について十分明確な定めを欠くとして、条約 8 条違反を認めた。

44） 白取祐司「電話盗聴と手続法定原則――欧州人権裁判所 Kruslin 判決を契機として」ジュリスト 977 号（1991 年）54-58 頁；永野貫太郎「ヨーロッパ人権裁判所判決と電話盗聴」国際人権 6 号（1995 年）74-75 頁参照。

約第 8 条の要請に適合するだけの保障と限界を備えているかという点へと移っている。具体的には、*Zakharov*判決においてECtHRは、秘密監視の文脈では、申立人が自己に対する具体的監視を立証できない場合であっても、法制度の存在それ自体が条約第 8 条上の問題を生じ得ることを認めたうえで、当該法制度には、秘密監視措置が「民主社会において必要」な範囲にとどまることを確保するための十分かつ効果的な保障が組み込まれていなければならないと判示した[45]。さらに、「セントラム・フォル・レットヴィサ」判決においては、大量の情報取得を可能にする制度についても、法制度全体にわたる「end-to-end safeguards」が要求されることが明示され、取得の開始段階から、通信経路の選定、識別子および検索条件の選択・適用、取得資料の利用・保存・外部提供・削除、ならびに監督および救済に至るまで、一貫した統制構造が備わっているかが審査の中心に据えられた。また、「ビッグ・ブラザー・ウォッチ」判決においても、ECtHRは、大量傍受それ自体を当然に条約違反としたのではなく、そのような制度が許容され得る前提として、独立機関による開始時の承認、令状申請における識別子の類型の提示、個人に結び付く識別子に対する事前の内部承認、実施過程に対する監督および事後的救済を含む、制度全体に及ぶ保障が必要であることを明らかにした[46]。

秘密監視は、その性質上、対象者に知られないまま実施される[47]ため、本人による事前の異議申立てはもとより、事後的にもその実施の有無自体が容易には明らかとならない。そのため、個別の行為の違法性を事後的に判断するという通常の審査手法のみに依拠することには限界がある[48]。こ

45）Bart van der Sloot, “The Quality of Law: How the European Court of Human Rights Gradually Became a European Constitutional Court for Privacy Cases” 11 JIPITEC (2020), pp. 166-167, 183-184.

46）杉木志帆「情報機関による大量傍受に伴う私生活の尊重への権利および表現の自由への干渉――A：セントラム・フォル・レットヴィサ対スウェーデン事件、B：ビッグ・ブラザー・ウォッチほか対英国事件（ヨーロッパ人権裁判所2021年 5 月25日判決）」国際人権33号（2022年）107頁以下参照。

47）van der Sloot（n 33）290; Tzanou（n 20）352.

48）van der Sloot, “The Quality of Law”（n 45）160, 184.

の点につき、被監視者が自己に対する具体的監視の事実を立証し難いという構造を前提として、従来は原則として排斥されてきた「抽象的審査」がこの領域では例外的に受容され、その結果として、裁判所の中心的課題は、個別事案における干渉の有無や比較衡量それ自体ではなく、当該国家の法制度が備えるべき「法律の最低要件」（minimum requirements of law）を満たしているかを審査することに移ったと解される[49]。このような審査は、所管官庁による個別的な権限濫用の有無を点検するにとどまらず、立法府が執行機関に広範な権限を付与しつつ、それに対して十分な制約と保障を設けているかを問うという意味で、「立法過程・法制度それ自体に向けられた審査」の性格を帯びると説明される[50]。

㈢ 小　括

ECtHRが「法律の質」に関する判例法理として展開してきた以上のような要請は、EU法においても受容され、基本権制約を正当化する法的根拠の質を問う基準として位置づけられてきた。こうした「法律の質」に関する要請は、法執行領域における個人データ取得・利用等を統制するLED全体の構造の中で理解される必要がある。法執行領域における個人データ取得・利用等は、その実効性確保のため、一定の秘匿性および非予見可能性を不可避的に伴う。そのため、一般のデータ保護法制が前提とする事前的・全面的な透明性の確保は、法執行領域においては構造的に制約されざるを得ない。EU理事会も、LEDについて、法執行領域における透明性が進行中の捜査を害するおそれがあることを理由として、「透明性」を個人データの取得・利用等における諸原則の中に位置づけることはできないと説明している[51]。

49）Ibid., pp. 184-185.

50）Ibid., pp. 177-178, 184-185.

51）Council, Statement of the Council's reasons: Position (EU) No 5/2016 of the Council at first reading with a view to the adoption of a Directive of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the

このように、法執行領域においては、データ主体が自己の個人データの取得・利用等を事前に知り、これを自ら統制するという通常のデータ保護の構図が、そのまま妥当しない場合が少なくない。しかも、透明性は本来、アクセス権・訂正権等のデータ主体の権利行使や救済の実効性を基礎づける要素であるから、その制約は権利保護の空隙を生じさせる危険を内包する。ECtHRも、秘密監視のように当事者が干渉を知り得ない領域において、事後的通知を欠くことが救済の機会を奪い、救済を理論的・空疎なものにし得ることを指摘している[52]。また、CJEUの判例においても、少なくとも通信データへのアクセスの場面では、事後的通知が、とりわけ実効的救済の行使を可能にする前提となり得ることが示されている[53]。

それゆえ、法執行の文脈においては、「透明性」原則を通じた統制に一定の限界があるからこそ、個人データの取得・利用等を根拠づける明確な法律上の根拠がとりわけ重要となる[54]。すなわち、秘匿的に取得・利用等が行われる場合であっても、法律が取得・利用等の目的・対象・手段・限界をあらかじめ規範的に定めることにより、行政機関の裁量を拘束し、恣意的運用を抑制するとともに、監督機関や裁判所による事後的統制を可能にする。この意味で、LEDは、法執行領域の特性上、「透明性」原則をGDPRと同じ仕方で一般原則として前景化することが困難である一方、法律による権限付与とその質的統制を通じて個人データ取得・利用等の正当化を確保しようとする構造を採っているといえる。したがって、LEDに

---

purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA（2016/C 158/02）, OJ C 158, 3 May 2016, p. 47, Section III. B. 2（a）（“transparency”）.

52）　ECtHR, *Ekimdzhiev and Others v. Bulgaria,* no. 70078/12, Judgment of 11 January 2022, para. 350.

53）　CJEU, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Watson and Others, Joined Cases C-203/15 and C-698/15, Judgment of 21 December 2016, ECLI: EU: C: 2016: 970, para. 121.

54）　Tzanou（n 20）347, 358. 彼女は、「適法性」原則が、「透明性」及び「アカウンタビリティ」等の価値に資し、データ主体による権利行使及び救済の実効性を確保する機能を有すると述べる。

おける「適法性」原則は、単に個別の取得・利用等に法的根拠を要求するにとどまらず、その特性上制約せざるを得ない法執行領域において、個人データ取得・利用等を法の枠内に拘束し、個人データ保護権の保障のための中核的要素であると考える。

三 「目的特定」の原則――法執行目的の具体的特定

㈠ LED第1条第1項の目的列挙と「特定された」目的の区別

LED第4条第1項(b)は、個人データは「特定され、明確にされた、かつ正当な目的のために取得され、当該目的と両立しない態様で利用等されてはならない」[55) 56)]と定める。同号が要求する「目的特定」とは、単に「法執行目的」という広汎な表題を掲げることではなく、当該利用等が何のために、いかなる事件・事務の文脈において、いかなる態様で正当化されるのかについて、個々の具体的な目的単位で識別することを意味する[57)]。EUデータ保護指令に基づいて設置された「第29条作業部会」（以下、「WP29」という）は、「目的特定」は、個人データ取得・利用等の適法性判断および安全措置の適用の前提であり、目的が識別されていなければ、法令遵守状況を評価し、いかなる保護措置を適用すべきかを決定することが

55） LED, Art. 4（1）（b）: *"personal data shall be: ...（b）collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes."*

56） 本稿では、"specified"を「特定された」、"explicit"を「明確にされた」、判決上の"clear and precise"については、"clear"を「明瞭」、"precise"を「画定された」として、相互に区別して用いる。

57） European Commission, Commission Expert Group on Regulation（EU）2016/679 and Directive（EU）2016/680, Minutes of the Fifteenth Meeting, 20 February 2018, p. 1（Article 8 discussion）.

できないと説明する[58]。

「目的特定」の核心は、過度に包括的な目的の記述を排除する点にある。まず、「法執行それ自体」（law enforcement per se）は、特定され、明確にされた、正当な目的としてみなされない[59]。LED第 1 条第 1 項は、同指令の適用範囲を画する一般的な目的類型として、犯罪の予防・捜査・探知・訴追、刑の執行、ならびに公共の安全に対する脅威からの保護およびその防止を掲げている。このため、同項に列挙された事項のいずれかを示すことにより、個々の取得・利用等の目的が特定されたものと捉えられる余地がある。しかし、EU法上の一般的な理解によれば、第 1 条第 1 項に掲げられた目的類型のいずれかを単に援用するだけでは、個々の取得・利用等について目的が特定されたとはいえない。各類型は「目的」というより包括的な「目標」として位置づけられる。この点につき、欧州委員会はLED第 8 条に関する議論において次のとおり説明する。同条第 2 項は、加盟国法が、少なくとも、取得・利用等の「目標（objectives）」、取得・利用等される個人データ、および取得・利用等の「目的（purposes）」を明示しなければならない旨を定めている。欧州委員会は同項が両者を分けていることに着目し、第 1 条第 1 項の「objectives」が一般的・総括的に定義されるのに対し、「purposes」は各取得・利用等行為がなぜ行われるのかを明らかにするためにより具体的に定義されなければならないことで、両者は区別されると説明する。そのため、取得・利用等の「目的」として一般的に「捜査」のみを掲げることでは足りず、「捜査のために、生体データを用いて特定人を犯罪被疑者として識別する」といった形で、各取得・

58）Article 29 Data Protection Working Party, Opinion 03/2015 on the draft Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 3211/15/EN, WP 233, adopted 1 December 2015, p. 6.

59）Opinion of Advocate General Pitruzzella in *Ministerstvo na vatreshnite raboti*, C-205/21, delivered on 30 June 2022, ECLI: EU: C: 2022: 507, para. 50.

利用等行為の具体的な意味内容を画する必要がある[60]。

「目的特定」の重要性は、その機能に照らして説明される。第一に、目的が特定されることにより、個人データ取得・利用等を根拠づける立法の予見可能性が確保され、それを通じてデータ主体に法的安定性が付与される。第二に、目的特定は、データ最小化や保存期間の制限といった他のデータ保護原則の適用に際して、その判断基準を提供する。とりわけ後者との関係において、データ最小化原則は、特定された目的の達成に必要な範囲を超える個人データの取得・利用を排除することを要請し、保存期間の制限もまた、当該目的に照らして保存の必要性がなお存するか否かから判断される[61]。「法執行一般」は、個々の取得・利用等目的というよりも、法執行機関の活動領域を包括的に示すものにすぎない。また、第１条第１項の目的類型も、それ自体としては広範なカテゴリーである。取得・利用等の個々の目的がこれらを単に援用するにとどまる場合には、データ最小化や保存期間の制限といった諸原則について判断する基準を得られず[62]、これらの原則が形骸化する。これは、データ主体が、自己に関するデータの取得・利用等がいかなる目的の下で、いかなる範囲・態様で行われているのかを把握し、権利行使の要否および方法を判断するためにも重要であり、監督機関による審査・監督にとっても同様であろう。

この点について、最近のCJEUの*Policejní prezidium*判決は、特別な種類の個人データである生体データ・遺伝データの取得・利用等目的との関係で重要な判断を示している。本件は、チェコ警察が、刑事手続においてデータ主体に対し、指紋採取、頬粘膜の採取に基づく遺伝子プロファイルの作成、写真撮影および身体的特徴の記述を行い、これらの情報を警察データベースに記録した事案である。CJEUは、まず、生体データ・遺伝データの取得・利用等目的は、LED第10条にいう「厳格必要性」の審査

60） European Commission, Minutes of the Fifteenth Meeting（n 57）1.

61） Ruben Te Molder, Masha Fedorova, Marie Dubelaar and Sjarai Lestrade, “The principle of purpose limitation in data-driven policing: A guiding light or an empty shell?” New Journal of European Criminal Law 14（4）（2023）, p. 517.

62） van der Sloot（n 33）292.

を可能にする程度に、過度に一般的な文言ではなく、その範囲が十分に画定され、かつ具体的に定義されていなければならないと判示した。そのうえで、LED第 8 条第 2 項にいう「目標」が、同指令の適用範囲に属するために当該取得・利用等が追求すべき第 1 条第 1 項上の一般的な目標を指すのに対し、「目的」は、管理者の任務に照らして個人データの取得・利用等が追求する具体的かつ実際の目的（specific and real aims）を指すと判示する[63]。さらに、この区別は、2026年 3 月の *Comdribus* 判決においても確認されている。*Policejní prezidium* 判決を引用し、第 8 条第 2 項にいう「目標」と「目的」の区別を改めて確認した[64]。

「目的特定」については、それ自体の具体的内容が十分に明確ではないとの指摘がある。第 4 条第 1 項(b)は、個人データが「特定され、明確で、正当な目的」のために取得されなければならないと定めるが、これらの基準の意味はLED自体においてほとんど具体化されていない。前文26項は、取得・利用等目的が個人データの取得時に定められるべきことを述べ、第 8 条第 2 項は、加盟国法が少なくとも取得・利用等の目標、取得・利用等の目的を明確にすべきことを定めるにとどまる。そのため、「特定され、明確で、正当な目的」という各基準がいかなる場合に充足されるのか、またそれらが相互にいかなる関係に立つのかは、なお問題として残るとされる[65]。さらに、CJEUも、目的特定として何が要求されるのかについて十分な指針を示していないと評価されている。次の章で確認する *Inspektor* 判決はLEDにおける「目的拘束」原則に言及したものの、目的特定に何が要求されるかについては十分に踏み込んでいないとされる。また、法務官意見[66]、欧州委員会およびWP29において各基準はより詳細に論じられているが、それでもなお説明は限定的であり、加盟国は「目的特定」の要

63）CJEU, *Policejní prezidium*, C-57/23, Judgment of 20 November 2025, ECLI: EU: C: 2025: 905, paras. 18-19, 24-25 and 79-81.

64）CJEU, *Comdribus*, C-371/24, Judgment of 19 March 2026, ECLI: EU: C: 2026: 219, paras. 11-12 and 26-31.

65）Te Molder et al（n 61）517.

66）Opinion of Advocate General Pitruzzella（n 59）.

件充足を判断するにあたり十分な指針を得ていないと指摘されている[67]。

㈡ 「明確にされた」目的の実現態様

LED第 4 条第 1 項(b)は、目的が具体的に特定されることに加え、「明確にされた」(explicit) 目的であることをも要求している。なお、ここでいう「明確にされた」目的とは、目的が処理者の内心において設定されている[68]のではなく、理解可能な形態で表現され、説明され、伝達されていなければならないことを意味する[69]。WP29も、各言語版における「explicit」の訳語は様々であるものの、帰結としては、関係者が目的を曖昧さなく同じ意味で理解できるために必要な情報が十分に表現・伝達されていなければならないと説明している。この点、同意見書によれば、例えばドイツ語版では「explicit」に相当する語として「eindeutig」(一義的) が用いられる[70]。

もっとも、WP29によれば、この要請は、データ主体に対する情報提供義務又は監督機関への届出義務そのものと同一ではないと説明される。一方で、目的の表現が、データ主体に提供される通知、監督機関への届出、又は組織内部でDPOに提供される情報など、複数の方法によって達成され得ると説明する。また、同意見書はOECDガイドラインの説明を引用し、公表、データ主体への情報提供、立法、行政命令、監督機関による許可等の代替的又は補完的方法を通じて行われ得るとも述べている。したがって、

67） Te Molder et al (n 61) 519.

68） この意味で、実務上の各利用等行為についても、その目的が認識可能な形で具体化されている必要があると考えられる。

69） Article 29 Data Protection Working Party, Opinion 03/2013 on Purpose Limitation, 00569/13/EN, WP 203, adopted 2 April 2013, p. 17. なお、同意見書はDirective 95/46/EC下の解釈指針でありLEDに直接適用されるものではないが、LEDに関する学術文献においても参照されている。例えば、Paul De Hert & Juraj Sajfert, "The fundamental right to personal data protection in criminal investigations and proceedings: framing big data policing through the purpose limitation and data minimisation principles of the Directive (EU) 2016/680," Brussels Privacy Hub Working Paper No. 31 (2021), pp. 4-5.

70） WP29, Opinion 03/2013 (n 69) 17-18.

WP29から確認できるのは、「明確にされた」目的がデータ主体への直接的通知のみに還元されるものではなく、目的が認識可能な形で表現・伝達されているかという問題として把握されているという点である[71]。

このことは、法執行領域において特に意味をもつ。法執行活動では、捜査等の実効性確保のため、目的や取得・利用等態様をデータ主体に対して常に全面的かつ事前に通知することが困難な場合があるからである。Koningも、「明確にされた」目的を、データ主体、監督機関その他の関係者が取得・利用等の目的を一義的に理解し得るようにするため、当該目的が明らかにされ、説明され、開示されなければならないという要請として説明する。もっとも、彼は、刑事法執行の文脈において、秘密的な個人データ取得・利用等と、「明確にされた」目的という基準とは、一見すると緊張関係に立つように見えると指摘する。そのうえで、彼は、EU立法者がLED前文において、秘密的な手法よる個人データ取得を、法律上の根拠、自然人の正当な利益への配慮、ならびに民主的社会における必要性および比例性という要件との関係で位置づけていると説明する[72]。

㈢　小　括

第１条第１項で列挙された犯罪の捜査、訴追等の目的類型は、当該取得・利用等がLEDの適用領域に属することを示すにとどまり、それ自体が直ちに第４条第１項(b)のいう「特定された目的」となるわけではない。第４条第１項(b)は、個々の取得・利用等の目的をあらかじめ一律かつ詳細に列挙する規則ではなく、個人データの取得・利用等を方向づける基準ないし原則を定めるものである。「目的特定」について、詳細なEU法上の定義が置かれていないことは、必ずしも同要件の欠陥を意味すると解すべきではない。むしろそれは、目的を特定することが、加盟国法上の根拠規定および取得・利用等の文脈に即して具体化されるべき構造を有して

71）　Ibid., p. 18.

72）　Merel E. Koning, *The Purpose and Limitations of Purpose Limitation* (doctoral thesis, Radboud University Nijmegen 2020), pp. 68-69.

いることと関係していると捉えるべきである。重要なのは、「目的特定」要件の不明確性をLEDの欠陥として強調することではなく、第 1 条第 1 項の包括的な目的類型と、第 4 条第 1 項(b)にいう具体的な取得・利用等の目的とを区別することである。目的が具体的に特定されることにより、公益性の高い法執行領域において、個人データ取得・利用等が抽象的な「法執行目的」の名の下に正当化されるかのような事態を防止することができる。

なお、目的の「明確性」は、目的の意味・意図について曖昧さや多義性を残さず、関係者が取得・利用等の目的を同一の意味で理解し得るようにするための要請である。法執行領域における「明確にされた」目的については、データ主体に対してその内容を全面的に明示することには一定の限度がある。むしろ、取得・利用等の目的が、通知、届出、内部文書、法律上の定め等を通じて、関係者にとって認識可能な形で表現・伝達されているかが問題となる。法律による目的等の明確化は、法執行領域において明確性を実現し又は補完する方法の一つとして位置づけられる、と考える。

四 「目的拘束」の原則――目的変更の統制

㈠ GDPRとLEDにおける目的変更の統制の相違

「目的拘束」原則は、「目的特定」原則を前提として、個人データの取得・利用等を、原則として取得時に特定された目的の範囲内に限定するものと説明される[73]。伝統的には、旧データ保護指令（Directive 95/46/EC）の下において、「目的拘束」原則は、当初目的とは異なる目的のための利用等について「適合性（compatibility）[74] を積極的に命令する」ものではなく、「非適合性（incompatibility）を禁止する」という二重否定の構造を有する

73） van der Sloot（n 33）294.

74） 個人情報保護委員会のGDPR仮翻訳本では、“compatible”を「適合する」と訳すが、EDPB「同意に関するガイドライン05/2020」の日本語版は、“provision on compatibility of purposes”を「目的の両立性に関する規定」と訳す。

ものと解釈される[75]。LED第 4 条第 1 項(b)も、個人データが「適合しない」方法で利用等されてはならないと規定しており、この限りにおいて、「目的拘束」原則を「非適合性の禁止」として把握する理解は、LEDにおいても基本的に妥当し得る。すなわち、この構造は、取得時に特定された目的から逸脱する利用等に限界を設ける一方で、当初目的と適合し得る範囲において、処理者に一定の柔軟性を残すものといえる[76]。

GDPR第 5 条第 1 項(b)は、「目的拘束」原則を定めるとともに、当初目的と適合しない「追加的利用等」(further processing) を禁止する。他方で、同一管理者が同一の法的根拠に依拠して別の目的で個人データを利用等する場面では、当該目的が当初の取得目的と適合するかを判断する「適合性テスト」[77] が要求されており、適合性が肯定される限り別の目的のための利用等が許容される。GDPR第 6 条第 4 項は、別の目的のための利用等は、別目的に対する別途の同意や法的根拠がない場合、処理者等が当初目的との適合性を一定の事項に照らして判断すべきことを定めている。判断事項としては、(a)目的間の関連性、(b)管理者とデータ主体の関係および取得の経緯、(c)データの性質、(d)データ主体に発生する可能性のある事態、(e)適切な保護措置の存在などが挙げられ、これらを総合考量したうえで目的間の適合性を判断する。

これに対して、LEDにおける「目的拘束」原則は、 4 条第 1 項(b)において、「……その目的に適合しない態様で利用等をしてはならない」と規定される。次いで、LED第 4 条第 2 項[78] は、個人データを取得目的と

75） WP29, Opinion 03/2013 (n 69) 21.

76） Ibid.

77） “test of compatibility” Catherine Jasserand, “Law Enforcement Access to Personal Data Originally Collected by Private Parties: Missing Data Subjects’ Safeguards in Directive 2016/680?”, *Computer Law & Security Review* 34 (1) (2018); “compatibility test” De Hert & Sajfert (n 69).

78） LED, Art. 4 (2): “Processing by the same or another controller for any of the purposes set out in Article 1 (1) other than that for which the personal data are collected shall be permitted in so far as: (a) the controller is authorised to process such personal data for such a purpose in accordance with Union or

は異なる目的のために利用等する場合、同一又は他の管理者による個人データの利用等とを一定要件の下で許容する。その要件としては、(a)管理者がEU法又は加盟国法により、当該別の目的のために当該個人データを利用等する権限（法的根拠）を有すること、(b)当該別の目的のために利用等する必要で比例的であることが挙げられる。もちろん、別の目的であっても、第 1 条第 1 項の定める「目標」の範囲内に属する必要がある。前文第27項は、想定される場面の例として、犯罪活動に関する理解を深化させるための目的変更[79]、ならびに探知された相互に異なる犯罪間の関連性を導出するための目的変更を掲げている。つまり、LEDは、別の目的それ自体を、基本権制限の一般的基準、すなわち正当な目的、EU法又は加盟国法上の根拠、必要性および比例性に照らして正当化する構造へと重心を移している[80]。

De Hert & Sajfertは、LEDにおける「目的拘束」の体系が、GDPRにおける「追加的利用等」およびそれに随伴する「適合性テスト」の要件を置くのではなく、LEDの文言・体系が異なる目的のための利用等を「目的変更」（change of purpose）に関する旨で規律していると把握する。彼らは、LEDがGDPR上の「追加的利用等」という概念を用いないことに着目し、LEDの適用領域の内外で目的が転換される場合を包括する「目的変更ルール」（rules on change of purpose）を総称して「後続利用等」（subsequent processing）と呼び、その中心的な規律として、とりわけ第 4 条第 2 項を

Member State law; and (b) processing is necessary and proportionate to that other purpose in accordance with Union or Member State law."

79） 本稿では、取得目的とは異なる目的のために個人データを利用する場面を、原則として「目的変更」と表記する。とりわけLED第 4 条第 2 項にいう "processing ... for any of the purposes set out in Article 1 (1) other than that for which the personal data are collected" を念頭に置く。ただし、GDPR第 6 条第 4 項の "further processing" については「追加的利用等」とし、また先行研究が "subsequent processing" 等の語を用いる場合には、当該議論の紹介・検討に限り「後続利用等」と表記する。

80） Koning (n 72) 203.

「目的変更」を定める規定として位置づけている[81]。さらに、このような理解は、GDPRの「追加的利用等」が、原則として同一管理者・同一の法的根拠の下でのみ問題となり、データが別の管理者に移転され、又は法的根拠が変更された場合には、その利用等は新たに開始されるという前提を背景にしている点からも、LED第 4 条第 2 項が扱う異なる目的のための利用等を「追加的利用等」というよりも「目的変更」として概念化することを正当化すべきであるとする[82]。欧州議会の研究は、用語上の差異を超えて、「追加的利用等」と「後続利用等」との間にいかなる概念的差異が認められるのか、また、このような「後続利用等」が適合性要件といかなる関係に立つのかについては、ほとんど説明がないと指摘している。したがって、潜在的に適用され得るこの「後続利用等」概念の基礎にある論理および機能は、依然として不明確であり、それを支持する議論も説得力を欠くと評価される[83]。

㈡ 「捜査」目的と「訴追」目的の分離：*Inspektor*判決[84] ①

前節で検討したLEDにおける「目的拘束」原則および「目的変更」の理論的枠組みが、実際の法執行手続においてどのように具体化されるべきかを示したのが、*Inspektor*判決（C-180/21）である。以下では、同判決の事案の概要および判旨を検討し、捜査と訴追という一連の手続が「目的拘束」の観点からいかに分節化されるかについてみてみる。

81） De Hert & Sajfert（n 69）9-10; なお、この区別につき、European Commission, Minutes of the Fifteenth Meeting（n 57）.

82） De Hert & Sajfert（n 69）11.

83） Plixavra Vogiatzoglou and Thomas Marquenie, *Assessment of the Implementation of the Law Enforcement Directive*（Study requested by the LIBE Committee, European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, PE 740.209, December 2022）, p. 35.

84） CJEU, *Inspektor v Inspektorata kam Visshia sadeben savet*, C-180/21, Judgment of 8 December 2022, ECLI:EU:C:2022:967.

1　事案の概要

ブルガリアにおいて、ある刑事事件につき予審手続が開始され、その過程で、データ主体に関する個人データが、犯罪の「探知」および「捜査」の目的の下で取得された。当初、データ主体は当該犯罪の被害者として扱われていたが、その後、手続の進行に伴い、当局は同人を被疑者として把握するに至り、最終的には、当該データを同人の公訴提起のために用いた。これに対しデータ主体は、検察当局等による自己の個人データ利用等が適法でないとして争った。

2　判　旨

これに対しCJEUは、まず、国内裁判所から負託された質問を、LED第1条第1項を第4条第2項および第6条と併せて解釈する場合に①「探知」・「捜査」目的で取得された個人データを、その後「訴追」目的で利用することが第4条第2項にいう目的変更に当たるか、②当たるとすれば、それがいかなる要件の下で許容されるか、という問題として整理した（§39-40）。

そのうえでCJEUは、LED第1条第1項の文言自体が、犯罪の予防・探知・捜査・訴追・刑の執行等を相互に区別された目的として列挙していること、また第4条第2項も、個人データが取得目的とは異なる目的（ただし第1条第1項所定の目的の一つ）に利用等され得ることを予定していることに着目し、「探知」・「捜査」と「訴追」は、LEDの体系上、相互に区別された別個の目的であると判示した。したがって、犯罪の「探知」および「捜査」のために取得された個人データを、その後、当該人物の「訴追」のために用いることは、取得目的とは異なる目的のための利用等に当たるとした（§42-44）。

さらにCJEUは、LED第6条が、被疑者・有罪判決を受けた者・被害者等、異なるデータ主体類型を可能な限り区別すべきことを求めている点を確認しつつも、同条はあくまでデータ主体の類型区分に関する義務を定めるにとどまり、第4条第2項にいう目的変更の該当性そのものを決する規定ではないとした。すなわち、ある者が当初は被害者として把握され、

その後、訴追対象者として扱われるに至ったとしても、その事情は第 6 条上の区分義務との関係で意味を有するにすぎず、あくまで第 1 条第 1 項および第 4 条第 2 項の構造に即して判断されるべきものとされた。とりわけ同裁判所は、第 6 条が“where applicable”および“as far as possible”という文言を用いていることからも、捜査初期段階では同一人が複数の類型にまたがり得ることを前提としていると読み取れるとした（§45-49）。

そして、右のような目的変更が常に禁止されるわけではなく、LED第 4 条第 2 項(a)・(b)に従い、①当該管理者がEU法又は加盟国法によりその別目的のための利用等権限を付与されていること、かつ、②当該利用等がその別目的に照らして必要かつ比例的であることを要するとした（§51）。CJEUは、捜査段階で取得されたデータがそのまま当然に訴追目的に必要となるわけではなく、捜査目的における個人データ取得と訴追目的におけるデータ利用等とでは、必要とされるデータの範囲も、データ主体に対する影響も異なり得ると指摘した（§53-54）。そのため、当該利用等の適法性は、国内裁判所において、国内法上の権限付与の有無と、必要性・比例性の具体的審査を通じて判断されるべきであるとした（§61-62）。

したがって、CJEUは、犯罪の「探知」・「捜査」目的で取得された個人データを、その後、当該人物を「訴追」する目的で利用等することは、たとえ取得時にその者が被害者として扱われていたとしても、LED第 4 条第 2 項にいう目的変更に当たり得るが、当該利用等は、同項所定の要件、すなわち権限付与および必要性・比例性の要件を満たす限りで許容される、と結論づけた（§63）。

3　若干の検討

*Inspektor*判決の意義は、LED第 1 条第 1 項に列挙された――犯罪の予防・捜査、訴追など――各目的を、連続する法執行活動として捉えるのではなく、相互に区別される独立の利用等目的として把握した点にある。本判決は、LEDにおける「目的拘束」原則および目的変更の概念の解釈に本格的な含意を有する最初の判決として、捜査段階における利用等と訴追

段階における利用等とを別個の目的に属するものとして理解すべきことを明確にした。これにより、犯罪の「探知・捜査」という目的のために取得された個人データを、その後「訴追」その他の法執行目的のために利用等する場合には、それは単なる手続の継続ではなく、起訴のための利用等に対してEU法・加盟国法上の根拠、その利用等の必要性と比例性を再評価することが求められる。そのため、捜査段階において取得された個人データが事実上最初から起訴目的も含むと主張する余地はなくなったと評価される[85]。

また、捜査段階においては、なお犯罪事実が確定していない以上、潜在的に関連し得るより広範な個人データ取得が正当化され得るのに対し、訴追段階においては、国内裁判所が判断を下し得るよう、行為の証明力およびその法的評価を基礎づけるのに必要な範囲のデータのみが正当化される。したがって、捜査のために必要であったデータが、そのまま当然に訴追のためにも体系的に必要であるとはいえず、目的が「探知・捜査」から「訴追」へと転換する時点において、別の目的に照らしてEU法又は加盟国法上の根拠、利用等の必要性および比例性を改めて審査しなければならない。この点、刑事手続は一連の国家作用として連続しているとしても、本判決は、法執行領域における個人データの利用等を包括的に正当化することに一定の歯止めをかけることにつながる。

もっとも、Bonettoは、目的ごとに必要性・比例性を改めて審査することが実務にもたらす影響についても言及する。まず、目的変更に対する判断の結果はLED第41条に基づき設置されたデータ保護監督機関による事後的な審査に服し得る。検察が訴追目的での個人データ利用等を比例的と判断した場合であっても、監督機関においてその判断が争われ得るものであり、これは訴追に係る検察の裁量および独立性を制約し得ると彼は指摘する。他方で彼は、目的変更に対する判断が必ずしも新たな過大な負担を

85） Giacomo Bonetto, “The judgment of the CJEU in Inspektor（Purposes of the processing of personal data – criminal investigations）of 8 December 2022 and the concept of further processing under the Law Enforcement Directive” New Journal of European Criminal Law 15（1）（2024）, p. 64.

意味するわけではないとも論じる。加盟国の刑事訴訟法はすでに、捜査段階で取得された証拠を訴追に用いる際に必要性・比例性の判断を内在させている場合が多く、そのような場合には、捜査・訴追機能の通常の遂行過程においてこれを遂行し文書化することで足りると解されるからである。目的ごとの判断が監督機関の介入を通じて訴追機能の独立性を制約し得るが、他方で、加盟国の刑事訴訟法によってその負担が実質的に軽減され得るというのが、彼の分析である[86)]。また、目的変更の判断とデータ主体の類型変更とを区別した点にも、本判決の意義を見いだすことができる。本件では、データ主体が当初は被害者として位置づけられ、その後に訴追対象者へと身分が変動した。CJEUは、データ主体の類型変動という事実のみから直ちに目的の同一性ないし差異を導くことを避けている。本判決は、むしろLED第 6 条の機能をデータ主体の類型区分義務に限定し、第 4 条第 2 項の意味における別の目的に当たるか否かはまた別途に判断されるべきものとして、「誰に関するデータであるか」という類型区分の問題と、「何のための利用等か」という目的判断の問題とを、それぞれ別個の局面として分離して扱っている。この区別を曖昧にすると、所管官庁は、「データ主体の地位が変わったから利用等目的も当然に変わった」あるいは逆に「同一の事件に関するものである以上、目的は同一である」と捉え、利用等目的についての独立した審査を回避し得ることになる。本判決は、両問題を分離したことで、データ主体の身分変動のみを理由として「目的拘束」審査を免れる余地をなくさせた点で意義を有する。

㈢　LEDからGDPRへの目的変更：*Inspektor*判決②

*Inspektor*判決は、法執行目的で取得された個人データが非法執行目的のために利用等される場面における規律を明確化した点においても重要である。「目的特定」・「目的拘束」原則は、個人データの利用等をその取得時に特定された目的の範囲内に拘束することで、恣意的な利用等を統制する機能を担う。しかし、かかる原則の機能する局面は、単一の法的枠組み

86）　Ibid., pp. 65-66.

の内部に完結するものではない。民間事業者又は一般行政機関がGDPRの適用下において取得・保有していた個人データが法執行目的のために利用等される場面、あるいは所管官庁がLEDの適用下において法執行目的のために取得した個人データがその後、同目的の射程を外れた形で利用等される場面においては、その許容性判断にあたり、いずれの法制が適用されるかという問題が生じる。

このうち、所管官庁が法執行目的のためにLEDの適用下で取得した個人データを、その後、法執行目的の射程外にある目的のために利用等する場面を先に検討する。かかる場面において、所管官庁はLEDの適用主体とGDPRの適用主体の両方の地位を併せて有し得る。既に検討したLED第 4 条第 2 項の規定は、新たな目的もまた第 1 条第 1 項に定める目的の範囲内に属する場合にのみ変更を許容するものであり、法執行目的の射程を外れた利用等はその対象とならない。かかる場面において代わって機能するのがLED第 9 条である。同条は、所管官庁が法執行目的のために取得したデータを第 1 条第 1 項の射程外にある目的のために利用等しようとする場合には、まず当該利用等がEU法又は加盟国法によって許容されていることを要し、この場合には原則としてGDPRが適用される旨を定める。前述した*Inspektor*判決は、所管官庁が法執行目的のために取得された個人データが、その後、国家賠償訴訟における国家の法的・財政的利益を防御するために用いられる場合に、いかなる法的枠組みに服するかについても判断を示している。すなわち、当該場面では、もはやLED第 1 条第 1 項所定の法執行目的そのもののための利用等ではない以上、GDPRが適用され得るべきこと、そしてその利用等の根拠はGDPR第 6 条第 1 項(e)（公益又は公的権限行使に基づく職務遂行）を中心に判断されるべきことが示された。*Inspektor*判決においては、この点も争点となったところ、以下では、その事案の概要および判旨を整理する。

1　事案の概要

データ主体は、不合理に長期化した予審手続による損害を理由として、国内裁判所に国家賠償請求訴訟を提起した。本件で問題になったのは、同

訴訟において、検察当局が国家の防御のために、当該データ主体に関するファイルの存在を裁判所に示し、さらに当該ファイルの文書写しを提出した。

2　判　旨

CJEUは、まず国内裁判所から付託された第二の質問を、LED第3条第8号・第9条第1項および第2項ならびにGDPR第2条第1項および第2項に照らし、加盟国の検察庁が国家賠償訴訟において国家の法的・財政的利益を防御するため、当該訴訟当事者に関する事件記録の存在を裁判所に知らせ、これを裁判所に送付する場合にもGDPRが適用されるか、また、そのような利用等がGDPR第6条第1項(f)の「正当な利益」に基づき適法たり得るか、という問題として整理した（§64）。

①　国家賠償訴訟における国家の法的・財政的利益を防御するために検察による個人データ利用等に対するGDPRの適用

CJEUは、GDPR第4条にいう「個人データ」の定義およびその「利用等」概念はいずれも広範に解されるべきであり、検察庁が民事手続において刑事事件記録の存在を裁判所に通知し、又は当該記録を裁判所に送付する行為は、GDPR第4条(2)にいう個人データの「利用」および「送信による開示」に該当するとした（§70-72）。CJEUは、GDPR第2条第2項(d)の適用除外は厳格に解釈されるべきであるとした上で、所管官庁による法執行目的のための個人データの利用等が、まさにその適用除外の射程に属することを確認した（§73）。そのうえで、LED第9条が、同指令第1条第1項に定める目的のために取得された個人データを、それ以外の目的のために利用等する場合の法的枠組みを定めていることに着目した。この点につき、LED第9条第1項は、所管官庁が第1条第1項所定の目的のために取得した個人データをそれ以外の目的のために利用等する場合を規律し、そのような利用等はEU法又は加盟国法によって認められる場合に限って許容されるとしたうえで、当該利用等がEU法の適用範囲外の活動において行われるのでない限り、GDPRが適用されることを定めている。これに対して同条第2項は、所管官庁が加盟国法によって第1条

第 1 項所定の目的以外の任務の遂行を委ねられている場面を規律し、その任務の遂行に際して行われる利用等には、EU法の適用範囲外の活動に属しない限り、GDPRが適用される旨を定めている（§75-76）。たしかに検察が当初当該データを取得・保有したのはLED第 1 条第 1 項所定の法執行目的のためである（§77）。しかし、本件のように国家賠償訴訟の提起が「合理的期間内に裁判を受ける権利」の侵害等、刑事手続における検察庁の違法な職務執行を原因とする場合であっても、そのような訴訟において国家が防御する権利を行使する目的は、LED第 1 条第 1 項に規定された目的のための検察庁の任務をそれ自体として遂行することにあるのではないとした（§78）。また、それは「EU法の適用範囲外の活動」にも当たらないと判断した（§79）。

すなわちCJEUは、問題となる利用等がLED第 9 条第 1 項又は第 2 項のいずれに該当するかにかかわらず、LED第 1 条第 1 項所定の法執行目的のために取得された個人データがそれ以外の目的のために利用等される場合には、EU法の域外といった例外的状況にない限り、GDPRが適用されると解した（§81）。したがって、国家賠償訴訟において国家の防御のために、検察庁が訴訟当事者である自然人に関する事件記録の存在を裁判所に通知し、又は当該記録を裁判所に送付する行為には、GDPRが適用される（§82）。

② 国家賠償訴訟における国家の法的・財政的利益を防御するために検察による個人データ利用等の適法性

GDPR第 6 条は個人データの利用等の適法性根拠を限定列挙している（§83）。同条第 1 項第 1 段落(e)は公益又は公的権限行使に基づく職務遂行に必要な利用等を、(f)はデータ主体の利益や基本権・自由が優先しない限りにおいて管理者又は第三者の「正当な利益」のための利用等を適法根拠として規定する。しかし同項第 2 段落によれば、公的機関がその任務遂行の過程で行う利用等には(f)は適用されない（§84）。この点、CJEUは、公的機関による利用等が公益の遂行を目的とするものである場合には、原則として(e)が問題となり、(e)と(f)はこの場合、相互に排他的であるとした（§85）。

これを前提にCJEUは、検察庁がLED第 1 条第 1 項所定の目的のために取得した個人データを、国家又は公的機関の違法な職務執行を原因とする国家賠償訴訟において国家を防御するために利用等することが、GDPR第 6 条第 1 項前段(e)の意味における公益の遂行に必要な利用等に該当するかを検討した（§86）。CJEUは、刑事事務に関連して行われた公的機関の行為が問題となる国家賠償訴訟において、検察庁が国家の法的・財政的利益を防御する責任を負う場合、その防御は国内法上の公益の遂行として評価され得るとした（§87）。すなわち、公的機関は被告として手続上の防御する権利を行使することにより、公益的行為・決定の法的安定性を維持し、根拠のない又は過大な損害賠償請求によって公益的任務の遂行が萎縮することを防止し得るというのである（§88-89）。この点につき、国家賠償訴訟において検察庁が他の当事者と対等な地位に立ち、刑事手続におけるような公権力を直接行使しないという事情は、この判断を左右しないとした（§90）。

またCJEUは、本件国家賠償訴訟が国内法上の国家責任体系に基づくものであり、損害を生じさせた当局が手続上国家に代位して訴訟当事者となる点にも着目した。その結果、このような訴訟における当該当局の地位は単に私益を防御する私人的地位とは異なり、検察庁が国家を防御するために個人データを利用等する行為は、原則としてGDPR第 6 条第 1 項第 1 段落(f)ではなく(e)の適用範囲に属するとした（§91-93）。

さらにCJEUは、検察庁が国家賠償訴訟において管轄裁判所の求めに応じて個人データを送付する場合、適用される国内法上その求めに応じる義務を負うのであれば、かかる送付は同項(c)、すなわち法的義務の遵守のための利用等に該当する可能性もあるとした（§94）。

もっともCJEUは、以上の根拠のみをもって直ちに適法性が確定するわけではないとした。国内裁判所は、GDPR第 6 条第 3 項に従い、国内法が当該利用等の法的根拠と目的を規定しているか否か、また(e)との関係では当該利用等が検察庁の公益的任務の遂行に必要であるか否かを審査しなければならない。加えて、当該情報の開示がGDPR第 5 条第 1 項(c)のデータ最小化原則に適合するか否か、およびデータ主体が提出された情

報・証拠に対して実質的に意見を陳述し、又はGDPR第21条第 1 項に基づき国内法上許容される範囲でその提出に異議を申し立てることができるかといった適切な安全措置が確保されているか否かについても、あわせて審査されなければならないことを明らかにした（§96）。

3　若干の検討

本件では、検察が訴追目的で利用等した個人データが、その後、国家賠償訴訟における検察庁の防御という目的のために利用等されたことが問題となった。CJEUは、このような利用等はLED第 1 条第 1 項所定のいずれの目的にも属さず、このような利用等は、LED第 9 条第 1 項の下で、EU法又は加盟国法によって許容される場合に限り認められる目的変更に当たる。そのうえで、同条 2 項により、EU法の適用範囲を逸脱する例外的状況にない限り、当該利用等にはGDPRが適用されるとした。また、国家賠償訴訟において国家の法的・財政的利益を防御するための利用等は、原則としてGDPR第 6 条第 1 項(e)――公益又は公的権限行使に基づく職務遂行――に基づいて正当化され得るとした。

もっとも、Bonettoは、CJEUが示した適法性根拠の判断には問題が残ると指摘する。彼によれば、当初の訴追目的とは異なる目的のための利用等である以上、その適法性はGDPR第 6 条第 1 項(e)ではなく、「追加的利用等」の適法性を規律する第 6 条第 4 項によって判断されるべきであったと指摘する[87]。また彼は、CJEUがGDPRの適法性根拠の問題に直接進んだ点についても問題を指摘する。訴追目的で取得された個人データを民事訴訟における防御のために提供する行為は、LED第 9 条第 1 項が原則として禁止する目的変更に当たる。CJEUはこの点――LED第 9 条第 1 項との関係――を十分に論じないまま、直接GDPRの適法性根拠の問題に進んでいる。所管官庁としては、まず同条第 2 項以下に基づき、かかる利用等が認められるかを確認する必要があったと指摘される[88]。

87）　Ibid., p. 68.
88）　Ibid., p. 69.

㈣　GDPRからLEDへの目的変更

困難な問題は、GDPRの適用主体が法執行以外の目的で取得・保有していたデータを捜査機関に提供し、これが法執行目的のために利用等される場合である[89]。GDPRからLEDへの転用については、*Inspektor*判決のような明示的な先例は存在しない。また、LED第 9 条が比較的明確に規律しているのに対し、GDPRからLEDへの転用については、これに対応する規定が条文上に設けられていない。代わりに、GDPR第 2 条第 2 項(d)および前文第19項が方向性を示すにとどまる。これらの規定は、法執行目的のための利用等にはGDPRは適用されず、LEDが適用される旨を定めるのみである。これは、民間主体のみならず、公的機関がGDPRの下で利用等した個人データであっても、それが後に所管官庁により法執行目的のために利用等される場合には、LEDが規律することを意味する。

もともとGDPRの適用主体が当該データを所管官庁に提供する段階は、依然としてGDPRの問題である。GDPRの適用主体からLEDの適用主体への移転において、移転行為それ自体はGDPRの規律に服する[90]。欧州議会の研究は、ePrivacy指令[91]の文脈におけるCJEUの判例を通じてこの点を確認している。*La Quadrature du Net and Others*判決は、GDPRが法執行目的のために行われる所管官庁による利用等には適用されない一方で、同一の目的に関連する民間主体による利用等はGDPRの適用範囲に含まれ得ることを示している[92]。また同判決は、事業者に保存義務又は所管官

89）　van der Sloot（n 33）295; Vogiatzoglou & Marquenie（n 83）34 et seq.

90）　Vogiatzoglou & Marquenie（n 83）27–28; Nadezhda Purtova, “Between the GDPR and the Police Directive: Navigating Through the Maze of Information Sharing in Public-Private Partnerships” International Data Privacy Law 8（1）（2018）, pp. 61–62.

91）　Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector（Directive on privacy and electronic communications）.

92）　Vogiatzoglou & Marquenie（n 83）35.

庁による当該データへのアクセスを認める義務を課す国家措置と、国家が自ら措置をとる場合と区別している[93]。

次に、*Privacy International*判決も、加盟国が電子通信サービス提供者に個人データの保存・アクセスを認める義務を課す措置と、当該提供者に義務を課すことなく加盟国が自ら措置をとる場合とを区別し、前者についてはePrivacy指令の適用範囲内にあるのに対し、後者については同指令ではなく国内法によって規律され、場合によってはLEDの適用が問題となり得ると判示している[94]。したがって、これをGDPRとLEDの関係に照らすと、GDPRの適用を受ける主体が所管官庁に個人データを提供する段階は、少なくとも原則として、なお提供主体側の利用等として把握されるべきであり、この段階においては、原保有者による提供行為についてGDPR上の法的根拠がまず必要となると理解することができる。

所管官庁が当該データを受領し、法執行目的のために利用等する段階に至って初めて、LEDの問題となる。もっとも、当該LED段階における利用等を、LED第 4 条第 1 項(b)の「当初利用等」(initial processing) と解するか、それとも同条第 2 項の目的変更と解するかについては、かつて学説上争いがあった。この点、今日では論争は収まっており、いったん個人データが所管官庁に移転され法執行目的のための利用等に供された以降は、その「後続利用等」はLEDの適法性構造に服することとなり、現時点においてはこれをLED上の新たな「当初利用等」として把握する見解が有力になっている[95]。

㈤ 小　括

LEDがGDPRとは異なる構造を採用している理由は、法執行領域にお

93） CJEU, La *Quadrature du Net and Others* (Joined Cases C 511/18, C 512/18 and C 520/18), Judgment of 6 October 2020, ECLI: EU: C: 2020: 791, paras. 96, 98 and 103.

94） CJEU, *Privacy International* (Case C 623/17), Judgment of 6 October 2020, ECLI: EU: C: 2020: 790, paras. 39, 41, 47 and 48.

95） Vogiatzoglou & Marquenie (n 83) 36.

いては、データ主体による利用等の認知・統制が、制度構造上、私人間取引の文脈と同程度には予定されていないという点に求められる。すなわち、GDPR第 6 条第 4 項にいういわゆる「適合性テスト」は、概ね 5 つの事項を総合考慮する枠組みであり、その前提には、データ主体の合理的期待がなお一定の考慮に値するという理解がある[96]。これに対し、法執行領域においては、法執行活動の実効性確保の要請から、データ主体に対し利用等の存在、目的、範囲等を開示すること自体が制度的に制限されやすい。このことは、LEDの下では、データ主体が自己に関する利用等の具体的文脈を十分に認識し、それを基礎に利用等の「適合性」を争うというGDPR型の構造が、少なくともそのままの形では作動し難いことを意味する。

GDPRが営利・非営利、公的部門・民間部門を問わず、広範な個人データ利用等を対象とする一般規律であるのに対し、LEDの適用範囲は法執行領域に限定されている。そのため、LEDにおいて問題となるのは、法執行目的の内部における利用等に限定されることになる。したがって、当初とは異なる目的といっても、それは依然として、法執行目的の内部における異なる目的である[97]。この点を踏まえると、GDPRの仕組みは、LEDの文脈では抽象的な基準にとどまる危険も否定できない。すなわち、関連性、影響、保護措置等の要素を包括的に衡量することを要求するとしても、捜査・訴追等の各目的はいずれも広い意味では法執行目的に属する。そのため、GDPR型の「適合性テスト」をそのまま用いるだけでは、目的間の境界が曖昧化する危険がある。以上を踏まえると、LEDにおいては、GDPR型の「適合性テスト」モデルは具体的な判断枠組みというよりも宣言的水準にとどまるおそれがある。これに対し、個別の目的類型を法律レベルにおいて列挙・類型化する方式の方が、捜査実務の予測可能性および規範の明確性を確保するという観点からは、より適切な規律モデルとして

96）　Ivo Emanuilov et al., “Purpose Limitation by Design as a Counter to Function Creep and System Insecurity in Police AI” in *UNICRI Special Collection on Artificial Intelligence* (UNICRI 2020), pp. 28–29.

97）　De Hert & Sajfert, (n 69) 10–11.

評価され得る。LEDの下で問題となり得る目的の類型は比較的限定されていることを考慮すれば、想定可能な目的類型を法律上より具体的に規定し、これを厳格な比例原則によって統制するというアプローチこそが、法執行領域の特性を反映した最も適切な制度設計であると考えられる。

もっとも、GDPRとLEDとの間における目的の転換については、依然として規律上の不明確さが残る。LED第4条第2項は、法執行目的の内部における目的転換を明示的に規律しており、その要件も比較的明確である。これに対し、法執行目的で取得された個人データをGDPRの適用される目的のために利用等する場面、あるいはGDPRの適用下で取得された個人データを法執行目的のために転用する場面については、前者はLED第9条が、後者はGDPR第2条第2項(d)および前文第19項が方向性を示すにとどまり、具体的な判断枠組みが十分に整備されているとは言い難い。とりわけ、民間事業者が保有する個人データが法執行目的のために所管官庁に提供される後者の場面においては、提供する側のGDPR上の法的根拠と、受領する側のLED上の法的根拠とは、必ずしも連動するものではない。すなわち、提供行為がGDPR上正当化されるとしても、そのことは受領後の利用等のLED上の適法性を自動的に担保するものではなく、所管官庁は受領後の利用等についてLED上の独自の法的根拠を別途有していなければならない。しかし、この点を明示的に規律する条文は存在せず、提供側のGDPR上の法的根拠と受領側のLED上の法的根拠との関係は、今後の判例の蓄積に委ねざるを得ない。

五　おわりに

本稿は、LEDにおける個人データ取得・利用等の正当化構造を基礎づける「適法性」原則、ならびに「目的特定」・「目的拘束」原則について検討してきた。以上の検討から、法執行分野における個人データ取得・利用等の最低限の基準として、少なくとも次の三点が導出される。第一に、個人データの取得・利用等に関する法的根拠は、単なる権限付与規定にとどまらず、目的・対象・手段・限界を具体化し、所管官庁の裁量を拘束し得

るものでなければならない（「適法性」原則）。第二に、そのような法的根拠においても、「法執行一般」又は法執行活動の類型を抽象的に掲げるだけでは足りず、個々の取得・利用等目的が具体的に特定されなければならない（「目的特定」原則）。第三に、取得時の目的とは異なる目的のために個人データを利用等する場合には、同一の法執行領域内であっても、別途の法的根拠および必要性・比例性の審査が求められる（「目的拘束」原則）。

これらは、いずれも「はじめに」で提示した問い――法執行分野において国家による個人情報の取得・利用等の最低限の基準をいかに画定すべきか――に対する基礎的かつ重要な回答を構成するものである。これらの原則から導かれる理解は、日本法に対しても重要な示唆を与える。その示唆は、日本において法執行分野に関する特別法を設けるべきかという制度形式の問題にとどまるものではない。より重要なのは、法執行分野における個人情報の取得・利用等について、取得時の根拠だけでなく、取得後の保管・分析・共有・再利用に至るまで、法的統制の対象として把握する必要があるという点である。

この問題を具体的に示すのが、名古屋高裁判決（令和 6 年 8 月30日）[98]の事案である。同判決において問題となったのは、逮捕・捜査の過程で取得されたDNA型データを無罪確定後も継続保管することが、取得時の目的から逸脱する「目的変更」に当たるかという点であった。この点につき、国側は、国家公安委員会DNA型記録取扱規則第 1 条が「もって犯罪捜査に資すること」という目的を定めており、取得時も保管時も目的は同一である以上、目的変更は生じていないと主張した。

しかし、本稿が検討したLEDの「目的特定」原則に照らすと、このような主張には根本的な問題がある。LEDにおいては、「法執行それ自体」はもとより、第 1 条第 1 項に列挙された目的類型のいずれかを示すだけでは、当該取得・利用等の目的が「特定」されたことにはならない。かかる目的類型はあくまで「目標」であって、個別の取得・利用等が「何のために」「いかなる文脈において」行われるのかを具体的に示す「目的」と

98）　名古屋高裁・前掲注 6 ）。

は区別されなければならないからである。この観点からすれば、「犯罪捜査に資すること」という文言は、あらゆる将来の犯罪捜査に資する可能性を常に包含するような、過度に包括的な目的にとどまる場合には、当該目的変更が「目的拘束」原則を充足しているかを判断する基準が機能しなくなり、形骸化する。名古屋高裁が「一般的、抽象的な安心安全を唱えることによって、国民個々人の人権ないし自由を軽視し、捜査機関の便宜を優先して、恣意的な判断を押し通そうとするものといわざるを得ず、到底許容できるものではない」と断じた趣旨も、かかる構造的問題を射程に収めていると読み取ることができる。

さらに、*Inspektor*判決が明らかにしたように、「捜査」と「訴追」でさえ、LED第1条第1項上は相互に区別された独立の利用目的として把握されなければならず、目的変更として新たな法的根拠と必要性・比例性の再審査が求められる。特定事件の捜査目的で取得されたDNA型データを、当該事件の無罪確定後もなお保管し続けることが当初目的の継続として正当化し得ないことは、この観点からも明らかといえる。

以上を踏まえると、日本法への示唆として少なくとも次の点を指摘することができる。法執行目的の個人情報の取得・利用等を根拠づける法的根拠は、「犯罪捜査に資すること」といった包括的記述にとどまらず、具体的目的・対象・手段・限界を法律レベルで特定・明確にしたものでなければならない。そして、取得・利用等の各局面において別個の法的根拠と比例性審査が求められる以上、現行の内部規則への依存は、法治国家が個人情報の取得・利用等に課すべき最低限の規律を欠くものと把握されるべきである。名古屋高裁判決が指摘するとおり、「本来は、そのようなことを防止するための国会による立法措置が必要であ」って、「憲法の趣旨に沿った立法による整備が行われることが強く望まれる」ところである。

本稿が検討した「適法性」原則および「目的特定」・「目的拘束」原則は、法執行分野における個人データ取得・利用等の正当化構造の基盤をなすものである。データ最小化原則・保存期間の制限・データ主体の類型に応じた個人データの区別といった諸原則は、いずれも法的根拠と特定された目的を前提として初めて実質的に機能し得るものである。比較衡量を内容と

するこれらの諸原則については、法執行分野における個人情報の取得・利用等の法的統制をより具体化する課題として、今後さらに検討することとしたい。

〔付記〕 本研究は、潮田記念基金による博士課程学生研究支援プログラムの補助を受けたものです。

韓　修玼（ハン　スビン）
所属・現職　慶應義塾大学大学院法学研究科後期博士課程
韓国憲法裁判研究院国外通信員
旧優生保護法問題検証会議調査補助員
最終学歴　慶應義塾大学大学院法学研究科修士課程
所属学会　全国憲法研究会、憲法理論研究会、比較憲法学会
専攻領域　憲法
主要著作　「韓国における個人情報保護の憲法理論と実務」『慶應義塾大学大学院法学研究科論文集』第64号（2024年）。
「DNA型データベースに関する韓国法の基本構造：日本法との比較を含めて」『法律学研究』第70号（2023年）。
“생활보호기준 인하의 위법성과 생존권의 구체화—최고재판소 2025년6월27일 오사카 소송 판결을 중심으로—”［生活保護基準の引下げと生存権の具体化—最高裁判所2025年6月27日大阪訴訟判決を中心に—］,『세계헌법재판 조사연구보고서』［世界憲法裁判調査研究報告書］2026年第3号（通巻第78巻）。