国立国会図書館 調査及び立法考査局
Research and Legislative Reference Bureau
National Diet Library

論題 Title	欧州における顔認識技術の規制と基本権―EU の立法動向と欧州人権裁判所の判例―
他言語論題 Title in other language	European Regulatory Frameworks for Facial Recognition Technology and Fundamental Rights: Legislation in the EU and a Case by the European Court of Human Rights
著者 / 所属 Author(s)	門谷 春輝（KADOTANI Haruki）/ 前　国立国会図書館調査及び立法考査局　憲法課
雑誌名 Journal	レファレンス（The Reference）
編集 Editor	国立国会図書館 調査及び立法考査局
発行 Publisher	国立国会図書館
通号 Number	904
刊行日 Issue Date	2026-4-20
ページ Pages	61-80
ISSN	0034-2912
本文の言語 Language	日本語（Japanese）
摘要 Abstract	欧州における法執行分野の顔認識技術の規制について、EU 基本権憲章、刑事司法指令、AI 規則などの立法動向、2023 年の欧州人権裁判所判決を紹介し、基本権との関係性を検討する。

欧州における顔認識技術の規制と基本権
―EU の立法動向と欧州人権裁判所の判例―

前　国立国会図書館　調査及び立法考査局
憲法課　門谷　春輝

目　　次

キーワード：顔認識技術、EU 基本権憲章、刑事司法指令、AI 規則、欧州人権条約

要　旨

① 近年、カメラの性能の向上や、機械学習の一種である深層学習の進展に伴い、顔認識技術の利用が急速に拡大している。特に法執行分野の顔認識技術の利用に関しては、テロ対策や治安維持等に有用である一方、差別のリスクを始めとする基本権の侵害、誤認逮捕等への懸念が指摘されている。

② 近年では、一部の EU 加盟国で顔認識技術の実証実験が行われるようになっており、2019 年にフランス・ニース市で実施された実証実験はその代表例である。実証実験の進展を背景として、EU では顔認識技術の実用化に当たって基本権の観点から留意すべき課題が整理されている。様々な基本権を侵害する懸念から、特にリアルタイム顔認識（又はライブ顔認識）と呼ばれる顔認識技術の類型に対する規制の重要性が強調されている。

③ EU における法執行分野の顔認識技術の主な規制枠組として、EU 基本権憲章及び刑事司法指令に加えて、2024 年に制定された AI 規則が挙げられる。刑事司法指令は、法執行分野の個人データ保護の規制枠組であり、生体データの取扱いに係る規律を定めている。AI 規則は、特定の顔認識技術（法執行目的の公共空間におけるリアルタイム遠隔生体識別）の利用を原則として禁止しており、刑事司法指令の特別法として位置付けられている。

④ AI 規則では、行方不明者の捜索、テロ攻撃の防止、犯罪捜査を目的とする場合に限り、リアルタイム遠隔生体識別について、例外的な利用が認められている。その利用に当たっては、AI 規則で手続が定められており、最終的な判断は EU 加盟国の裁判所等に委ねられている。この点、法執行機関の権力の濫用を招くおそれがある点で批判も寄せられている。

⑤ 欧州人権裁判所が 2023 年に示した Glukhin v. Russia 判決は、同裁判所として顔認識技術に関する初の司法判断として注目されている。本判決では、警察によるリアルタイム顔認識を用いた捜査が欧州人権条約の表現の自由、私生活及び家族生活の尊重を受ける権利に違反すると判断したものである。欧州人権条約は、EU 法の法源の一つとして位置付けられており、EU 法、とりわけ AI 規則の解釈の指針となり得ると考えられている。

はじめに

近年、カメラの性能の向上や、機械学習（machine learning）(1)の一種である深層学習（deep learning）(2)の進展によって、様々な分野で顔認識技術（facial recognition technology）の利用が急速に拡大している。そのうち、犯罪捜査・予防等を目的とする法執行（law enforcement）(3)分野の顔認識技術の利用に関して、差別のリスクを始めとする基本権(4)の侵害、誤認逮捕等の懸念が指摘されており(5)、各国や国際的なレベルでその規制へ向けた具体的な取組が実施されている(6)。本稿では、欧州における法執行分野の顔認識技術の利用規制に注目する。

欧州連合（European Union. 以下「EU」という。）は、2024年制定の包括的な人工知能（Artificial Intelligence. 以下「AI」という。）規制立法であるAI規則（Artificial Intelligence Act）(7)において、基本権侵害のリスクの強弱に応じて、AIシステムに対する規制を類型化している。AI規則第5条第1項（h）は、「法執行を目的として、公衆がアクセス可能な場所内で、リアルタイム遠隔生体識別システム（real-time remote biometric identification system）を使用すること」(8)を原則

＊本稿の内容は、2026年1月22日現在の情報に基づく。インターネット情報の最終アクセス日も、同日である。また、文中で言及する人物の肩書は、当時のものである。

(1) 機械学習とは、1950年代に「明示的にプログラミングすることなく、コンピュータに学ぶ能力を与えようとする研究分野」として始まったものである（神嶌敏弘「機械学習の動向と深層学習の位置づけ」中島秀之ほか編『AI事典　第3版』近代科学社, 2019, p.80.）。

(2)「深層学習とは、層の数が多い（深い）階層構造を持つニューラルネットワーク（深層ニューラルネットワーク）をモデルとして用いる機械学習の1種である。」（麻生英樹「深層学習・表現学習」同上, p.84.）

(3) 法執行とは、「実力の裏づけのもとに法の違反を抑制し、秩序を維持する警察官、保安官などの作用」をいう（田中英夫編集代表『英米法辞典』東京大学出版会, 1991, p.500.）。

(4)「基本的人権」及び「人権」と同義に用いられる場合には、「人がただ人間であることにより当然に有する権利」とされる（佐藤幸治「基本的人権・人権・基本権」大須賀明ほか編『三省堂憲法辞典』三省堂, 2001, p.73.）。欧州連合（European Union: EU）では、保護の対象となる基本権のカタログとして「EU基本権憲章」が規定されている（後述第Ⅱ章第1節参照）。

(5) Caroline Lequesne and Céline Castets-Renard,“Law Enforcement Technologies: The Realm of Facial Recognition,” *European Review of Digital Administration & Law*, vol.6 iss.1, 2025.11, p.5. <https://www.erdalreview.eu/free-download/97912218211161.pdf>

(6) 小川有希子氏（帝京大学）は、「表現の自由や内心の自由に対する侵害、偏見や差別の問題、公共空間における匿名性の低下、監視社会への不安、取得される情報の膨大さなど、その社会の文化的歴史的背景によってリスク評価項目の比重は異なるものの、顔認識技術に対する予防的措置の必要性が、先進諸国において認識されている。」と指摘している（小川有希子「顔認識技術の法規制」『法学館憲法研究所Law Journal』30・31号, 2024.10, p.52.）。

(7) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 2024/1689, 2024.7.12. <http://data.europa.eu/eli/reg/2024/1689/oj>「AI法」とも呼ばれるが、法形式が「規則」（regulation. 加盟国に直接適用される。）であるため、本稿では「AI規則」と訳す。条文の翻訳については、井奈波朋子訳『外国著作権法令集（63）―EU AI規則 編―条文』著作権情報センター, 2025, pp.1-149. <https://www.cric.or.jp/db/world/EU_AI/AI_article.pdf> を参考に、適宜用字を変更している。

(8) 同上, p.14; *ibid.* リアルタイム顔認識は、基本権侵害のリスクが特に高い顔認識技術の類型であると考えられている。AI規則は、「リアルタイム遠隔生体識別システム」（real-time remote biometric identification system）を「生体データの取得、比較および識別のすべてが著しい時間的格差なく行われる遠隔生体認証システムであり、即時の識別だけでなく、あらゆる規制回避を避けるため限定的な短い時間的格差があるものを含む」と定義し（第3条第42項）、禁止されるAI実務（第Ⅱ章）の一つに指定している。他方で、「リアルタイム遠隔生体識別システム以外の遠隔生体識別システム」を「事後的遠隔生体識別システム」（post remote biometric identification system）と定義し（第3条第43項）、高リスクAIシステム（第Ⅲ章）に指定している（同, p.14; *ibid.*）。なお、リアルタイム顔認識は、ライブ顔認識（live facial recognition）とも呼ばれるが、本稿ではこれらを同義のものとして扱う。

として禁止するものである。この規定は特定の顔認識技術を念頭に置いたものとされるが(9)、顔認識技術が犯罪捜査・予防等に有用であることから、一定の条件を満たす場合に例外が認められている。AI 規則は、EU 基本権憲章（Charter of Fundamental Rights of the European Union）(10)及び刑事司法指令（Law Enforcement Directive: LED）(11)と並んで、EU における法執行分野の顔認識技術の規制枠組の中核を成している。

また、欧州評議会（Council of Europe: CoE）(12)の司法機関である欧州人権裁判所（European Court of Human Rights: ECtHR）(13)は、2023 年の Glukhin v. Russia 判決(14)において、同裁判所として顔認識技術に関する初の司法判断を示した。本判決は、EU の立法等を参照した上で、警察によるリアルタイム顔認識を用いた捜査が欧州人権条約に違反すると判断したものであり、EU の規制枠組みとも密接に関連している。

以下では、顔認識技術の概略を説明した上で（第Ⅰ章）、AI 規則を始めとする EU の立法動向を概説し（第Ⅱ章）、欧州人権裁判所の判例を検討する（第Ⅲ章）。

Ⅰ　顔認識技術とは

1　略史

コンピュータを用いた顔認識の研究は、東西冷戦下の 1960 年代に諜報活動への応用を主な目的として開始された。しかし、この時期はコンピュータの黎明期に当たり、ほとんど成果を上げることができなかった(15)。

⑼　古川直裕「第 1 回　総則と禁止 AI（1 条～ 5 条）」古川直裕ほか編著『EU　AI 法概説』（別冊 NBL　No.192）商事法務, 2025, p.7.

⑽　Charter of Fundamental Rights of The European Union, OJ C 326, 2012.10.26, pp.391-407. EUR-Lex Website <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>「この憲章は、…（中略）…とりわけ加盟国に共通する憲法の伝統及び国際法上の義務、人権及び基本的自由の保護のための条約、連合及び欧州評議会の採択した社会憲章並びに欧州司法裁判所及び欧州人権裁判所の判例法から生じる権利を再確認する」（前文）。翻訳として、岡久慶・山口和人訳「欧州連合基本権憲章」『外国の立法』No.211, 2002.2, pp.14-20 を参照。

⑾　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, OJ L 119, 2016.5.4, pp.89-131. <http://data.europa.eu/eli/dir/2016/680/oj> 条文の翻訳として、石井夏生利『EU データ保護法』勁草書房, 2020, pp.301-351 を参照。

⑿　欧州評議会は、「人権、民主主義、法の支配の分野で国際社会の基準策定を主導する汎欧州の国際機関として、1949 年フランスのストラスブールに設立され」、「伝統的に人権、民主主義、法の支配等の分野で活動しており、最近では薬物乱用、サイバー犯罪、人身取引、テロ対策、偽造医薬品対策、女性に対する暴力、子供の権利、AI 等の分野にも取り組んでい」る。欧州の 46 か国が加盟しており、日本を含む 5 か国がオブザーバー国である。「欧州評議会（Council of Europe）」2025.2.21. 外務省ウェブサイト <https://www.mofa.go.jp/mofaj/area/ce/index.html> なお、2022 年 2 月 24 日以降のロシア連邦によるウクライナ侵略を受けて、欧州評議会の閣僚委員会は「ロシア連邦は 2022 年 3 月 16 日から欧州評議会の加盟国であることを止める」旨の決定を下した。そのため、欧州人権条約第 58 条第 3 項の規定に基づき、ロシア連邦は 2022 年 9 月 16 日限りで欧州人権条約の締約国ではなくなった。ただし、欧州人権裁判所の裁判官会議は、同日までに生じた条約違反に関してロシア連邦に対する申立があればそれを処理する権限があること等を確認する旨を決議している（清水賢「欧州評議会によるロシア連邦の除名―ウクライナ侵略を受けて―」『立法と調査』452 号, 2022.12, pp.111-120. <https://www.sangiin.go.jp/japanese/annai/chousa/rippou_chousa/backnumber/20221216.html>）。

⒀　欧州人権裁判所の任務は、欧州人権条約（European Convention of Human Rights）を適用し、「加盟国が当該条約に規定された権利や保障事項を尊重することを保証にすること」である（ヨーロッパ人権裁判所『よくある質問とその答え』pp.3-4. <https://www.echr.coe.int/documents/d/echr/Questions_Answers_JPN>）。なお、欧州人権裁判所の判例動向を解説した主な書籍として、戸波江二ほか編『ヨーロッパ人権裁判所の判例　Ⅰ』信山社出版, 2019; 小畑郁ほか編『ヨーロッパ人権裁判所の判例　Ⅱ』信山社出版, 2019 がある。

⒁　Glukhin v. Russia, Judgement, ECtHR, App. No. 11519/20, 2023.7.4. <https://hudoc.echr.coe.int/?i=001-225655>

⒂　今岡仁『顔認証の教科書』プレジデント社, 2021, p.127.

1970年代に入ると、顔画像自動認識技術が登場した。昭和45（1970）年に開催された日本万国博覧会（大阪万博）では、訪問者の顔画像から顔の輪郭を抽出し、そこから得られる特徴量から性格診断を行う「コンピュータ天眼鏡」が展示され、顔認識技術の研究への機運が醸成された。また、昭和48（1973）年に金出武雄氏が京都大学に提出した博士論文は、顔認識技術の研究の先駆けとして引用される(16)。

1980年代には、顔認識技術の研究は停滞していた。一方、1990年代以降は、コンピュータの処理性能の向上、商用利用への関心が高まったこと等を背景として、顔認識技術の研究への関心が著しく増大した(17)。1990年代には、統計的な分析手法を応用した方法を始めとして、顔認識を自動化するための研究が行われたものの、実用化は難しいとされた(18)。

2000年代に入ると、顔認識技術の普及を後押しする出来事が相次いだ。2001年1月に、米国・フロリダ州で開催されたナショナル・フットボール・リーグ（National Football League: NFL）の優勝決定戦「スーパーボウル」では、現地警察による顔認識技術の実証実験が行われ、約10万人の観客の中から犯罪歴のある19名を識別することに成功した。この実証実験では警察による職務質問等は行われなかったが、公共の安全と個人のプライバシーのバランスをめぐる課題が社会に問いかけられた。また、2001年9月に発生した米国同時多発テロ事件を契機として、国際民間航空機関（International Civil Aviation Organization: ICAO）は、各国に対し、パスポート等の渡航文書に顔画像等の生体情報を電磁的に記録することを義務付けた(19)。

2010年代以降、深層学習を用いた手法が注目を集めている(20)。この手法は、2011年頃から顔認識を含む物体認識に応用され始め、2015年には人間に匹敵する性能を獲得したとされる(21)。近年、顔認識技術は、高い利便性と精度を兼ね備えた生体認証（biometrics. バイオメトリクス）(22)の方法として、幅広い用途で普及が進んでいる(23)。

2　概要

顔認識技術には、「顔認証」（facial verification）、「顔識別」（facial identification）という2つの認証方法がある(24)。顔認証とは、「一対一照合」（1:1 matching）とも呼ばれ、2枚の画像を照合し、同一人物か否かを判定する方法である。顔識別とは、「一対他照合」（1:N matching）

---

⑯　同上, pp.128-129; Takeo Kanade, *Picture Processing System by Computer Complex and Recognition of Human Faces*（計算機結合による画像処理システムと顔の認識）, 京都大学, 1973, 工学博士, 甲第1486号. <https://doi.org/10.14989/doctor.k1486>

⑰　Wenyi Zhao et al.,“Face Recognition: A Literature Survey,”*ACM Computing Surveys*, vol.35 iss.4, 2003.12, p.402. <https://doi.org/10.1145/954339.954342>

⑱　今岡　前掲注⑮, pp.131-132.

⑲　同上, pp.132-134.

⑳　Murat Taskiran et al.,“Face recognition: Past, present and future (a review),”*Digital Signal Processing*, vol.106, 2020.11, p.2. <https://doi.org/10.1016/j.dsp.2020.102809>

㉑　岡谷貴之「物体認識」中島ほか編　前掲注⑴, p.192.

㉒　生体認証とは、人の身体的な特性・特徴や行動的な特性・特徴に基づいて、その人物を自動的に識別・確認することをいう（大阪大学「モダリティ別の技術動向」国立国会図書館調査及び立法考査局編『生体認証技術の動向と活用―科学技術に関する調査プロジェクト2018報告書―』（調査資料2018-6）国立国会図書館, 2019, p.2.（村松大吾執筆部分）<https://doi.org/10.11501/11257103>）。

㉓　今岡　前掲注⑮, pp.28-32.

㉔　派生技術として、顔検出、異常検出、属性推定、健康や感情の分析等が挙げられるが（大阪大学「分野別の実用化動向」国立国会図書館調査及び立法考査局編　前掲注㉒, pp.44-47.（岸本充生執筆部分）<https://doi.org/10.11501/11257104>）、本稿では検討しない。

とも呼ばれ、多数の人物の中からある1名を探し出す方法である[25]。

顔認識技術の基本的な処理[26]は、①画像や映像の入力、②顔の検出･位置合わせから成る「前処理」(preprocessing)、③特徴抽出・画像の照合から成る「認識」(recognition)、④結果の出力の順に行われる[27]。③の特徴抽出とは、顔画像からその特徴を抽出し、数値データ（特徴量）に置き換える処理のことをいう。顔認識技術の認証精度は、この特徴抽出に用いられるAIの性能に大きく依存している[28]。すなわち、顔認識技術とは、顔の特徴を表す数値データの類似度をコンピュータで計算することにより、本人確認や識別を行う技術である。

3　利用動向と課題

これまで、米国や英国では法執行分野の顔認識技術の利用が積極的に行われてきた一方、EUではその利用は活発ではないとされてきた[29]。しかし、近年では、一部のEU加盟国で実証実験が行われたことを一つの契機として、基本権の侵害への懸念や実用化に向けた課題が論じられている。

カロリーヌ・ルケーヌ（Caroline Lequesne）氏（コートダジュール大学）によると、フランスでは、①文化的イベント、②教育機関、③サッカー場等の競技場といった特定の場面において、リアルタイム顔認識の実証実験が行われている。そのうち、最も広く知られているのが、2019年2月、フランス・ニース市で開催のカーニバルで実施された顔認識技術の実証実験である[30]。

ニース市は、既に市内に設置されていたCCTV（closed circuit television. 以下「監視カメラ」という。）に顔認識ソフトウェアを組み込んだ上で、群集から対象者を発見する顔識別等を試行した。同市によると、約5,000人のボランティアが参加したこの実証実験では、誤認識は報告されていない。後に、フランスのデータ保護機関である情報処理及び自由に関する国家委員会（La Commission Nationale de l'Informatique et des Libertés: CNIL）は、同市に対し、顔認識技術の有効性､肌の色や性別に基づく偏見が生じた場合の影響について報告を求めた[31]。しかし、同市は、顔認識技術の開発主体が民間企業であることから、技術の詳細に関する説明を行うことができなかったとされる[32]。

EU基本権庁（European Union Agency for Fundamental Rights）[33]の長官であったミカエル・オ

⑵⑸　Md. Tahmid Hasan Fuad et al.,“Recent Advances in Deep Learning Techniques for Face Recognition,”*IEEE Access*, vol.9, 2021, p.99112. <https://doi.org/10.1109/ACCESS.2021.3096136>

⑵⑹　今岡仁氏（日本電気株式会社）は、顔認証の代表的な用途として空港の入国審査、顔識別の代表的な用途としてオフィスビルの入退場管理を挙げている。5,000人の社員が登録されたオフィスビルの入退場管理の場合、顔認証と同様の処理を5,000回繰り返し、一番近い人物を本人とみなすことから、顔認識技術の基本的な処理は顔認証であると指摘している。今岡　前掲注⑴⑸, pp.102-104.

⑵⑺　Fuad et al., *op.cit.*⑵⑸, p.99113.

⑵⑻　今岡　前掲注⑴⑸, pp.107-112.

⑵⑼　大阪大学「海外の法規制及び社会動向」国立国会図書館調査及び立法考査局編　前掲注⑵⑵, pp.52-56, 70-85, 90.（岸本充生執筆部分）<https://doi.org/10.11501/11257105>

⑶⑽　Caroline Lequesne,“Facial Recognition Through the Lens of National Legislations - France,”*European Review of Digital Administration & Law*, vol.6 iss.1, 2025.11, pp.37-38. <https://www.erdalreview.eu/free-download/97912218211165.pdf>

⑶⑴　Martin Untersinger,“Reconnaissance faciale: la CNIL tique sur le bilan de l'expérience niçoise,”2019.8.28. Le Monde Website <https://www.lemonde.fr/pixels/article/2019/08/28/reconnaissance-faciale-la-cnil-tique-sur-le-bilan-de-l-experience-nicoise_5503769_4408996.html> ニース市による実証実験の報告書として、Ville de Nice, *Rapport: Expérimentation Reconnaissance Faciale*, 2019. <https://embed.documentcloud.org/documents/6350838-Bilan-Reconnaissance-Faciale/> を参照。

⑶⑵　Lequesne, *op.cit.*⑶⑽, p.38.

⑶⑶　EU基本権庁とは、「EU機関及び構成国が措置を採ったり、行動指針を決めたりする際に、基本権に関する支

フラヘッティー（Michael O'Flaherty）氏は、2020年2月に、顔認識技術と基本権についての論文を公表した。この論文は、EU基本権庁が2019年に公表した報告書「顔認識技術：法執行の文脈において考慮すべき基本権」（Facial recognition technology: fundamental rights considerations in the context of law enforcement）(34)に基づき、前述のニース市での実証実験を始めとする複数の実証実験の事例を引用した上で、顔認識技術の実用化に当たって基本権の観点から留意すべき課題を整理したものである(35)。

オフラヘッティー氏によると、基本権への影響は、顔認識技術の利用の目的・文脈・射程により異なるが、主にその精度が不十分であることに起因するものである。例えば、顔認識技術は、女性や有色人種に対する誤認識の割合が高いことが報告されており、差別が懸念される。しかし、その精度が完全であったとしても、顔画像の収集・処理が本人同意やオプトアウトの機会を経ずに行われるため、人間の尊厳に対して負の影響を与えるほか、特に顔識別は集会及び結社の自由、表現の自由に対する萎縮効果（chilling effect）をもたらす。さらに、プライバシーは、リベラル・デモクラシーや多元的な社会に固有の中核的価値であるため、大量の個人データの処理によってプライバシーが簒奪（さんだつ）されると、民主主義の機能そのものに重大な影響を及ぼす(36)。

このような基本権侵害の懸念を踏まえて、オフラヘッティー氏は、顔認識技術の実用化に当たって留意すべき点として、以下の6項目を挙げている(37)。

① 顔認識技術の利用は、明白で詳細な法的枠組みにより規制されなければならない。

② 顔認証と顔識別を区別した上で、基本権侵害のリスクがより大きいと考えられる顔識別について、より厳格な必要性（necessity）と比例性（proportionality）(38)の基準が適用されなければならない。

③ ライブ顔認識（live facial recognition）は、特に問題となる。その利用は、テロリズムや重大犯罪の予防、行方不明者の捜索等の目的に限定して行われるべきである。

④ 顔認識技術のアルゴリズムは、確定的な結果を出力するものではなく、2枚の顔画像を比較して同一人物である確からしさを提示するものである。これは、法執行の文脈では、一定の割合で誤認識が生じることを意味する。顔認識技術を利用する際には、誤認識のリスクを最小限にしなければならない。

⑤ 公的部門は、顔認識技術の開発や運用を民間企業に依存している。そのため、その使用

援及び専門知識を提供することを目的とする」機関であり、他のEU機関から「完全に独立して任務を遂行する、専門機関」である。中西優美子『EU基本権の体系』法律文化社, 2024, pp.58-59.

(34) European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2020. <https://doi.org/10.2811/231789>

(35) Michael O'Flaherty, "Facial Recognition Technology and Fundamental Rights," *European Data Protection Law Review*, vol.6 iss.2, 2020.2, pp.170-173. <https://doi.org/10.21552/edpl/2020/2/4> オフラヘッティー氏は、EU加盟国における法執行分野の顔認識技術の利用動向として、フランス・ニース市での実証実験に加えて、2018年にドイツ・ベルリンで行われた実証実験にも言及している。

(36) *ibid.*, p.171.

(37) *ibid.*, pp.172-173.

(38) EU基本権憲章第52条第1項は、「この憲章において認められる権利及び自由の行使に対するいかなる制限も、法律によって規定され、これらの権利及び自由の本質的内容を尊重しなければならない。比例性の原則を条件として、制限は、それが必要であり、かつ連合によって認められた一般利益の性質を有する目的又は、他者の権利及び自由を保護する必要性に明白に合致する場合にのみ行うことが許される。」と規定している。岡久・山口訳前掲注(10), p.20.

や契約に当たって、基本権の観点が組み込まれなければならない。

⑥　顔認識技術の利用に当たって、基本権影響評価（Fundamental Rights Impact Assessment）が不可欠であるが、それを実施するために、公的部門は顔認識技術の技術的詳細を含む全ての情報を保有しなければならない。営業秘密等によって、この取組が妨げられるべきではない。

Ⅱ　EU の立法動向

本章では、法執行分野の顔認識技術の利用規制について、EU における立法の動向を概説する。EU のデータ保護機関である欧州データ保護機関（European Data Protection Board: EDPB）が2023 年 4 月に採択した「法執行分野における顔認識技術の利用に関するガイドライン」（Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement）(39)は、EU 基本権憲章及び刑事司法指令に言及の上、次のように指摘している。

「顔認識技術の利用は、特別な種類の個人データを含む個人データの処理と深く結び付いている。さらに、EU 基本権憲章に規定された数多くの基本権に直接的又は間接的な影響を及ぼす。これは、法執行や刑事司法（criminal justice）の分野において特に重要である。したがって、顔認識技術の利用は、適用され得る法的枠組みを厳格に遵守しつつ行われるべきである。」(40)

2024 年に制定された AI 規則は、EU 基本権憲章で明示された基本権の保障が目的の一つとされているほか、刑事司法指令の特別法(41)として位置付けられている。以下では、EU 基本権憲章、刑事司法指令及び AI 規則を紹介し、これらの立法の関係性を整理する。

1　EU 基本権憲章

EU 法の法源(42)は、第一次法（primary law）と第二次法（secondary law）に区分される。このうち、EU 基本権憲章は、EU 条約（Treaty on European Union）(43)、EU 運営条約（Treaty of the Functioning of the European Union）(44)、EU 司法裁判所（Court of Justice of the European Union: CJEU）の判例法等と共に、第一次法を構成する法である(45)。その適用範囲は、EU の機関及

---

(39)　European Data Protection Board, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, Version 2.0, 2023. <https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf> このガイドラインは、EU 及び加盟国の立法者、顔認識技術を利活用する法執行機関やその職員に対し、技術の特性や法執行分野において適用され得る法的枠組みに関する情報提供を目的としたものである。2022 年 5 月 12 日に第 1 版（Version 1.0）が採択された後、パブリックコメントを経て、2023 年 4 月 26 日に最終版である第 2 版（Version 2.0）が採択された。

(40)　*ibid.*, p.13.

(41)　「通常は相対的に，「特別法」の適用領域を包摂する一層広い適用領域をもつ法を「一般法」，「一般法」の適用領域の一部を適用領域とするものを「特別法」と呼ぶ。」高橋和之ほか編『法律学小辞典　第 6 版』有斐閣，2025，p.32.

(42)　法源とは、「通常は法を適用するにあたって法として援用しうる法形式，特に裁判官が判決理由でそれを援用して裁判の理由となしうる法形式を意味する。」（同上，p.1243.）。

(43)　Treaty on European Union, OJ C 202, 2016.6.7. <http://data.europa.eu/eli/treaty/teu_2016/oj>

(44)　The Treaty on the Functioning of the European Union, OJ C 326, 2012.10.26, pp.47-390. <http://data.europa.eu/eli/treaty/tfeu_2012/oj>

(45)　庄司克宏『新 EU 法　基礎編』岩波書店，2013，p.198.

び部局である。加盟国には、EU 法を執行する場合に限り、適用される（第 51 条第 1 項）(46)。

顔認識技術による個人データの処理は、私生活の尊重を受ける権利（第 7 条）と個人データ保護権（第 8 条）(47)との関係で問題となる。時間や位置情報に紐（ひも）付けた自然人の顔画像を技術的に処理することによって、ある人物の私生活のほか、人種若しくは民族的出身、健康状態、宗教、日常の嗜好（しこう）、住所、行動等を推知することができる。そのほかにも、顔識別の萎縮効果によって、人間の尊厳（第 1 条）、思想、良心及び宗教の自由（第 10 条）、表現及び情報の自由（第 11 条）、集会及び結社の自由（第 12 条）にも深刻な影響を及ぼすと考えられている(48)。

顔認識技術による個人データの処理に法的根拠を与える法令は、私生活の尊重を受ける権利と個人データ保護権に対する直接的な介入（interference）を構成する。また、EU 基本権憲章第 1 条、第 10 条、第 11 条、第 12 条に対する介入を構成し得るほか、顔認識技術が裁判における決定的な証拠として用いられた場合には、実効的な救済及び公正な裁判に対する権利（第 47 条）、無罪の推定及び防御の権利（第 48 条）にも関連する。この点、顔認識技術に特有の誤認識の可能性に加えて、自動化された意思決定支援システムを過度に信頼してしまう人間の認知的傾向（automation bias. 自動化バイアス）も問題となる(49)。こうした介入は、EU 基本権憲章第 52 条第 1 項及び EU 司法裁判所の判例法に基づき、「法律によって規定され」（provided for by law）、正当な目的を有し、必要性や比例性の原則に沿ったものである限りで正当化される(50)。

２　刑事司法指令

刑事司法指令は、2016 年 4 月に一般データ保護規則（General Data Protection Regulation. 以下「GDPR」という。）(51)、旅客機搭乗者記録指令（Passenger Name Record Directive）(52)とともに採択された、EU における個人データの保護に関する統一的な規制枠組み(53)の一つである。なお、刑事司法指令の法形式は「指令」（directive）であるため、各加盟国は指令に基づき立法

---

(46)　EU 加盟国であるポーランド等、EU 加盟国であった英国には、EU 基本権憲章の適用が除外されている。その経緯について、植月献二「【EU】リスボン条約発効へ」『外国の立法』No.241-2, 2009.11, pp.6-7. <https://doi.org/10.11501/1000016> を参照。

(47)　私生活の尊重を受ける権利（第 7 条）と個人データ保護権（第 8 条）の沿革及びこれらの関係性について論じた学説の紹介として、佐藤太樹「EU のデータ保護法制とデジタル立憲主義―AI 規制の憲法的ガバナンス―」『レファレンス』878 号, 2024.2, pp.30-39. <https://doi.org/10.11501/13336315> を参照。

(48)　European Data Protection Board, *op.cit.*(39), p.14.

(49)　*ibid.*, pp.14-15.

(50)　*ibid.*, pp.15-19.

(51)　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), OJ L 119, 2016.5.4, pp.1-88. <http://data.europa.eu/eli/reg/2016/679/oj> 翻訳として、個人情報保護委員会の仮訳（個人情報保護委員会訳「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（一般データ保護規則）【条文】」<https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf>）を参照。

(52)　Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 2016.5.4, pp.132-149. <http://data.europa.eu/eli/dir/2016/681/oj>

(53)　データの越境保護の観点から、GDPR、刑事司法指令及び旅客機搭乗者記録指令（PNR 指令）の関係性を検討した論文として、星周一郎「GDPR と刑事司法指令・PNR 指令の相関―データの越境移転の規律を中心に―」『ジュリスト』1521 号, 2018.7, pp.20-25 を参照。

の義務を負う(54)。

GDPR は、個人データの取扱いであっても、「公共の安全への脅威からの保護及びその脅威の防止を含め、所管官庁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」(55)には、その適用が除外される（第 2 条第 2 項（d））。この場合に適用される個人データ保護の規制が刑事司法指令である。

顔認識技術による個人データの処理に関連して、刑事司法指令は、顔画像（facial image）を始めとする個人データを生体データ（biometric data）に位置付け、その取扱いに係る規律を設けている。生体データとは、「自然人の身体的、生理的又は行動的な特性に関連する特別な技術的取扱いから得られる個人データであって、顔画像や指紋データのように、当該自然人を一意に識別できるようにするもの、又は、その識別を確認するものを意味する。」(56)と定義される。この点、2018 年に欧州データ保護機関が設立されるまで EU のデータ保護機関であった第 29 条作業部会（Article 29 Data Protection Working Party）は、生体データを「人の身体的特徴を「機械判読可能な」（machine-readable）形式に変換」したものと位置付け、顔写真（photograph of a face）と明確に区別している。すなわち、EU の個人データ保護の文脈では、カメラ等で撮影された顔写真は生体データに該当しない一方、特徴抽出を経た数値データ（特徴量）が生体データの一つである、顔画像と定義される(57)。

生体データは、「特別な種類の個人データ」（special categories of personal data. いわゆる「センシティブデータ」）の一つとして位置付けられている。特別な種類の個人データの処理は、「厳密に必要」（strictly necessary）であって、データ主体の権利及び自由に対する「適切な保護措置」（appropriate safeguards）を講ずる場合に、以下に列挙された場合に限り認められる（第 10 条）。

「（a）EU 法若しくは加盟国法で許可されている。

（b）データ主体若しくは他の自然人の重要な利益を保護するため、又は、

（c）当該取扱いが、明らかにデータ主体によって公開されたデータに関係する場合。」(58)

また、管理者（data controller）は、特別な種類の個人データの処理に関連して、「データ保護・バイ・デザイン及びバイ・デフォルト」（第 20 条）、「データ保護影響評価」（Data Protection Impact Assessment: DPIA）（第 27 条）等の義務を負う。

3　AI 規則

AI 規則は、約 3 年の審議を経て、2024 年 5 月 21 日に欧州理事会（European Council）により正式に採択され、7 月 12 日に EU の官報に掲載された。第 113 条の規定に基づき、官報に掲載されてから 20 日後の 8 月 2 日から効力を有し、原則として 2026 年 8 月 2 日から施行されることが予定されている。ただし、一部の規定については、以下のとおり段階的に施行される。

①第 I 章及び第 II 章：2025 年 2 月 2 日施行

---

(54)　庄司　前掲注(45), pp.210-212. 本稿では、加盟国の国内法については検討しない。

(55)　条文の翻訳として、個人情報保護委員会訳　前掲注(51), p.1 を参照。

(56)　同上, p.5 を参照。なお、生体データの定義は、刑事司法指令（第 3 条第 13 項）及び GDPR（第 4 条第 14 項）で同一である。

(57)　Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies*, 00720/12/EN WP193, 2012.4.27, pp.3-4. European Commission Website <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf>

(58)　条文の翻訳として、石井　前掲注(11), pp.317-318 を参照。

②第 III 章第 4 節、第 V 章、第 VII 章、第 XII 章、及び第 78 条（ただし、第 101 条は除く）：2025 年 8 月 2 日施行

③第 6 条第 1 項及び本規則における該当の義務：2027 年 8 月 2 日施行（予定）

AI 規則の目的は、AI システムの有害な影響から、健康、安全、EU 基本権憲章に明示された基本権を高い水準で保護し、イノベーションの促進、域内市場の機能の向上、人間を中心とする信頼できる AI（Trustworthy AI）の採用を促進することであり（第 1 条）、基本権に対する保護以外にも多様な目的が掲げられている。また、AI 規則の法的根拠は、域内市場の統合に関する EU の権限を定めた EU 運営条約第 114 条に求められる。そのため、AI 規則は、EU における製品安全の取組である NLF（New Legislative Framework）の一環であると指摘される(59)。他方で、AI 規則を始めとする EU の立法の背景に、デジタル立憲主義（digital constitutionalism）(60)と呼ばれる憲法学説が存在するとの立場も有力である(61)。

この点、法執行を目的とする公共空間におけるリアルタイム遠隔生体識別システムの利用を原則として禁止する規定（第 5 条第 1 項（h））は、個人データ保護権との関係性が明確化されている。法執行を目的とする遠隔生体識別等の AI システムの利用に対する制限については、個人データ保護権の保障に関する EU の権限を定めた EU 運営条約第 16 条が法的根拠となる（前文第 3 項）。そのため、AI 規則の当該規定は、同様に EU 運営条約第 16 条に基づき立法された刑事司法指令の特別法（*lex specialis*）と位置付けられている（前文第 38 項）(62)。

AI 規則第 5 条第 1 項（h）は、主に顔識別を念頭に置いた規定であり、国家による監視や誤認識に対する懸念が提起されたため、「禁止される AI 実務」（第Ⅱ章）の中でも最も大きな議論となった(63)。欧州委員会（European Commission）が 2021 年 4 月 21 日に示した AI 規則案は、公共空間における法執行目的のリアルタイム遠隔生体識別を原則として禁止した上で、3 つの例外を認めていた(64)。その後、欧州議会（European Parliament）が例外を容認しない方針を示したため、一時は全面的な禁止が法案に盛り込まれた(65)。しかし、非公式の三者対話（trilogue. トリローグ）(66)において、テロ対策を始めとする犯罪捜査・予防等の例外が再び認められるこ

---

59 弁護士の古川直裕氏（株式会社 ABEJA）は、「AI 法の目的として、基本的人権ももちろん尊重すると書いてはいますが、1 つ目の目的が市場の効率化というところが EU 独自の事情を反映しています。」と指摘している（吉永京子ほか「座談会　EU AI 法を読み解く」古川ほか編著　前掲注(9), pp.110-111.（古川直裕氏発言部分））。NLF 等と AI 規則の関係について、中崎尚ほか「EU AI 法における製品規制枠組みの構造」同, pp.84-94 を参照。

60 山本健人氏（北九州市立大学）によると、デジタル立憲主義とは、EU の AI 規制等の取組に呼応する形で発展してきた、「急速に発展するデジタル技術を扱う私的主体が権力者となりうるデジタル空間に立憲的価値を持ち込むことを志向する新たな研究潮流」である（山本健人「デジタル立憲主義と情報空間の立憲化」『法律時報』96 巻 5 号, 2024.5, p.9.）。

61 同上, pp.8-13; 佐藤　前掲注(47), pp.48-52 を参照。

62 Catherine Jasserand, "The European Regulatory Frameworks for Facial Recognition. From the LED to the AI Act," *European Review of Digital Administration & Law*, vol.6 iss.1, 2025.11, pp.91-92. <https://www.erdalreview.eu/free-download/979122182111610.pdf>

63 古川　前掲注(9)

64 European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative Acts*, COM(2021) 206 final, 2021.4.21. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206>

65 European Parliament, *Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 - C9-0146/2021 - 2021/0106(COD))*, P9_TA(2023)0236, 2024.1.23. <http://data.europa.eu/eli/C/2024/506/oj>

66 三者対話とは、通常立法手続の第一読会において、欧州議会、欧州評議会、及び欧州委員会の代表者により行われる非公式の交渉である。三者対話には、立法成立を促進する側面がある一方、非公式に行われるため透明性

ととなった(67)。リアルタイム遠隔生体識別システムを始めとする定義については、AI 規則第 3 条第 41 項から第 46 項にかけて詳細に規定されている(68)。

また、AI 規則第 5 条第 1 項（h）では、次の目的によるリアルタイム遠隔生体識別システムの使用が必要最小限であり、かつ必要最小限の範囲内である場合には、例外的に認められると規定している。

「（ⅰ）誘拐、人身売買または性的搾取の特定の被害者を対象とする捜索、および行方不明者の捜索；

（ⅱ）自然人の生命もしくは身体の安全に対する特定の、具体的かつ差し迫った脅威の防止、またはテロリスト攻撃の現実かつ現在の、もしくは現実かつ予見可能な脅威の防止；

（ⅲ）附属書Ⅱに定める犯罪であり、かつ、関係する加盟国において最長期間が少なくとも 4 年間である拘禁刑または留置命令によって処罰される犯罪に対する、刑事捜査、訴追または刑事罰の執行を目的とする、刑事犯罪を犯した被疑者の所在の特定または身元の特定。」(69)

これらに関連して、AI 規則第 5 条第 2 項から同条第 8 項にかけては、リアルタイム遠隔生体識別システムの例外的な利用に当たっての手続を定めている(70)。具体的には、利用の契機となった状況の性質、関係者の権利及び自由への影響を考慮することや、第 27 条に基づく基本権影響評価が求められている（第 2 項）。また、その利用に際して、事前又は 24 時間後までに裁判所等から許可を得ることが求められている（第 3 項）。この点、欧州委員会は、2025 年 2 月に「禁止される AI 実務に関するガイドライン」（Guidelines on prohibited artificial intelligence practices）を公表し、例外的な利用の対象となり得る事例やその要件、具体的な手続を明らかにしている(71)。ただし、キャサリン・ジェサランド（Catherine Jasserand）氏（ルーヴェン･カトリック大学）は、このガイドラインに法的拘束力がないことを指摘した上で、「最終的な AI 規則の条文の解釈は、EU 司法裁判所に委ねられている」と述べている(72)。

リアルタイム遠隔生体識別システムの例外的な利用に関しては、具体的な手続が定められているのにもかかわらず、多くの批判も寄せられている。例えば、ナタリー・スムハ（Nathalie A. Smuha）氏（ルーヴェン・カトリック大学）とカレン・ユン（Karen Yeung）氏（バーミンガム大学）は､EU 加盟国が公共空間に顔認識カメラを設置することにより､権限の静かな拡大（function creep）と法執行機関による権力の濫用のおそれが高まっていることを指摘している(73)。

４　小括

本章で概説した EU 基本権憲章、刑事司法指令及び AI 規則は、EU における法執行分野の顔

に欠けるとの批判もある。庄司　前掲注(45), p.91.

(67)　Nathalie A. Smuha and Karen Yeung, “The European Union’s AI Act Beyond Motherhood and Apple Pie?” Nathalie A. Smuha, ed., *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, Cambridge: Cambridge University Press, 2025, p.237. <https://doi.org/10.1017/9781009367783.015>

(68)　条文の翻訳として、井奈波訳　前掲注(7), p.14 を参照。

(69)　AI 規則第 5 条第 1 項（h）の条文の翻訳として、同上, p.19 を参照。同規則附属書Ⅱの条文の翻訳として、井奈波朋子訳『外国著作権法令集（63）―EU AI 規則 編―付属書』著作権情報センター, 2025, p.5. <https://www.cric.or.jp/db/world/EU_AI/AI_Annex.pdf> を参照。

(70)　井奈波訳　前掲注(7), pp.20-22 を参照。

(71)　European Commission, Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 5052 final, 2025.7.29, pp.95-134. <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>

(72)　Jasserand, *op.cit.*(62), p.91.

(73)　Smuha and Yeung, *op.cit.*(67), p.237.

認識技術の規制枠組の中核を成しているが、これらの関係性を整理すると、次のとおりである。

まず、EU 法における第一次法と第二次法の区分に着目すると、EU 基本権憲章は第一次法に当たり、刑事司法指令と AI 規則は第二次法に当たる。刑事司法指令と AI 規則は、ともに個人データ保護権に関連する EU の立法権限を定めた EU 運営条約第 16 条に基づき立法されたものであり、基本権の保障とも密接に関連している。

また、AI 規則は刑事司法指令の特別法であるため、刑事司法指令による生体データの取扱いに係る規律を補完するものである。両者の法形式に着目すると、刑事司法指令の法形式は、加盟国が国内法化する必要のある指令であったのに対して、AI 規則の法形式は、加盟国に直接適用される規則である。このため、AI 規則で規制の対象となったリアルタイム遠隔生体識別システム等に該当する顔認識技術は、これまで刑事司法指令及び加盟国の国内法により規制されていたが、AI 規則の制定によって、加盟国の国内法にかかわらず EU 域内で統一的な規制が設けられることとなった。

AI 規則第 5 条第 1 項（h）は、リアルタイム遠隔生体識別の利用を原則として禁止した上で、犯罪捜査・予防等を目的とする場合に例外を認めているが、課題も指摘されている。例外的な利用の可否を最終的に判断するのは裁判所等であり、AI 規則の条文の最終的な解釈は EU 司法裁判所に委ねられる。この点、欧州人権裁判所が 2023 年に示した判決は、AI 規則の解釈に当たり参考となる可能性がある。そこで、次章では、その判決を紹介した上で、EU 法への示唆を検討する。

Ⅲ　欧州人権裁判所 Glukhin v. Russia 判決

1　事実の概要

本判決[74]の事実の概要は、次のとおりである。

ロシア連邦･モスクワ市内では、2017 年以降、監視カメラの設置台数が急速に増加している。2022 年 9 月 1 日時点では、同市内に設置された 22 万台以上の監視カメラ全てに、ライブ顔認識技術が搭載されている[75]。

申立人であるロシア国籍のニコライ・セルゲイヴィッチ・ガルキン（Nickolay Sergeyevich Glukhin）氏は、政治活動家のコンスタンチン・コトフ（Konstantin Kotov）氏が逮捕・起訴されたことに抗議するため、2019 年 8 月 23 日に、コトフ氏の段ボール製の等身大パネルと抗議文を記した横断幕を掲げて同市内の地下鉄に乗車した（以下「本件抗議活動」という。）[76]。

申立人に対する捜査を開始した警察は、通信アプリ「テレグラム」（Telegram）に投稿された本件抗議活動の写真等のスクリーンショットを収集・保管したほか、複数の地下鉄の駅に設置された監視カメラから映像を入手し、申立人の画像を収集・保管した。これらの画像を照合した結果、申立人の身元と自宅住所が判明した。2019 年 8 月 30 日、同市内に設置された監視カメラと顔認識技術を用いて申立人の居場所を識別した上で、警察は申立人を逮捕した[77]。

後に申立人は、本件抗議活動が行政犯罪法典[78]第 5 節第 20 条第 2 項に違反した疑いで起訴

⑺④ Glukhin v. Russia, *op.cit.*⑴④
⑺⑤ *ibid.*, para.5.
⑺⑥ *ibid.*, paras.6-7.
⑺⑦ *ibid.*, paras.9-12.
⑺⑧ Code of Administrative Offences of the Russian Federation; Кодекс об административных правонарушениях (КоАП

された。ロシア連邦法の公共イベント法[79]は、デモの主催者に対して、「素早く組み立てられた物体」（быстровозводимая сборно-разборная конструкция; quickly (de)assembled object）を使用するデモの開催に当たり、法律で定められた期限内に事前に届出を行うことを義務付けている[80]。

第1審のモスクワ市メシュチャンスキー地区裁判所（Meshchanskiy District Court of Moscow; Мещанский районный суд города Москвы）は、2019年9月23日に、本件抗議活動において「素早く組み立てられた物体」が用いられたことを認定し、行政犯罪法典に基づき罰金20,000ロシア・ルーブル（日本円で約34,000円）[81]の支払を命じる判決を下した。申立人はこの判決を不服として控訴したが、第2審のモスクワ市裁判所（Moscow City Court; Московский городской суд）も、2019年10月30日に、第1審の結論を支持する判決を下した[82]。

申立人は、2020年1月31日に、欧州人権条約（European Convention of Human Rights. 以下「人権条約」という。）[83]第10条（表現の自由）、人権条約第8条（私生活及び家族生活の尊重を受ける権利）等の侵害の被害者であると主張して、人権条約第34条に基づき、欧州人権裁判所へ申立を行った。

欧州人権裁判所（小法廷）が2023年6月13日に下した判決は、本件申立を審理する管轄権の存在を確認した上で[84]、人権条約第8条及び第10条の違反をそれぞれ認定した（後述第Ⅲ章第2節参照）。また、人権条約第41条に基づく申立人の損害賠償請求（請求額15,000ユーロ（日本円で約2,190,000円））について、ロシア連邦政府に対し、9,800ユーロ（日本円で約1,430,800円）の損害賠償[85]と弁護士費用等の支払いを命じた[86]。なお、申立人は、人権条約第6条に基づき、行政犯罪として逮捕・起訴された一連の手続が不当であるとも主張したが、人権条約第8条及び第10条の違反が認定されたこと等を理由に当該主張は退けられた[87]。

2　判旨

本判決の概要は次のとおりである。

(1) 表現の自由

人権条約第10条がいう表現の自由の保障は、話し言葉や書き言葉だけではなく、非言語的な手段又は自然人の行為によっても伝達され得ることを再確認する。本件抗議活動の性質や文脈を考慮すると、申立人が表明しようと試みた意見は、人権条約第10条第2項に基づく制約の余地がほとんどない公共の利害に関するものであったと考えられる。そこで、申立人が逮捕・

РФ).

⑺⑼　The Public Events Act (no. FZ-54 of 19 June 2004); Федеральный закон от 19 июня 2004 года N 54-ФЗ «О собраниях, митингах, демонстрациях, шествиях и пикетированиях».

⑻⓪　Glukhin v. Russia, *op.cit.*⑭, paras.18-20.

⑻①　日本円換算は、令和元（2019）年9月分報告省令レートに基づき1ロシア・ルーブル＝約1.7円として行った。

⑻②　Glukhin v. Russia, *op.cit.*⑭, paras.15-17. ロシア連邦の裁判所制度については、杉浦一孝「裁判制度」小森田秋夫編『現代ロシア法』東京大学出版会, 2003, pp.122-125を参照。

⑻③　人権条約の条文の翻訳は、ヨーロッパ人権裁判所『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』<https://www.echr.coe.int/documents/d/echr/Convention_JPN> を参照。

⑻④　ロシア連邦によるウクライナ侵略により、ロシア連邦は2022年9月16日限りで欧州人権条約の締約国ではなくなったが（前掲注⑿を参照）、欧州人権裁判所は、本件で申し立てられた事実が同日以前に発生したため、本件申立を審理する管轄権を有することを決定した（Glukhin v. Russia, *op.cit.*⑭, paras.41-43.）。

⑻⑤　日本円換算は、令和5（2023）年6月分報告省令レートに基づき1ユーロ＝約146円として行った。

⑻⑥　Glukhin v. Russia, *op.cit.*⑭, paras.93-98.

⑻⑦　*ibid.*, para.92.

起訴され、有罪判決を受けたことは申立人の表現の自由に対する介入（interference）に当たる(88)。

公共イベント法の「素早く組み立てられた物体」という規定は、どのような物体が適用対象か予見可能な基準が含まれていないほか、ロシア連邦の裁判所においても基準の明確化が行われていない。そのため、人権条約第10条第2項がいう「法律によって定められた」（prescribed by law）という基準の予見可能性は疑わしい(89)。

しかし、仮にこの介入が法律によって定められたものであり、正当な目的を追求するものであったとしても、以下の理由から「民主的社会において必要」（necessary in a democratic society）とは認められない。申立人が有罪判決を受けた犯罪は、本件抗議活動に関する事前の届出を怠ったことにとどまり、本件抗議活動が交通の妨げ、暴力行為等により大きな混乱を引き起こしたことは立証されていない。これらの考慮すべき事項に加えて、申立人が段ボール製の等身大パネルを使用したことが意見の表明に当たるかの検討も行われていない。したがって、人権条約第10条の違反が存在する(90)。

(2) 私生活及び家族生活の尊重を受ける権利

(ⅰ) 私生活に対する介入の存在

一般原理として、私生活に関するデータの単なる保管も、人権条約第8条が意味するところの介入（interference）に当たる。当裁判所の判例によれば、公的活動に関するデータの収集・保管や、公共の場所におけるデータ収集は、人権条約第8条がいう介入に当たるとされている(91)。

一般原理を本件に適用すると、警察は、ソーシャルメディアに投稿された本件抗議活動の様子のスクリーンショットを取得・保管し、申立人を識別するために顔認識技術を利用したとされる。本件抗議活動が同市内の地下鉄で行われたことを特定した上で、複数の地下鉄の駅に設置された監視カメラの映像を取得・保管した。また、申立人を逮捕する際にも、ライブ顔認識技術を利用したとされる(92)。

申立人の私生活に関するデータの収集・保管の事実が、人権条約第8条がいう介入に当たる点について、当事者間で争いはない。申立人は、①ソーシャルメディアに投稿された本件抗議活動の様子から申立人を特定するため、及び②申立人を逮捕する際に居場所を特定するために、顔認識技術が利用されたと主張しているが、ロシア連邦政府はこれらの主張に応答していない。ロシア連邦の国内法では、警察が顔認識技術を利用するに当たって公的記録を作成することを義務付けた規定は存在しないため、申立人がこれらの主張を立証することは困難と思われる(93)。

ロシア連邦政府は、顔認識技術の利用を明確に否定していないほか、申立人を識別するために用いた手段について言及していない。申立人によると、警察は逮捕の際にライブ顔認識技術を利用したことを認めている。また、モスクワ市内に監視カメラを設置し、ビデオ監視システムによる対象者の検出・識別を行うことが法令により定められている。当裁判所は、このような背景を考慮して、本件において顔認識技術が利用されたことを認める。したがって、申立人の個人データの処理は、人権条約第8条がいう介入に当たる(94)。

---

(88) *ibid.*, paras.51-53.
(89) *ibid.*, para.54.
(90) *ibid.*, paras.55-57.
(91) *ibid.*, paras.65-67.
(92) i*bid.*, para.68.
(93) *ibid.*, para.69.
(94) *ibid.*, paras.71-73.

（ii）介入の正当化

一般原理として、人権条約第8条がいう介入は、それが法律に基づいたものであり、人権条約第8条第2項がいう正当な目的を追求するものであり、そして「民主的社会において必要」（necessary in a democratic society）である場合にのみ、人権条約第8条第2項に基づいて正当化され得ることを再確認する(95)。

個人データの保護は、人権条約第8条の私生活及び家族生活の尊重を受ける権利の保障の基礎である。国内法は、人権条約第8条と矛盾するような個人データの利用を防止するために、適切な保護措置を講じなければならない。このような保護措置の必要性は、個人データの自動処理が関係する場合、特にそれが警察目的で用いられる場合、そして科学技術が絶えず進歩している場合に、より一層高まる。刑事司法システムにおける現代の科学技術の利用が、技術の利用による潜在的な利益と私生活の尊重という重要な利益との衡量を慎重に行うことなく行われるのであれば、人権条約第8条の保障は容認し難いほどに弱められるであろう(96)。

平和的抗議活動の参加に関する情報等、政治的意見を開示する個人データは、高度の保護を受ける特別なカテゴリーのセンシティブデータに当たる(97)。

したがって、個人データの収集・処理の文脈では、措置の範囲及び適用に関する明白かつ詳細な規則、並びに特に期間、保管、利用、第三者によるアクセス、データの完全性及び機密性を保持するための手続、並びにその破棄の手続等に関する最低限の保護措置を定めることが不可欠である。これによって、濫用や恣意性のリスクに対する十分な保証が与えられる(98)。

これを本件に適用すると、適法性、正当な目的の存在に関する問題は、介入が「民主的社会において必要」であったかという問題と不可分であると考えられるため、以下ではこれらを併せて検討する(99)。

警察による申立人の個人データの収集、ライブ顔認識技術を搭載した監視カメラの設置は、共に法令に基づいて行われており、申立人に対する措置は国内法上の根拠を有している。申立人はこれらの国内法が「法の品質」（quality of law）の要件を満たしていないと主張するが、顔認識技術を導入する上で、濫用や恣意性のリスクに対する強力な保護措置だけでなく、措置の範囲及び適用に関する詳細な規則を設けることが不可欠であると考えられる。ライブ顔認識技術を利用する場合には、このような保護措置の必要性は一層高まる。国内法は、生体データの処理を「司法行政に関連する」場合に広く認めており、これが「法の品質」の要件を満たしているかに対して強い疑念がある。ロシア連邦政府はこの条文の解釈・適用例を示しておらず、国内法上、あらゆる司法手続において顔認識技術の利用、生体データの処理を認めているように思われる。さらに、ロシア連邦政府は顔認識技術の利用に関する保護措置にも言及していない(100)。

本件措置が犯罪防止という正当な目的の下で行われたと仮定すると、今日の欧州が直面する課題の一つである組織犯罪やテロリズムに対する闘いが、捜査・識別を目的とした現代的な科学技術の利用に大きく依存していることは議論の余地がない。しかし、本件で問題となるのは、

---

(95) *ibid.*, para.74.
(96) *ibid.*, para.75.
(97) *ibid.*, para.76.
(98) *ibid.*, para.77.
(99) *ibid.*, para.78.
(100) *ibid.*, paras.81-83.

申立人の個人データの処理が、人権条約第8条第2項に基づいて正当化されたか否かである(101)。

申立人の個人データの処理が、「民主的社会において必要」であったか否かを判断する際には、まず私生活の尊重に対する介入の水準を評価する。警察は、申立人のデジタル画像を収集・保管し、そこから生体データを抽出・処理するために顔認識技術を利用した。これは、①ソーシャルメディアで公開された写真と映像から申立人を識別するため、及び②モスクワ市内の地下鉄に乗車中であった申立人の居場所を特定し、逮捕するために用いられた。これらの措置は、特にライブ顔認識技術に関する限りで、極めて侵襲的（particularly invasive）であると考える。したがって、これらの措置が「民主的社会において必要」とみなされるためには、高い水準の正当化が要求され、特にライブ顔認識技術の利用には最も高い水準の正当化が要求される(102)。

捜査に関連する個人データの処理が「民主的社会において必要」であったかを評価する際に、問題となる犯罪の性質と重大性は考慮されるべきであるが、国内法は、犯罪の性質と重大性にかかわらず、生体データの処理を広範に認めている。また、本件抗議活動は公共の秩序又は交通安全に危険を及ぼすものではなく、この点、既に人権条約第10条の違反を認定している。平和的な抗議活動の参加者を識別し、逮捕することを目的として、極めて侵襲的な顔認識技術を利用することは、表現の自由、集会の自由に萎縮効果を及ぼす可能性があると考えられる(103)。

このような状況で、申立人に対する捜査等のために、ライブ顔認識技術を利用したことは、「差し迫った社会的必要」（pressing social need）に応えるものではなかった(104)。

申立人が表現の自由を行使する文脈で、極めて侵襲的な顔認識技術を利用することは、人権条約が維持・促進する、法の支配による民主的社会の理想と価値に相いれないと結論付ける。申立人に対する捜査等のために、顔認識技術を利用して申立人の個人データを処理することは「民主的社会において必要」であるとはみなされない(105)。

3　本判決の特徴と示唆

(1) 特徴

本判決では、人権条約第10条及び第8条の違反が認定されたが、人権条約第10条の違反を認定するに当たっては、本件抗議活動に公共イベント法を適用したことの是非が問題となった一方、顔認識技術への言及はなかった。そこで、以下では、ソーシャルメディア上の投稿や監視カメラから申立人の画像等を収集・保管し、ライブ顔認識技術を用いた識別を目的として当該画像等の処理を行うロシアの法実践（行政犯罪法典等に基づく。）の人権条約への適合性が問題となった、人権条約第8条の違反を認定した説示（本章第2節（2））に注目し、その特徴を明らかにする。

まず、警察による申立人の私生活に関するデータの収集・保管等が人権条約第8条に対する介入に当たるという点は、当事者間で争いはない。また、欧州人権裁判所は、申立人の証言、監視カメラによる犯罪捜査の実施を規定するロシア連邦の法令等を参照した上で、本件で顔認識技術が利用されたことを認定した（本章第2節（2）（ⅰ）参照）。

(101) *ibid.*, paras.84-85.
(102) *ibid.*, para.86.
(103) *ibid.*, paras.87-88.
(104) *ibid.*, para.89.
(105) *ibid.*, para.90.

次に、人権条約第 8 条に対する介入は、それが「民主的社会において必要」とされる場合に認められる。本判決では、適法性、正当な目的の存在及び「民主的社会において必要」の要件が相互に関連していることから、これらを併せて検討する上で、いわゆる比例原則(106)が用いられている。欧州人権裁判所は、生体データの処理を広範に認めるロシア連邦政府の国内法が「法の品質」の要件に合致するか疑わしいと述べた上で、①ライブ顔認識技術が極めて侵襲的な特性を有すること、及び②人権条約第 8 条＋αの基本権の侵害に着目して、その審査密度を高め、申立人に対する捜査等の目的で顔認識技術を利用したことは人権条約第 8 条に違反すると結論付けた（本章第 2 節（2）（ⅱ）参照）。

この点、②人権条約第 8 条＋αの基本権の侵害に関して、本判決で違反が認定された人権条約第 10 条に加えて、人権条約第 11 条（集会及び結社の自由）に対する萎縮効果を踏まえ、人権条約第 8 条に対する介入を検討する際の審査密度を厳格化した点は、本判決の大きな特徴である。

(2) 示唆

本判決は、顔認識技術の基本権に対する影響について、欧州人権裁判所が示した初の判決として欧州の法律雑誌で引用されている(107)。欧州人権裁判所は、国際連合人権高等弁務官（United Nations High Commissioner for Human Rights）の報告書(108)、欧州評議会のガイドライン(109)、EU の刑事司法指令、及び欧州データ保護機関が 2023 年に公表したガイドライン（第Ⅱ章参照）等を参照した上で、本判決を下しており、欧州や国際的なレベルにおける顔認識技術の規制へ向けた議論や立法動向の影響を受けている。

また、2024 年に欧州評議会の閣僚理事会が「人工知能と人権、民主主義及び法の支配に関する欧州評議会枠組条約」（Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law）(110)を採択し、同年に EU が AI 規則を制定した中で、2023 年に下された「本判決が AI システムや顔認識技術の利用に関する現在の欧州における議論に潜在的な影響を与え得る」と指摘される(111)。そこで、本判決の EU 法、とりわけ AI 規則への示唆を検討する。

フェデリカ・パオルッチ（Federica Paolucci）氏（ボッコーニ大学）によれば、欧州人権裁

---

(106) 目的と手段の均衡を要求する法原則（高橋ほか編　前掲注(41), p.1164.）。

(107) Francesca Palmiotto, “Facial Recognition Before the European Court of Human Rights,” *European Review of Digital Administration & Law*, vol.6 iss.1, 2025.11, p.103. <https://www.erdalreview.eu/free-download/979122182111611.pdf> 判例評釈として、Monika Zalnieriute, “Glukhin v. Russia. App. No. 11519/20. Judgment,” *American Journal of International Law*, vol.117 iss.4, 2023, pp.695-701. <https://doi.org/10.1017/ajil.2023.52> も参照。

(108) United Nations High Commissioner for Human Rights, *Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests*, A/HRC/44/24, 2020.6.24. <https://www.ohchr.org/en/documents/thematic-reports/ahrc4424-impact-new-technologies-promotion-and-protection-human-rights>

(109) Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), *Guidelines on facial recognition*, 2021. <https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html>

(110) Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, CETS 225. <https://rm.coe.int/1680afae3c>「この条約は、人工知能（AI）を主題とする初めての国際約束として、AI システムのライフサイクルにおける活動が、人権、民主主義及び法の支配に合致することを目的としており、締約国による適当な措置の採用・維持や国際協力の奨励等を定めたもの」であり、日本は 2025 年 2 月 11 日に批准している。「人工知能と人権、民主主義及び法の支配に関する欧州評議会枠組条約の署名」2025.2.11. 外務省ウェブサイト <https://www.mofa.go.jp/mofaj/press/release/pressit_000001_01725.html>

(111) Francesca Palmiotto and Natalia Menéndez González, “Facial recognition technology, democracy and human rights,” *Computer Law and Security Review*, vol.50, 2023, p.105859. <https://doi.org/10.1016/j.clsr.2023.105857>

判所が本判決において、基本権に対する有効な保護及び法の支配の原則を意味する「法の品質」に言及し、その内実について詳細な検討を行ったことに関して、EU 法にも共通する要素を見いだすことができる(112)。EU の基本的価値を規範化する EU 条約第 2 条は、EU が人間の尊厳の尊重、自由、民主主義、平等、法の支配、及び少数者に属する者の権利等の人権を尊重し、促進すると規定している。また、EU における不文原則である法の一般原則には、欧州人権裁判所の判例法が含まれる。EU 基本権憲章は、「この憲章は、…（中略）…とりわけ加盟国に共通する憲法の伝統及び国際法上の義務、人権及び基本的自由の保護のための条約、連合及び欧州評議会の採択した社会憲章並びに欧州司法裁判所及び欧州人権裁判所の判例法から生じる権利を再確認する」（前文）として、法の一般原則を反映したものであると考えられている。このため、欧州人権裁判所の判例法は、EU 法の法規範上の欠落を埋めるために用いられるほか、EU 法の解釈の補助にも用いられる(113)。この点、パオルッチ氏は、EU 条約第 2 条等を媒介して欧州人権裁判所の判例が EU 法の解釈の指針となり得ることを確認した上で、本判決を AI 規則の基本権本位の（rights-oriented）アプローチを補完する重要な手段として位置付けている(114)。

また、本判決が、警察による顔認識技術の利用が「差し迫った社会的必要」を満たすものであるか否かを比例原則に基づき判断した点について、AI 規則のリアルタイム遠隔生体識別の例外的利用の可否を判断する指針として参照する見解もある。フランチェスカ・パルミオット（Francesca Palmiotto）氏（ヘルティ・スクール）とナタリア・メネンデス・ゴンザレス（Natalia Menéndez González）氏（欧州大学院大学）は、AI 規則における顔認識技術の例外的利用の可否も本判決と同様に、「顔認識技術が差し迫った社会的必要を満たす上で唯一の解決策であるのか、そして伝統的かつより侵襲的でない法執行の技法で足りるか」について、比例原則の観点から検討すべきであると指摘している(115)。

おわりに

本稿では、欧州における法執行分野の顔認識技術の規制について、EU の立法動向及び欧州人権裁判所の判例を概説してきた。EU の AI 規則におけるリアルタイム遠隔生体識別に対する規制の背景には、私生活の尊重を受ける権利や個人データ保護権を中心としつつ、人間の尊厳、思想、良心及び宗教の自由、表現及び情報の自由、集会及び結社の自由を始めとする様々な基本権の侵害の懸念があった。また、欧州人権裁判所の 2023 年の判決は、私生活及び家族生活の尊重を受ける権利の違反を認定する上で、表現の自由、集会及び結社の自由も考慮していた。

ただし、欧州委員会は、2025 年 11 月 19 日に、GDPR や AI 規則等のデジタル関連法を包括的に見直し、簡素化を目指す法案である「デジタル・オムニバス」（Digital Omnibus）を公表した(116)。現段階では、本稿で注目したリアルタイム遠隔生体識別に対する規制を含む AI 規則

(112) Federica Paolucci, "Enhancing Oversight and Addressing Gaps: Assessing the Impact of the AI Act on Biometric Identification Systems," Natalia Menéndez González and Giuseppe Mobillio, eds., *Next Democratic Frontiers for Facial Recognition Technology*, Cham: Springer, 2025, p.85.

(113) 庄司　前掲注(45), pp.199-203.

(114) Paolucci, *op.cit.*(112), p.85.

(115) Palmiotto and González, *op.cit.*(111), p.105860.

(116) European Commission, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations*

の「禁止されるAI実務」（第Ⅱ章）は見直しの対象となっていないが、「高リスクAIシステム」（第Ⅲ章）の事後的遠隔生体識別システムに該当する顔認識技術については、AI規則の適用開始が延期される可能性がある。また、欧州人権裁判所の判例法は「生ける文書」（living document）として位置付けられているため、今後も発展的な解釈が行われる可能性が残されている。そのため、本稿で紹介したEUの立法動向や欧州人権裁判所の判例について、今後の動向を注視する必要があると思われる。

（かどたに　はるき）

（本稿は、筆者が憲法課在職中に執筆したものである。）

(EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), COM(2025) 837 final, 2025.11.19. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0837>