

欧州主要国における顔識別機能付カメラの利用
に関する法制度に関する調査

2022年3月31日

渥美坂井法律事務所・外国法共同事業

目次

第1 本調査について.....	1
1 調査事項.....	1
2 調査体制.....	1
第2 EU法.....	2
1 個人情報保護の観点からの規律.....	2
(1) 一次法.....	2
(2) 二次法（GDPR、LED）.....	2
(3) 欧州評議会ガイドライン.....	4
2 近時の動向.....	5
(1) AI規制提案.....	5
(2) 欧州データ保護委員会・欧州データ保護監察機関共同意見.....	6
(3) 欧州議会決議.....	6
第3 フランス.....	7
1 犯罪予防や安全確保のための顔識別又は顔認識機能付きカメラの利用に関する法令.....	7
(1) 個人情報保護の観点からの規律.....	7
(2) 個人情報保護以外の観点からの規律.....	12
2 その他参考情報.....	12
(1) 顔認識技術の利用主体.....	12
(2) 顔認識機能付きカメラの導入に対する姿勢・政策.....	12
第4 ドイツ.....	14
1 犯罪予防や安全確保のための顔識別又は顔認識機能付きカメラの利用に関する法令.....	14
(1) 個人情報保護の観点からの規律.....	14
(2) 個人情報保護以外の観点からの規律.....	16
2 その他参考情報.....	17
(1) ドイツ連立政権による公共の場での生体認識を用いた監視を禁止する公約.....	17
(2) ドイツ国内の警察・地方自治体による顔認識技術の試験的導入.....	17
(3) その他生体情報利用に対する姿勢・政策.....	18
第5 英国.....	20
1 犯罪予防や安全確保のための顔識別又は顔認識機能付きカメラの利用に関する法令.....	20
(1) 個人情報保護の観点からの規律.....	20
(2) 個人情報保護以外の観点からの規律.....	22
2 その他参考情報.....	24
(1) 顔認識技術の利用状況.....	24
(2) 顔認識技術にかかる政策・動向.....	24

第1 本調査について

1 調査事項

令和4年3月「欧州主要国における顔識別機能付カメラの利用に関する法制度に関する調査調達仕様書」記載のとおり。

2 調査体制

次の各弁護士・外国弁護士により調査を実施した。

【渥美坂井法律事務所・外国法共同事業 所属】

- 落合孝文（パートナー弁護士）
- 松下外（パートナー弁護士）
- 岸田梨江（パートナー弁護士）
- 湊健太郎（パートナー弁護士）

【Atsumi & Sakai New York LLP 所属】

- 勝見将也（アソシエイト）

※米国イリノイ州弁護士（日本における外国法事務弁護士登録はない。）

また、調査の過程において、次の各弁護士・外国弁護士の協力を得た。

【渥美坂井法律事務所・外国法共同事業 所属】

- 金久直樹（パートナー弁護士）

※Atsumi & Sakai Europe Limited（ロンドンオフィス）代表

【Atsumi & Sakai Europa Rechtsanwalts- und Steuerberatungsgesellschaft mbH 所属】

- フランク・ベッカー（代表パートナー）

※ドイツ連邦共和国弁護士（日本における外国法事務弁護士登録はない。）

第2 EU 法¹

1 個人情報保護の観点からの規律

(1) 一次法²

顔識別機能付きカメラによる監視の態様として、①ターゲットを特定しない人口の全体又は重要部分を見張る大衆監視 (mass surveillance) と②ターゲットを定めた監視 (targeted surveillance) がある。②ターゲットを定めた監視は、犯罪活動に関与しているとの事前の嫌疑に基づいて特定の個人又は集団に対して実施される点において、大衆監視とは概念上区別される。

EU 法の一次法には、これら監視を直接規律する規範は存在しない。もっとも、これまでの欧州人権裁判所 (ECHR)³及び欧州司法裁判所 (EUCJ)⁴の諸判決に照らせば、①大衆監視 (mass surveillance) は、個人の基本権に深刻な影響をもたらすことから禁止されるとの解釈が示されている⁵。他方、EU 法の下でも、②ターゲットを定めた監視 (targeted surveillance) は、EU 基本権憲章第 52 条第 1 項で正当化される限り、適法に実施可能であるものの⁶、いかなる場合にいかなる限度で許容されるかは一次法からは明らかではない。

(2) 二次法 (GDPR、LED)

データ保護に関する二次法が、犯罪予防や安全確保のための顔識別機能付きカメラの利用に関して実践的なガイダンスを提供している⁷。

¹ EU 域内における顔識別付きカメラによる監視に関する現状を整理した文献として、Greens/EFA, *Biometric and Behavioural Mass Surveillance in EU Member States: Report for the Greens/EFA in the European Parliament* (Oct. 2021), <http://extranet.greens-efa-service.eu/public/media/file/1/7297>

² EU における法源には、一次法 (primary legislation) と二次法 (secondary legislation)、判例 (case-law) の3つがある。一次法はEUの基本条約を指し、二次法は一次法である基本条約を根拠に制定される法令を意味する。概要は、国立国会図書館ウェブサイト (<https://rnavi.ndl.go.jp/politics/entry/eu-law.php>) 参照。

³ 欧州人権裁判所 (ECHR: European Court of Human Rights) は、2008年12月4日、*S and Marper v UK* において、犯罪の検知及び予防目的での指紋及びDNA情報を一般的かつ無差別に取得することは個人の私生活の尊重の権利を均衡を失って比例的 (disproportionately) に侵害するものであることから、欧州人権条約第8条に違反すると判示した (*S and Marper v UK* [2008] ECHR 1581, <http://www.bailii.org/eu/cases/ECHR/2008/1581.html>)

⁴ 欧州司法裁判所 (EUCJ: Court of Justice of the European Union) は、2014年4月8日、Digital Rights 事件判決において、知らされることなく個人データが取得され利用される場合には、当該データ主体の心の中に自らの私生活に常に監視にさらされているとの感情を生じさせるとした (*Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* Joined cases Case C-293/12 and C-594/12, <https://curia.europa.eu/juris/liste.jsf?num=C-293/12>)。

⁵ Greens/EFA, 前掲注1・48-49頁

⁶ Greens/EFA, 前掲注1・49頁

⁷ EPRS, *Regulating facial recognition in the EU* (Sept. 2021), [https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA\(2021\)698021_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf)

ア 民間機関による利用に関する規制

EUにおける個人データ（「個人データ (personal data)」保護の中心的枠組である EU 一般データ保護規則 (GDPR: General Data Protection Regulation, REGULATION (EU) 2016/679) では「生体データ (biometric data)」⁸が特別なカテゴリーの個人データ (special categories of personal data) に位置づけられており、その処理が原則として禁止されている (GDPR 第 9 条第 1 項)。

ただし、「求められる目的と比例的であり、データ保護の権利の本質的部分を尊重し、また、データ主体の基本的な権利及び利益の安全性を確保するための適切かつ個別の措置を定める EU 法又は加盟国の国内法に基づき、重要な公共の利益を理由とする処理が必要となる場合」(GDPR 第 9 条第 2 項 (e) には例外的に処理が可能な場合があるが、この場合にも、GDPR 第 6 条所定の各処理原則を充足する必要がある⁹。

なお、EU の個人データ保護の諮問委員会である EDPB (欧州データ保護会議) は 2020 年 1 月 29 日に、「ビデオ機器を通じた個人データ処理に関するガイドライン」¹⁰を策定、公表している。同ガイドラインは、GDPR (一般データ保護規則) におけるカメラ画像や顔識別技術等の取扱いに関する指針であり、執行を行う際の根拠となるものでもある。

イ 公的機関による利用に関する規制

GDPR は、「個人データ (personal data)」の「処理 (processing)」が「公共安全への脅威からの保護及びその脅威の防止を含め、所轄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」には適用されない (GDPR 第 2 条第 2 項(d))。一方で、法執行指令 (LED: Law Enforcement Directive, DIRECTIVE (EU) 2016/680) ¹¹においては、所轄官庁により犯罪行為の防止、捜査、検知、訴追又

⁸ 「生体データ」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処理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」とされている (GDPR 第 4 条第 14 項)。後述する LED も同様の定義を採用している (LED 第 3 条第 13 項)。

⁹ 調査の範囲では、民間機関に適用される LED 類似の規制は見当たらなかった。なお、European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (2020), https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf 6 頁も参照されたい。

¹⁰ European Data Protection Board, *Guidelines 3/2019 on processing of personal data through video devices Version 2.0* (29 Jan. 2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

¹¹ Law Enforcement Directive, DIRECTIVE (EU) 2016/680, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN>. LED は EU 加盟国の所轄官庁による法執行目的での国内又は越境での個人データ処理に対して適用される (LED 第 1 条第 1 項及び第 2 条第 1 項)。LED を受けて各加盟国は、LED の内容に沿った国内立法を行っている。また、シェンゲン協定加盟国であるアイスランド、リヒテンシュタイン、ノルウェー及びスイスについては、LED は直接適用されないものの、LED の内容に沿った国内立法を行っている。

は刑罰の執行のために個人データが処理される場合の規則が定められている（LED 前文第 11 条及び第 12 条並びに本文第 1 条）。

具体的には、LED では「生体データ (biometric data)」¹²が特別なカテゴリーの個人データに位置づけられているところ、顔識別機能付きカメラによって撮影された顔の写真又は動画が個人の特定識別のために処理される場合には当該写真や動画は「生体データ」に該当する¹³。そして、LED においては、生体データについて、所轄官庁による個人の特定識別のための処理を原則として禁止しつつも、①厳に必要であり（データ処理と目的との間の厳格な衡量が要求される。）、②データ主体の権利自由のための適切な保護措置に従う場合であって、かつ、③以下のいずれかの目的が認められる例外的な場合には、これを許している（LED 第 10 条）。

- EU 又は加盟国の国内法による承認がある場合¹⁴
- データ主体又は他の自然人の重要な利益を保護する目的の場合（例えば、物理的若しくは法的に同意を与えることが不可能であり又は人道的緊急性がある場合）
- 処理がデータ主体によって明白に公開されたデータに関する場合

(3) 欧州評議会ガイドライン

また、EU そのものではないものの、2021 年 2 月、欧州評議会（CoE: Council of Europe¹⁵）は、顔認識技術（facial recognition technology。リアルタイム顔認識技術を含む。）の開発・利用に関するガイドライン¹⁶を発表した。同ガイドラインでは、顔認識

¹² 「生体データ」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処理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」とされている（GDPR 第 4 条第 14 項）。LED も同様の定義を採用している（LED 第 3 条第 13 項）。

¹³ European Data Protection Board, 前掲注 10, 段落 74 「GDPR に定義された生体データとして認められるためには、自然人の身体的、生理的または行動的特徴等の生データの処理が、この特徴の測定を意味するものでなければならない。生体データはこのような測定の結果であるため、GDPR はその第 4 条 14 項で、『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処理から得られる個人データであって、当該自然人を一意に識別できるようにするもの…』と述べている。しかし、個人のビデオ映像は、個人の識別に寄与するために特別に技術的に処理されていない場合、それ自体では第 9 条に基づく生体データとみなすことはできない。」

¹⁴ なお、GDPR 第 9 条第 4 項は生体データの処理について、制限を含む付加的な条件の導入をする権限を加盟国に付与している。

¹⁵ 欧州評議会（CoE）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た団体である。外務省ウェブサイト

（<https://www.mofa.go.jp/mofaj/area/ce/index.html>）参照。

¹⁶ Council of Europe, Guideline on Facial Recognition (28 Feb. 2021), <https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html>

技術の利用に際しては、人間としての尊厳、人権、基本的人権及び自由（個人情報保護に関する権利）に悪影響を及ぼさないために、次の各関係者は、次の各事項を検討すべきであるとしている。

- 立法者・政策決定者： 合法性、監督当局の関与、認証、データ主体への注意喚起
- 開発者・製造業者・サービス提供者： データ及びアルゴリズムの品質、利用するツールの信頼性、注意喚起、アカウントビリティ
- 顔認識技術の利用者： データ処理の正当性及びデータ品質、データ・セキュリティ、アカウントビリティ、倫理

2 近時の動向

(1) AI 規制提案

2021年4月21日、欧州委員会（EC: European Commission）は、顔認識（facial recognition）技術を含むAI技術の利用に関する規制の立法提案（以下「AI規制提案」という。）を行った¹⁷。そこでは、顔認識技術を含むAI技術によってもたらされるリスクを、①受諾不可、②高リスク（high-risk）、③低リスク（low-risk）の3種類に区分した上で、それぞれのリスク程度に応じた措置を要請するというアプローチが提唱されている。

AI規制提案では、多くの顔認識技術は、受諾不可又は厳格な要件（リスク管理システムの構築、アルゴリズムの教育に用いるデータの質の最低レベルの設定、ユーザーに対する透明性と情報提供の義務、人間による監督等）による規制を受ける高リスクの技術に分類される。そして、法執行の目的については、加盟国が重要な公安上の理由¹⁸でそれらを許可することを選択しない限り、公的にアクセス可能な空間において、リアルタイム顔認識技術を使用することは禁止される。他方、法執行以外の目的（国境管理、市場、公共交通機関、学校等）で使用されるリアルタイム顔認識技術は、EU市場に参入する前に、適合性評価といくつかの安全要件への準拠を条件として許可される可能性があると考えられている。

また、性別、年齢、髪の色、目の色、タトゥーの有無、民族的出身、性的・政治的指

¹⁷ 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 Act, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>

¹⁸ たとえば、第5条1(d)では、次の各場合が挙げられている。

- ① 行方不明の子供を含む、特定の潜在的な犯罪被害者の的を絞った捜索
- ② 自然人の生命又は身体の安全に対する具体的、実質的かつ差し迫った脅威又はテロ攻撃の防止
- ③ 理事会枠組み決定2002/584/JHA62の第2条(2)に言及され、当該加盟国において少なくとも3年の最長期間の拘禁刑または拘留命令により処罰される犯罪の犯人または容疑者の発見、位置確認、特定または訴追

向等への分類を行う目的で使用される顔認識技術は低リスクとみなされ、限定的な透明性と（対象者への）情報開示要件が適用される。ただし、リアルタイム顔認識と分類目的利用の区分自体が適切であるか議論がある状況とのことである¹⁹。

(2) 欧州データ保護委員会・欧州データ保護監察機関共同意見

欧州データ保護委員会（EDPB: European Data Protection Board）及び EDPS（欧州データ保護監察機関（EDPS: European Data Protection Supervisor）は、2021年6月、前記 AI 規制提案に関連して、公的にアクセス可能な場所での人間の特徴を自動認識（automated recognition）するための AI の使用、及び不当な差別につながる可能性のある AI のその他の使用の禁止を求めることを含む共同意見を公表している²⁰。

(3) 欧州議会決議

欧州議会（EP: European Parliament）も、2021年10月、犯罪被害者の識別（identification）の目的で厳密に使用されない限り、識別機能を有する法執行目的の顔認識システムの開発は、①技術的基準が完全に基本的権利に適合していると考えられ、②導き出された結果が非偏向かつ非差別的であり、③法的枠組みが誤用に対する厳格な保護措置と厳格な民主的統制・監視を提供し、④当該技術の必要性と比例性について経験則上の証拠が存在するまで、一時中止する旨の決議をしている²¹。

その際、欧州議会は、EU 市民を含む SNS やインターネットの他の部分から違法収集された 30 億枚以上（当時）の顔画像データのデータベースを用いた Clearview AI²²のような民間の顔認識（facial recognition）データベースを、法執行機関や諜報部門が使用することについて、大きな懸念を表明し、加盟国に対し、法執行機関が Clearview AI の技術や他のプロバイダーの同等の技術を使用しているか否かの開示を義務付けるよう要請すると共に、欧州データ保護委員会による、EU の法執行機関による Clearview AI のようなサービスの利用は「EU におけるデータ保護の仕組みと整合しない可能性が高い²³」との見解を踏まえて、法執行の際、民間顔認識データベースを使用することの禁

¹⁹ EPRS, 前掲注 7 24-31 頁

²⁰ European Data Protection Board, European Data Protection Supervisor, *EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)* (18 June 2021), https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf 段落 32

²¹ MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION, on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)) https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.html 段落 27

²² Clearview AI, <https://www.clearview.ai/>。同ウェブサイトでは、同社の活動内容として、犯罪捜査や公共安全の促進のための法執行に利用される最先端技術を提供することが紹介されている。最新版の Clearview AI 2.0 では、2022年3月28日現在、200億枚以上の顔画像データが用いられているとのことである。

²³ European Data Protection Board, *Thirty-first Plenary session: Establishment of a taskforce on TikTok, Response to MEPs on use of Clearview AI by law enforcement authorities, Response to ENISA Advisory Group, Response to Open*

止を求めている²⁴。

また、欧州議会は、欧州委員会に対し、法執行のために、公共空間における大衆監視につながる顔画像を含む生体情報の処理を、立法的及び非法律的手段により、また必要ならば侵害訴訟を通じて、禁止するべく要請する決議をしている²⁵。

第3 フランス

1 犯罪予防や安全確保のための顔識別又は顔認識機能付きカメラの利用に関する法令

(1) 個人情報保護の観点からの規律

ア 改正 1978 年法（加盟国法）

フランスは、1978 年に同国における個人情報保護に関する基本法である「情報処理、情報ファイル及び自由に関する 1978 年 1 月 6 日法律第 78-17 号²⁶」を制定していたところ、GDPR の前身である EU データ保護指令 (Data Protection Directive 95) 等の EU 指令の国内法化を図るため、2004 年に改正がなされ（「個人情報のデータ処理に関する個人保護について 1978 年法を改正する 2004 年 8 月 6 日法律第 2004-801 号²⁷」）、更に GDPR の制定を受けて、2018 年に再改正がなされた（以下、2018 年改正後の同法²⁸を「改正 1978 年法」という。）。

改正 1978 年法では、GDPR 及び LED と同様に、生体データの処理は原則として禁止され（改正 1978 年法第 6 条第 1 項）、GDPR 第 9 条第 2 項に規定された場合のみ許容される（改正 1978 年法第 6 条第 2 項）。

また、改正 1978 年法第 III 部では、犯罪活動の防止、捜査、発見若しくは訴追又は刑事罰の執行のための権限ある当局による個人データの処理に関して特別の規定が設けられている。ここでは、「生体データ」（改正 1978 年法第 6 条第 1 項）は、原則としてその処理が禁止され、例外的に、①絶対的な必要性があり、かつ、②立法上又は規制上の規定により定められたデータ主体の権利自由のための適切な保護措置に従うことを条件として、③以下のいずれかが認められる場合に限って、処理が許容されている（改正 1978 年法第 88 条）。

Letter NYOB (10 June 2020), https://edpb.europa.eu/news/news/2020/thirty-first-plenary-session-establishment-taskforce-tiktok-response-meps-use_en

²⁴ European Data Protection Board, 前掲注 21・段落 28

²⁵ European Data Protection Board, 前掲注 21・段落 31

²⁶ Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/>

²⁷ Loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000441676/>

²⁸ Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles (1), <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037085952>

- 自然人の重要な利益を保護するために必要である場合
- その処理がデータ主体により明白に公表されたデータに関連する場合

生体データが含まれることによって個人データの処理を運用することが自然人の権利自由に高いリスクをもたらす可能性が高い場合には、当該個人データの管理者²⁹はデータ保護影響評価を実施する必要がある（改正 1978 年法第 90 条）。また、管理者が国家に代わってこれらのデータの取り扱いを行う場合は、データ保護影響評価をフランスのデータ保護機関であるフランス共和国データ保護機関（CNIL: Commission Nationale de l'Informatique et des Libertés）に送付することとされており（同条）、その他の場合には、個人データの取扱いの実施に先立ち、管理者は CNIL と協議することとされている（同条）。

加えて、前記各目的のために権限のある当局によって収集された個人データは、立法上若しくは規制上の規定又は EU 法によって認められていない限り、他の目的のために処理してはならないことも規定されている（改正 1978 年法第 91 条）。

イ CNIL 報告書「Reconnaissance faciale : pour un débat à la hauteur des enjeux」

フランスのデータ保護機関である CNIL は、2019 年 11 月 15 日、報告書「Reconnaissance faciale : pour un débat à la hauteur des enjeux」（以下「CNIL 報告書」という。）を公表した³⁰。同報告書は 4 部構成であり、その概要は以下のとおりである。

第 I 部では、顔認識 (la reconnaissance faciale) を「顔に基づいて人物を自動的に認識し、本人であることの認証又は本人の識別を行うコンピュータ・ベースの確率的手法」とした上で、以下の 2 つの異なる機能を有すると整理されている。

- 人物の認証 (authentication) (ある人物が本人であると主張している人物であることを確認することを目的とする。)
- 人物の識別 (identification) (場所、画像又はデータベースにおいて集団の中から個人を発見することを目的とする。)

その上で、監視ビデオカメラで撮影すること自体によって自動的に顔認識がなされるわけではないとの前提の確認の重要性が説かれ、また、顔認識技術には以下の特徴があると指摘されている。

- 顔認識は他の様々なデバイスと関連付けられることが可能であり、このよう

²⁹ 「管理者」とは、自然人又は法人、公的機関、部局又はその他の組織であって、単独で又は他の者と共同で、個人データの取扱いの目的及び方法を決定する者をいう（GDPR 第 4 条。改正 1978 年法第 2 条によって GDPR 第 4 条の定義が改正 1978 年法にも適用されることとされている。）したがって、「管理者」には、公的主体と民間主体の双方が含まれる。

³⁰ CNIL, *Reconnaissance faciale : pour un débat à la hauteur des enjeux* (15 Nov. 2019), https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf

な他のデバイスとの結びつきの可能性によって、人々に対して大きな影響をもたらす。

- 顔認識は、商用目的から公共の安全の目的までを含む幅広い目的を遂行するために利用することができること。あるものは既に日常化し、幅広く利用されており、他のあるものは未だ計画や予想の段階である³¹。
- 個人データに対するデータ主体による管理の程度、顔認識技術を利用する際のデータ主体のイニシアティブの程度、顔認識技術の利用により生じる結果、顔認識技術によって生じた個人データの取り扱いがなされる範囲等に応じて顔認識には幅広い潜在的な利用可能性があることに鑑みれば、個人の媒体に搭載される顔認識が、大衆の中の通行人を比較して特定の人物を認識する目的で用いられる顔認識と同一の問題を提起するとは考えられない。したがって、顔認識の利用についてはケースバイケースの検討が必要となる。
- 個人データの取り扱いが適法であるかどうかは、そのデータが関連性を有し、均衡がとれており、保管期間と安全性が適切であるか等についての評価を特定の目的に照らして行うことによってのみ行われ得る。正当で適法な顔認識の使用事例がひとつ存在したからといって、すべての顔認識が望ましくて許容されることになるわけではない。

第II部では、顔認識技術のリスクとして、①特別の保護を必要とする、特にセンシティブなデータであること、②非接触で、潜在的にユビキタスな技術であること、③潜在的に「見えない監視」であること及び④可謬性を有する高価な技術であること等が指摘されている。

第III部では、顔認識技術の導入指針として、政府当局による実験的なアプローチを通じて導入を進展させることが検討されている。この取組については、市民のプライバシーと個人データを保護する原則が尊重されること、及び顔認識技術に対する市民の信頼を確保するために、その実施において、次の3つが指針とされるべきであるとする。

- 「レッドライン」を引くこと：顔認識を実施するにあたっては、それを実験的に行うかどうかにかかわらず、EUの枠組み（GDPR及びLED等の諸指令）が遵守されなければならない。追求される目的の正当性と、実施することの厳格な必

³¹ 例えば、フランスのみならず、ヨーロッパにおいて使用されている例として、Facebookのようなソーシャルネットワークの画像上に映っている人物を自動認識すること、ATMの利用においてカメラに映っている顔と銀行等が保有している顧客の顔のデータベースとを照合して顧客の認証を実施すること、身元確認ができない人物（被害者、被疑者等）についてデータベースにより身分を探索すること（例えばフランスにおける犯歴記録ファイル（TAJ）など）、公共空間における人の異同のモニタリング、公道上の指名手配犯の識別などが挙げられている。

要件が必要であり、更に目的に照らして手段が比例していることも重要な要件である。

- プロセスの中心に人々（の権利）の尊重を据えること：データ保護とプライバシーの権利は基本的な権利である。したがって、顔認識技術を用いる各デバイスの利用においては同意が取得される必要がある。また、データのコントロール、透明性（明確で理解可能で容易にアクセス可能な情報の提供）、生体データのセキュリティといった要素はいずれもデータの処理において重要な条件とならなければならない。
- 真に実験的なアプローチを採用すること：顔認識がもたらす問題点に鑑みれば、初期のフレームワークの準備には実験的なアプローチ³²が望ましく、その結果が前もって予断されることがあってはならない。

最後に第IV部では、CNIL の果たすべき役割について、政治的な選択は政府や議会の責任において行われるものであるが、その中において CNIL は、①公的機関に助言を行うと共に②法令の遵守をモニタリングするという 2 つのミッションにおいて、「人々の自由、プライバシー、個人データを保護するという原則」の独立した保証人としての役割を果たす旨が宣明されている。

ウ スマートカメラに関する CNIL 勧告草案

CNIL は、2022 年 1 月 14 日、スマートカメラに関する勧告草案を公表した³³。同草案において、CNIL は、リアルタイムかつ継続的に撮影画像を分析することを可能とするというスマートカメラの特性に鑑み、スマートカメラを公共空間に配備することによってもたらされる、個人のプライバシーに対する多数のリスクを特定している。なお、

³² CNIL 報告書が「実験的なアプローチ」を提唱するに当たり、国務院が 2019 年 10 月 3 日に発表した、より一般的な法的枠組についての研究である「実験：公共政策の実施をいかに刷新するか？」(Conseil d'État, *Les expérimentations : comment innover dans la conduite des politiques publiques ?* (3 Oct. 2019), <https://www.vie-publique.fr/sites/default/files/rapport/pdf/194000762.pdf>) を参照している旨が言及されている。国務院の同研究によると、2003 年にフランスにおいて、限定された期間内に限って法令の適用を制限しつつ実験を実施することが可能とされた。これを受けて同年以降に実施された 269 の実験の評価を踏まえてまとめられたものが同研究であるとのことである。

³³ CNIL, *PROJECT DE POSITION: RELATIVE AUX CONDITIONS DE DÉPLOIEMENT DES CAMÉRAS DITES « INTELLIGENTES » OU « AUGMENTÉES » DANS LES ESPACES PUBLICS* (14 Jan. 2022), https://www.cnil.fr/sites/default/files/atoms/files/projet-position-cnil-relative-conditions-deploiement-des-cameras-dites-intelligentes-ou-augmentees-espaces-publics_consultation-publique.pdf。CNIL は、本文記載の勧告草案を自ら公表するとともに、ステークホルダーに対して 2022 年 3 月 11 日までに公的協議のための意見表明を行うことを求めている。その意見表明を受けた後、CNIL は、スマートカメラ及びその使用に対する GDPR 等の法令の適用に関する最終的な見解を公表することを予定しているとのことである (<https://www.cnil.fr/fr/cameras-dites-intelligentes-ou-augmentees-dans-les-espaces-publics-la-cnil-lance-une-consultation>)。

生体認証デバイス（特に上記イの CNIL 報告書の議論の対象となるもの）や一般的に公開されていない場所（オフィス、店舗、倉庫）における利用や厳密に私的な利用、学術研究目的での利用は対象外とされている。

CNIL は、データ処理の目的の決定、必要性、比例性の確保、法的根拠の決定、データ主体のデータに対する権利の尊重などが重要な原則であることを改めて指摘している。そして、年齢、性別、ジェスチャーや表現から感知された感情、センシティブ・データ等に基づいてターゲット広告を表示又は送信するために人々を分析して区分する目的でスマートカメラを使用することは、正当な利益及び適法性を欠き、基本的には GDPR に違反することになるのではないかという見解を整理している。

このように、スマートカメラを使用する場合に GDPR を遵守することは容易ではないことにも照らし、CNIL 草案では、特に公的機関に対し、「技術的に可能であること」と「法的・社会的・倫理的に受容可能であること」の線引きを行うことが提唱されている。

エ 自治体の取り組みに関する法的紛争

ニース市は、2018 年 6 月に民間事業者との間でパートナーシップを締結し、公道上や公共交通機関に顔認識機能付きカメラを設置した（「Safe City」プロジェクト）。そして、2019 年 2 月から同年 3 月にかけて、ニースで開催されるカーニバルの期間中、カーニバルに参加した群衆（およそ 1000 人）をその顔認識機能付きカメラで撮影した上で、虚構のデータベースとの間でマッチングを試みるというシミュレーション実験を実施した。この実験を行うにあたっては、参加者に対して撮影を行う旨が事前に告知され、参加者は撮影されることに同意する場合にはブレスレットを着用するよう要請がなされた。

ニース市は、2019 年に新たなプロジェクトとしてニース及びマルセイユの高校において建物敷地に入出入りするための門に顔認識機能付きカメラを設置したところ、2020 年、マルセイユの行政裁判所はこの措置を違法と判断した。その判決では、高校の敷地への出入りをコントロールするために顔認識システムを配備することの法的基礎はデータ主体の明示的な同意に求められるとされた上で、本件においては生徒又は保護者から必要な同意が取得できていなかったとされた。また、この判決では、実質的な公的利益に基づいて生体データの取り扱いが正当化されるものではないとも判示された³⁴。

ニース市以外の事例としては、パリ市の事例がある。国務院（Conseil d'État）は、2020 年 12 月 22 日、パリ市警察が COVID-19 対策としてのソーシャルディスタンスを遵守させるための監視のために顔認識装置を搭載したドローンを利用することを禁

³⁴ Greens/EFA, 前掲注 1・84 頁以下

止する決定を下した³⁵。

(2) 個人情報保護以外の観点からの規律

刑事手続規則 (Code de procédure pénale) R40-26 では、警察が犯罪歴データベースを保持し、犯罪活動に参加していた被疑者や被害者、捜査対象者の写真を取得することができ、顔識別画像を利用することができる³⁶とされている。

2 その他参考情報

(1) 顔認識技術の利用主体

フランスにおいて、顔認識技術は政府機関及び民間事業者によって様々な形で利用されているが、犯罪予防や安全確保の目的という観点からは主に政府機関によって顔認識機能付きカメラの導入が進められているというのが現状である。これについては、フランスがラグビー・ワールドカップ (2023 年) やオリンピック (2024 年) といった世界的スポーツイベントの開催を控えているため、そのためにこれまで以上に顔認識機能付きカメラの導入を進めているという社会的背景が指摘されている³⁷。

(2) 顔認識機能付きカメラの導入に対する姿勢・政策

フランスにおいて政府機関によって顔認識機能付きカメラの導入が進んでいるとしても、現段階においては、地理的かつ時間的な制限が付された試験運用にとどまっております、本格的な展開には至っていない³⁸。その意味で、フランスは犯罪予防や安全確保の目的での顔認識技術の利用に対しては未だ慎重な姿勢に留まっていると言える。その理由としては、一つには、個人情報やプライバシーの権利が侵害されることへの警戒感から市民団体を中心に根強い批判があることが挙げられる。また、CNIL が独立の監督者・保護者として顔認識技術の利用に対して慎重な姿勢を示していることもその理由であると考えられる。

なお、CNIL は、2021 年 12 月、第 2・2・(3) で前述した Clearview AI が適切な同意を得ることなく人々の顔画像データを収集・利用していたとして GDPR 違反を認定し、同社のデータベースに保管されているフランス市民の個人情報を削除するよう命じた³⁹。

³⁵ Conseil d'Etat. ECLI:FR:CECHR:2020:446155.20201222, <https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2020-12-22/446155>

³⁶ 2018 年の議会の報告書によると、犯歴記録データベース (TAJ) には 700 万～800 万の顔写真が保管されているとのことである。Greens/EFA, 前掲注 1・86 頁。

³⁷ Renaissance numerique, *Regulation of facial recognition technologies: A Comparative Analysis of France and the United Kingdom* (June 2021), https://www.renaissancenumerique.org/ckeditor_assets/attachments/626/renaisancenumerique_eventssummary_facial_recognitionukfr.pdf 4 頁。

³⁸ European Data Protection Board, 前掲注 21・5 頁以下

³⁹ CNIL, *Facial recognition: the CNIL orders CLEARVIEW AI to stop reusing photographs available on the Internet* (16 Dec. 2021), <https://www.cnil.fr/en/facial-recognition-cnil-orders-clearview-ai-stop-reusing-photographs-available-internet>

具体的には、同事案では、Clearview AI は、インターネット上のウェブサイトで閲覧可能となっている写真や動画から個人の画像を抽出し、全世界中から 100 億以上（当時）の画像をデータベース化した上で顔認識を用いた検索エンジンを用いて検索できるようにしていた。これに対して CNIL は、Clearview AI が、①法的根拠なく生体データを収集・使用していること（GDPR 第 6 条違反）、②個人の権利（特にデータ主体による自らの個人データへアクセスする要求）に対して効果的かつ満足な形で考慮を払っていないこと（GDPR 第 12 条、第 15 条、第 17 条の違反）の二点において GDPR に違反している旨を認定した⁴⁰。

他方、一般のフランス国民が顔認識技術に対してどのように感じているかについて正確に把握することは困難であるが、ある調査⁴¹によると、全体的に顔認識技術の利用に賛成する傾向が見てとれるとのことである。この点に関して、2021 年 5 月、フランス議会の議員である Didier Baichère が議会に対して「人工知能に基づく顔認識技術に関する実験と協議」を導入する法案を提出した。この法案では、「透明で倫理的な」実験のためのフレームワークを構築すると共に、「市民的及び教育的議論を促進し、フランス国民がこの問題をどのように認識しているか、そしてどこがレッドラインになるのかを評価する」ための公的協議の開始が意図されている⁴²。このようにフランスにおいては、国家的な取り組みとして、国民的議論によって顔認識技術の使用に関するレッドラインを決定していこうとする取組が進展している。

2015 年のパリ同時多発テロ事件や 2018 年の黄色ベスト運動の記憶が新しいフランスにおいて犯罪の予防や社会の安全に対するニーズは高まっている。他方で、個人データ保護のための独立した監督者である CNIL による慎重な姿勢、更には個人データ保護を強める EU の方針との整合的な規律を策定する必要性があり、これらの（場合によっては相反する）要請の中でどこに「レッドライン」が引かれるのかについてはこれからの議論を注視する必要がある。

⁴⁰ なお、2022 年 3 月 10 日、イタリアの個人データ保護機関は Clearview AI に対して同様の GDPR 違反を理由として 2000 万ユーロの罰金の支払いを命じる決定を下している。European Data Protection Board, *Facial recognition: Italian SA fines Clearview AI EUR 20 million* (10 March 2022), https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en

⁴¹ Renaissance numérique, *Reconnaissance faciale: quell regard des Français?* (Dec. 2019), https://www.renaissancenumerique.org/ckeditor_assets/attachments/449/rn-sondage_reconnaissancefaciale.pdf

⁴² PROPOSITION DE LOI d'expérimentation créant un cadre d'analyse scientifique et une consultation citoyenne sur les dispositifs de reconnaissance faciale par l'intelligence artificielle, https://www.assemblee-nationale.fr/dyn/15/textes/115b4127_proposition-loi

第4 ドイツ

1 犯罪予防や安全確保のための顔識別又は顔認識機能付きカメラの利用に関する法令

(1) 個人情報保護の観点からの規律

ドイツは、EU 加盟国であるため、GDPR の適用を受ける。また、加盟国法としては、2018 年 5 月の GDPR の発効にあわせて 2018 年に改正されたドイツ連邦データ保護法 (BDSG: Bundesdatenschutzgesetz⁴³) が存在する。同法は、①公的機関が業務執行をする際、②立ち入り拒否を判断する権利を行使する際又は③具体的に設定された目的のために、正当な利益を保護する際のいずれかに該当し、かつ、これらを覆すデータ主体の正当な利益 (legitimate overriding interest of data subject) がない場合に、管理者による、公共の場におけるビデオ監視が実施できることを明示している (BDSG 第 4 条第 1 項⁴⁴)。

また、スポーツ施設・歓楽街、ショッピングセンター・駐車場などの大型公開施設又は、公共鉄道・船・バスなどの車内若しくは大型公開施設では、その場の個人の人命、健康及び自由の確保が、非常に重要な利益 (very important interest) とみなされる (同項)。

加えて、BDSG では、GDPR 第 9 条(1)の権限委任に基づき、次のいずれかに該当し、かつ、管理者の利益がデータ主体の利益を上回る場合に、特別なカテゴリーのデータの処理が認められている (BDSG 第 22 条)。

【公的機関及び民間機関によるデータ処理が認められる場合】

- データ処理が、社会保障及び社会保護の権利から派生する権利の行使、またそれに関連する義務の履行に必要な際 (BDSG 第 22 条(1)1.(a))
- データ処理が、予防医学、従業員の労力容量の判断、医療診断、医療・公的介護・治療もしくは医療・公的介護システムと業務の管理に必要である際、又はデータ処理がデータ主体の医療関係者との接触に基づく場合、並びに当該データが医療関係やその他職業上の守秘義務もしくは医療関係者の監督下に置かれる者によって処理される際 (BDSG 第 22 条(1)1.(b))
- データ処理が、国際的に深刻な健康への脅威からの市民の保護や、医療、医療製品及び医療機器の高い品質安全を確保するためなど、公衆衛生分野にお

⁴³ Bundesdatenschutzgesetz https://www.gesetze-im-internet.de/englisch_bdsdg/

⁴⁴ ②と③の場合は、BDSG 第 4 条第 1 項の原文の表記を踏まえると、公的部門のみならず民間部門の管理者が対象になると考えられる。

ける公共の利益のために必要である際（BDSG 第 22 条(1)1.(c)）

- データ処理が、重大な公共の利益のために急遽必要な際（BDSG 第 22 条(1)1.(d)）

【公的機関によるデータ処理のみが認められる場合】

- データ処理が、治安に対する深刻な脅威を防ぐために必要な際（BDSG 第 22 条(1)2.(a)）
- データ処理が、公益への深刻な被害を防ぐ、もしくは公益における重大な関心事項の保護のため急遽必要である際（BDSG 第 22 条(1)2.(b)）
- データ処理が、国防のために急遽必要である際や、危機管理や紛争防止、人道的支援の分野における連邦政府の超国家的もしくは政府間の義務履行のために必要である際（BDSG 第 22 条(1)2.(c)）

ここで、BDSG における特別なカテゴリーのデータは、特定の自然人を識別する目的で利用する場合には生体データ（BDSG 第 46 条第 13 項）を含むとされている（BDSG 第 46 条第 14 項 c）。

また、BDSG 第 22 条第 1 項に基づくデータ処理の際には、データ主体の利益を保護するために適切かつ具体的な措置を取る必要がある（BDSG 第 22 条第 2 項）。

ア 地方自治体の規定⁴⁵

連邦レベルの法律（BDSG）の他に、地方自治体によっては独自の規律を設けている州も存在する。

例えば、バイエルン州警察義務法（PAG: Gesetz über die Aufgaben und Befugnisse der Bayerischen Polizei⁴⁶）では、ある程度の重要性行政犯罪又は刑事犯罪が行われている兆候が見受けられる場合等、一定の要件を充足するときには、公共の場でのビデオ監視が認められている（PAG 第 33 条）。

また、ノルトライン＝ヴェストファーレン州警察法（PoIG NRW: Polizeigesetz des Landes Nordrhein-Westfalen）⁴⁷においても、危険回避のための措置や刑事・行政犯罪の訴追を行う場合であって、個人の人命や身体の保護に必要な場合には、ビデオ撮影が可能とされている（PoIG NRW 第 15c 条）

⁴⁵ これら規定の英訳は存在しないためその存在及び概要を指摘するにとどめる。なお、ドイツ、オランダ及びポーランドに関する現状をまとめた資料として、EDRI, *The Rise and Rise of Biometric Mass Surveillance in the EU* (Nov. 2021), https://edri.org/wp-content/uploads/2021/11/EDRI_RISE_REPORT.pdf がある。

⁴⁶ Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei (Polizeiaufgabengesetz – PAG) <https://www.gesetze-bayern.de/Content/Document/BayPAG>

⁴⁷ Polizeigesetz des Landes Nordrhein-Westfalen (PoIG NRW) https://recht.nrw.de/lmi/owa/br_text_anzeigen?v_id=3120071121100036031

(2) 個人情報保護以外の観点からの規律⁴⁸

ア 連邦警察庁法 (BKAG) ⁴⁹

連邦警察庁法 (BKAG: Bundeskriminalamtgesetz) では、ドイツ連邦警察庁 (BKA: Bundeskriminalamt) による情報の収集や処理が規律されている。たとえば、個人データが収集された当初の目的の他にも、当該目的と同等の利益を保護する場合や同等の犯罪を防止する目的のためであれば、当局が個人データを処理することを許可する旨明示されている (BKAG 第 12 条)。

イ 連邦警察法 (BPoIG) ⁵⁰

連邦警察法 (BPoIG: Gesetz über die Bundespolizei) は、ドイツ連邦警察 (BPOL: Bundespolizei) に対し、次のいずれかに該当する場合に、被疑者・対象者の画像を処理する一定の権限を付与している。ただし、いずれの場合においても、記録したデータは一定期間を経た後に削除されなければならないとされている。

- 被疑者による犯行を防ぐなどの目的を含む一定の条件下において、当該被疑者の画像 (録画・写真など) を記録し保存する権限 (BPoIG 第 24 条)。
- 国境の安全やその他対象者 (物) に重大なリスクがある場合に、公共のイベントなどにおいて参加者の個人データ (写真・音声など) を記録し保存する権限 (BPoIG 第 26 条)
- 不法入国防止や国境安全、又は警察機関や鉄道・空港など特定の施設 (及びその中の物資や人間) に対する危害を防ぐ目的で、連邦警察が対象者の画像を自動記録する権限 (BPoIG 第 27 条)

ウ 刑事訴訟法 (StPO)⁵¹

刑事訴訟法 (StPO: Strafprozeßordnung) は、刑事訴訟手続に際し、警察が被疑者の写真、指紋又はその他身体的な測定値などの情報を記録することを認めている (StPO 第 81b 条)。また、対象者の許可が無くとも、写真やその他監視目的のために用意された特別な機器の使用が許可されている (StPO 第 100h 条。ただし、前記の手段は、事実の立証や被疑者の身元特定などの方法が成果に乏しい場合に限られる)。

刑事訴訟手続における警察による個人データ使用の一般的な権限としては、警察が運営するデータベースとその他の個人情報を自動照合することが認められている (StPO

⁴⁸ これら規定の英訳は存在しないためその存在及び概要を指摘するにとどめる (刑事訴訟法を除く)。

⁴⁹ Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz - BKAG) https://www.buzer.de/BKAG_Bundeskriminalamtgesetz.htm

⁵⁰ Gesetz über die Bundespolizei (Bundespolizeigesetz - BPoIG) <https://www.buzer.de/gesetz/6381/index.htm>

⁵¹ THE GERMAN CODE OF CRIMINAL PROCEDURE <https://policehumanrightsresources.org/content/upload/s/2016/08/Criminal-Procedure-Code-Germany-1987.pdf?x19059>

第 98c 条)。

なお、個人データの使用については、裁判所や検察などの特定の関係当局が、刑事訴訟手続のために個人データを扱うことが許可されており、これには別件刑事訴訟に際する使用も含まれている (StPO 第 483 条)。加えて、将来的な刑事訴訟手続のために、関係当局が被疑者個人の特徴などを記録し使用できると規定されている (StPO 第 484 条)。

2 その他参考情報

(1) ドイツ連立政権による公共の場での生体認識を用いた監視を禁止する公約

2021 年 11 月 24 日、連立政権を樹立したドイツ社会民主党、緑の党及び自由民主党は、顔認識 (facial recognition) を含む生体認識を通じて公共の場での監視を行う事を禁止する公約を連名で掲げた⁵²。本公約では、欧州連合レベルでの規定としてその是非が議論されている欧州 AI 規制法案を支持する立場を取り、AI 規制法案と同様、顔認識 (facial recognition) によるプライバシーの侵害や、国家による市民の格付けなどを未然に防ぐ姿勢を明確にしたものと解される。

(2) ドイツ国内の警察・地方自治体による顔認識技術の試験的導入

ドイツ国内では近年、警察や地方自治体により顔認識 (facial recognition) 技術が試験的に導入されている。

2017～2018 年には、首都ベルリンのズートクロイツ駅にて、テロ防止を目的に顔認識ソフトウェアの試験的導入がなされた⁵³。同プロジェクトは 2 つの試験期間から成り、1 期目は 2017 年 8 月～2018 年 1 月まで、312 人の自主参加者を対象に行われ、2 期目は 2018 年 2～7 月まで、201 人の自主参加者を対象に開催された。この試験的導入では、参加者を駅構内で歩かせ、事前に記録した同参加者の画像と一致するかを調べた。結果としては、顔認識 (facial recognition) 技術の精度は必ずしも完璧とはいえず、誤認識も一定数検出された模様である。

また、同じく 2017 年にハンブルクで行われた G20 サミットに際し、ハンブルク警察は、警備の目的のために 8 つの異なる駅に設置された監視カメラから収集した情報など約 17 テラバイト相当のデータを収集し、その他インターネットやメディア上から集められたデータも含め、膨大なデータをもとに顔認識 (facial recognition) 技術を使って被疑者照合用のデータベースを作り上げた⁵⁴。同データは、その後専門家によるマニユ

⁵² Frank Hersey, *Incoming German gov backs EU ban on AI public facial recognition, social scoring* (26 Nov. 2021), <https://www.biometricupdate.com/202111/incoming-german-gov-backs-eu-ban-on-ai-public-facial-recognition-social-scoring>

⁵³ Marcel Fürstenau, *Germany's facial recognition pilot program divides public* (24 Aug. 2017), <https://www.dw.com/en/germanys-facial-recognition-pilot-program-divides-public/a-40228816>

⁵⁴ Matthias Monroy, *G20 in Hamburg: Data protection commissioner considers face recognition illegal* (15 Aug. 2018), <https://digit.site36.net/2018/08/15/g20-in-hamburg-data-protection-commissioner-considers-face-recognition-illegal/>

アルベースのチェックも経ている。このリソースと技術をもとに、特定個人の行動、イベントへの参加、趣向そして政治や宗教感についても判断ができることになると思われる⁵⁵。

更に、ベルリン、ハンブルク、ミュンヘンに次ぐドイツ第4の都市とされるケルンでは、「biometric ready」と呼ばれるカメラが、ケルン警察により法律事務所や礼拝所などを含むエリアに設置され運用され⁵⁶、正当な理由が無く人権を不当に制限するとの批判の声も上がった⁵⁷。2020年11月時点でケルン中心部に（警察の捜査目的で）設置されていた監視カメラの総数は約79台にのぼるとされる⁵⁸。

2018年にはマンハイムにおいても、対象人物の動き（moving patterns）を分析する68台の監視カメラが警察によりマンハイム各地に設置されている⁵⁹。当該監視カメラは犯罪が比較的多いエリアに主に設置されており、犯罪や暴力的な行為が検知された際には警察に通達され、検出の2分後には捜査が開始されるとの運用がされた。実際には、抱擁が「不審な行動（suspicious behavior）」と見なされるなど、誤判定も検出されたとのことであるが、情報を蓄積しトライアンドエラーを繰り返す中で判定ソフトウェアが学習を続け、不適切な行為を検知する能力及び精度も向上が確認されたとのことである。

(3) その他生体情報利用に対する姿勢・政策

第2・2・(3)及び第3・2・(2)で前述した Clearview AI に関しては、2021年1月、ハンブルクのデータ保護当局は、同社の顔画像データベースがEU圏内では違法である旨の決定を下している⁶⁰。本件は、Clearview AIのデータベースに自身の顔画像データが同意無く保存されていることを知った個人が、同社に対し、その削除を求めたものの、対応が無かったため、当局に届け出たことが端緒となった。しかし、約11か月に及ぶ調査の結果、当局は Clearview AI に対し、データの部分的な削除（各生体情報プロフィールのハッシュ値の削除）のみを求める処分を下したとのことである⁶¹。

2022年2月には、顔認識以外の方法による認証情報に関する論点であるが身分証明書に持ち主の指紋情報を記録する義務を不服とする市民団体がドイツ国内で提起した

⁵⁵ EDRI, 前掲注 45・p. 92

⁵⁶ EDRI, 前掲注 45・p.16-21

⁵⁷ EDRI, *Biometric mass surveillance flourishes in Germany and the Netherlands* (7 July 2021), <https://edri.org/our-work/biometric-mass-surveillance-flourishes-in-germany-and-the-netherlands/>

⁵⁸ Kameras stoppen, *Stand der Videoüberwachungsorte in Köln* (2020), <https://kameras-stoppen.org/videobeobachtung-in-koeln/>

⁵⁹ Saskia Bricmont, *Facial Recognition In European Cities – What You Should Know About Biometric Mass Surveillance*, <https://www.greens-efa.eu/opinions/2021/10/22/facial-recognition-in-european-cities-what-you-should-know-about-biometric-mass-surveillance/>

⁶⁰ Reclaim Your Face, *How he reclaimed his face from ClearviewAI* (10 Feb. 2021), <https://reclaimyourface.eu/how-to-reclaim-your-face-from-clearview-ai/>

⁶¹ NOYB- European Center for Digital Rights, *Clearview AI's biometric photo database deemed illegal in the EU, but only partial deletion ordered* (28 Jan. 2021), <https://noyb.eu/en/clearview-ai-deemed-illegal-eu>

訴えが、欧州司法裁判所（EUCJ）に持ち込まれた⁶²。ドイツでは2021年8月、新たに発行される身分証明書に所有者の指紋情報を記録したチップを搭載するよう法を改正しており、プライバシー等の基本的人権の侵害として、反発を受けた。なお、欧州司法裁判所での本件に関する公聴会の日程については、現時点では未定とのことである。

⁶² Biometric Update.com, *German court escalates ID card fingerprints requirement to European Court of Justice* (28 Feb. 2022), <https://www.biometricupdate.com/202202/german-court-escalates-id-card-fingerprints-requirement-to-european-court-of-justice>

第5 英国

1 犯罪予防や安全確保のための顔識別又は顔認識機能付きカメラの利用に関する法令

(1) 個人情報保護の観点からの規律

ア UK GDPR 及び 2018 年データ保護法 (DPA2018)

英国は 2020 年 1 月 31 日に EU を離脱し、同年 12 月 31 日時点で適用されていた GDPR を含む EU 法は国内法となっている(以下、国内法化した GDPR を「UK GDPR⁶³」という)。また、2018 年データ保護法 (DPA2018: Data Protection Act 2018)⁶⁴は、UK GDPR を補完し調整する形で英国のデータ保護制度の枠組みを定めた一般法であり、UK GDPR が適用されない法執行又は諜報目的に関する国内実施法部分を含んでいる。

イ ICO による公共の場所におけるライブ顔認識技術の利用についての意見

英国のデータ保護機関である情報コミッショナー事務局 (ICO: Information Commissioner's Office) は、2019 年、公共の場所における法執行機関によるライブ顔認識技術 (live facial recognition technology) の利用について意見 (以下「2019 年意見」という)⁶⁵を出し、更に、2021 年、公共の場所におけるライブ顔認識技術の利用について意見 (以下「2021 年意見」という)⁶⁶を出している。

2019 年意見は、ライブ顔認識の比率的ではない利用によって生じる個人の権利と自由へのリスク、個人の日常生活への不必要な侵入、警察の不当な介入等のライブ顔認識の利用による潜在的な不利益を踏まえ、法執行機関が公共空間において顔認識技術を展開するにあたっての個人情報の取り扱いに関して、法執行機関を導くために ICO が公表したものである。同意見では、ライブ顔認識の利用は個人情報の取り扱いを伴うため、DPA2018 が技術展開の必要性や比例性の検討、ウォッチリストの編集、生体データの取り扱い、当該データの保持・削除まで、ライブ顔認識のプロセス全体に適用されるとした。

2021 年意見は、より広範な目的及び様々な環境においてライブ顔認識を利用する管理者を対象とし、ライブ顔認識に伴う複雑で新しい種類の情報の取り扱いに DPA2018 がどのように適用されるかを説明するために公表された⁶⁷。同意見では、ライブ顔認識

⁶³ Regulation (EU) 2016/679 of the European Parliament and of the Council, <https://www.legislation.gov.uk/eur/2016/679/contents>

⁶⁴ Data Protection Act 2018, <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

⁶⁵ Information Commissioner's Office, *Information Commissioner's Opinion: The use of live facial recognition technology by law enforcement in public places* (31 Oct. 2019), <https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf>

⁶⁶ Information Commissioner's Office, *Information Commissioner's Opinion: The use of live facial recognition technology in public places* (18 June 2021), <https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf>

⁶⁷ 以下の記載は、2021 年意見 (前掲注 66) の「1. Executive Summary」を主に参照したものである。

の利用は個人情報の取り扱い、生体データ及び多くの場合において特別なカテゴリーのデータの取り扱いを伴うものであり、管理者は UK GDPR 及び DPA2018 の関連規定を遵守する必要があるとされ、具体的に次のものが挙げられている。

- 適法性、公正性、透明性、目的の限定、データの最小化、正確性、記録保全の制限、完全性、機密性及び説明責任等の原則の遵守 (UK GDPR 第 5 条)
- 適法性の要件の充足 (UK GDPR 第 6 条)
- 特別なカテゴリーのデータ⁶⁸や犯罪歴のあるデータの処理根拠と条件の開示 (UK GDPR 第 9 条及び第 10 条)
- 公共の場所でのライブ顔認識の使用決定に先立つデータ保護影響評価 (DPIA) の実施 (UK GDPR 第 35 条)

その上で、2021 年意見は、全体として、管理者は、厳格なレベルの精査によりその計画を慎重に評価すべきであり、法令は、管理者に、その情報の取り扱いが公正で必要かつ比例的であると正当化できることの証明を要求するものとしている。また、これら要件を踏まえると、ライブ顔認識が公共の場所で自動的かつ無差別に生体データを収集する場合、その適法な使用には高いハードルがあるとしている。

ウ 監視カメラ及び個人情報のための情報保護実施準則

2000 年、ICO は、1998 年データ保護法 (DPA1998: Data Protection Act 1998) に基づき、CCTV (Closed Circuit Television) の利用に関する実施準則を策定した。同準則は 2008 年に改訂されたが、その後、従来型の CCTV に加え、自動ナンバープレート認識 (automatic number plate recognition)、身体装着カメラ、顔識別 (to identify individuals' faces) 等の自動認識技術 (automated recognition technologies) を含める形で更に改訂された (最新版は 2017 年 6 月 9 日付の version 1.2⁶⁹であるものの、DPA2018 年の内容は反映されていない)。下記第 5・1・(2)・ア記載の監視カメラ実施準則と異なり、すべての公共機関・民間事業者が対象となる。

同準則では、自動認証技術の利用にあたっては、データ主体に対しデータの取り扱いにかかる情報 (privacy notice) を提供すること、顔識別という目的 (to identify individuals' faces) のために十分に正確に個人を撮影するために高品質のカメラを使用すること、自動照合の結果は、誤照合がないように訓練された人間により管理されるべきであること、同技術の利用にあたっては一定の human interaction が必要であること (完全な自動処

⁶⁸ UK GDPR において、生体データは、自然人を一意的に特定する目的で取り扱われる場合は、特別なカテゴリーのデータを構成し、かかるデータの取り扱いには UK GDPR 第 9 条を遵守する必要がある。

⁶⁹ Information Commissioner's Office, *In the picture: A data protection code of practice for surveillance cameras and personal information (Version 1.2)* (9 June 2017), <https://www.enlutc.co.uk/wp-content/uploads/2019/08/cctv-code-of-practice.pdf>

理のみで行われるべきではないこと）等が規定されている（同準則 7.4）。

エ ビデオ監視に関するガイダンス

2022年2月、ICOは、ビデオ監視（Video Surveillance）に関するガイダンスを公表した⁷⁰。同ガイダンスは、個人情報収集及び処理のためにビデオ監視システムを利用する公共機関及び民間事業者が、UK GDPR 及び DPA2018 の法的要求を遵守できるようにすべく策定され、また、UK GDPR に基づいてビデオ監視を利用する法執行機関にも関連するものとしている。

特定個人の個人情報を処理する監視システムを利用する組織は、UK GDPR 及び DPA2018 を遵守する必要がある。同ガイダンスにおける ICO の提言は、すべて UK GDPR 第 5 条の定める原則に基づくものであり、監視システムのライフサイクル及び実務に従うことを目指したものである。また、同ガイダンスは、ビデオ監視システムを利用する公共機関及び民間事業者が利用すべき複数のチェックリストを提供している。

同ガイダンスは、CCTV、自動ナンバープレート認識、身体装着カメラ、顔認識技術（facial recognition technology）、ドローン、スマートドアベルカメラ（smart doorbell cameras）及び車載カメラ等の技術を広くカバーしているが、DPA2018 第 3 章に基づく所轄官庁による特定の刑法執行目的でのデータの処理及び個人又は家庭活動の目的でのデータの処理には適用されない。

(2) 個人情報保護以外の観点からの規律

ア 2012年自由保護法及び監視カメラ実施準則

2012年自由保護法（PFA2012: Protection of Freedoms Act 2012）⁷¹は、第二部で CCTV その他の監視カメラシステムを規制しており、具体的には、国務大臣による監視カメラ実施準則の策定義務や監視カメラコミッショナー（Surveillance Camera Commissioner。監視カメラに関する監督機関であり、内部大臣により任命される。）の設置等を規定している（PFA2012 第 29 条から第 31 条等）。監視カメラコミッショナーは、同準則の遵守を促進し、同準則の運用をレビューし、同準則について助言するものとされている（PFA 第 34 条）。

FPA2012 に基づき、2013年、地方自治体又は警察による監視カメラシステムの適切な利用にかかる監視カメラ実施準則（Surveillance Camera Code of Practice）⁷²が策定された（2021年に改訂）。同準則では、地方自治体又は警察が監視カメラを設置し、そこ

⁷⁰ Information Commissioner’s Office, *Video Surveillance* (24 February 2022), <https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance-0-0.pdf>

⁷¹ Protection of Freedoms Act 2012, <https://www.legislation.gov.uk/ukpga/2012/9/contents/enacted>

⁷² Home Office, *Surveillance Camera Code of Practice* (Nov. 2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1035067/Surveillance_Camera_CoP_Accessible_PDF.pdf

から得られた情報を利用する際に従うべき 12 の原則（透明性、説明責任、一定の技術水準の充足等）を規定している（同準則 Guiding Principles 1.1～12.3）。なお、同準則はイングランド及びウェールズの地方自治体及び警察が対象であり、それ以外の民間事業者等は直接の対象ではない（民間事業者等は、任意に同準則を適用することが推奨される）（同準則第 2 項及び第 7 項）。

イ その他関連法令

前記記載の他、警察による顔識別又は顔認識機能付きカメラの利用を規制しうる法令としては、以下があげられる⁷³。

- 1998 年人権法（Human Rights Act 1998）⁷⁴
- 2010 年衡平法（Equality Act 2010）⁷⁵
- 2000 年捜査権限規制法（Regulation of Investigatory Powers Act 2000）⁷⁶

ウ 警察による顔認識技術の利用にかかる紛争

2019 年、市民団体が、ライブ顔認識技術の利用は 1998 年人権法、DPA1998 及び DPA2018 並びに 2010 年衡平法に違反しているとして、南ウェールズ警察を提訴した。

高等法院（High Court）は、顔認識技術の適切かつ恣意的でない利用を確保する十分な法的枠組み（監視カメラ実施準則を含む。）があり、南ウェールズ警察はその枠組みのなかで顔認識技術を利用していたとして、市民団体の訴えを退けた⁷⁷。

しかし、2020 年 8 月、上訴法院（Court of Appeal）⁷⁸は、顔認識技術の利用に関する明確なガイダンスは存在せず、南ウェールズ警察は当該技術が性的又は人種的偏見を持たないようにするための合理的な手続を取っていないとして、南ウェールズ警察による顔認識技術の利用を違法と判断した。なお、同判決を受けて、監視カメラコミッショナーは、2020 年 11 月、イングランド及びウェールズの警察による顔認識技術の利用にかかるガイダンス（Facing the Camera）を公表した。⁷⁹

⁷³ The Centre for Data Ethics and Innovation, *Snapshot Paper – Facial Recognition Technology* (28 May 2020), <https://www.gov.uk/government/publications/cdei-publishes-briefing-paper-on-facial-recognition-technology/snapshot-paper-facial-recognition-technology> 9.2 参照。

⁷⁴ Human Rights Act 1998, <https://www.legislation.gov.uk/ukpga/1998/42/contents>

⁷⁵ Equality Act 2010, <https://www.legislation.gov.uk/ukpga/2010/15/contents>

⁷⁶ Regulation of Investigatory Powers Act 2000, <https://www.legislation.gov.uk/ukpga/2000/23/contents>

⁷⁷ R (Bridges) v Chief Constable of South Wales Police and others [2019] EWHC 2341 <https://www.bailii.org/ew/cases/EWHC/Admin/2019/2341.html>

⁷⁸ R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058 <https://www.bailii.org/ew/cases/EWCA/Civ/2020/1058.html>

⁷⁹ Surveillance Camera Commissioner, *Facing the Camera* (2020), <https://www.gov.uk/government/publications/police-use-of-automated-facial-recognition-technology-with-surveillance-camera-systems>

2 その他参考情報⁸⁰

(1) 顔認識技術の利用状況

英国における公共空間における顔認識技術の利用は、警察によるものが多い。たとえば、南ウェールズ警察は、フットボールの試合や音楽コンサート、公共デモ及び王室の旅行時において利用しているほか、ロンドン警視庁は、刃物や銃、幼児の性的搾取又はテロリズム等の重大犯罪に焦点を当て、拘禁可能犯罪で指名手配された者をターゲットに顔認識技術を展開していると公表した。

顔認識技術の利用は民間の警備にも広がっており、多くの民間事業者が警備目的で顔認識技術を利用していると報告されている（たとえば、不動産会社によるロンドンのキングスクロス再開発地での利用や、小売店(Facewatch)の万引犯の照合の為の利用等）。なお、キングスクロス再開発地における防犯目的の顔認識技術の利用に関しては、ICOは不適切な技術利用の可能性を懸念しており、DPA2018違反の有無を調査中である⁸¹。

(2) 顔認識技術にかかる政策・動向

2020年、スコットランド議会は、顔認識技術等の次世代の生体技術及び顔に関する情報を扱う Scottish Biometrics Commissioner を設立するための法案を可決している⁸²。

⁸⁰ The Centre for Data Ethics and Innovation, 前掲注 73 を参考に記載した。

⁸¹ Zoe Kleinman, *King's Cross developer defends use of facial recognition* (12 August 2019), <https://www.bbc.com/news/technology-49320520>

⁸² The Centre for Data Ethics and Innovation, 前掲注 73・9.4 参照。