

〈エッセイ〉

公共空間における情報識別と警察活動についての覚え書き

永 石 尚 也

1. はじめに 「空気」を介した感染＝接触

本誌 no.55 掲載の拙稿では、2020 年 8 月初頭から 2020 年 9 月末までの在外研究・滞在で得られた情報に基づき、シンガポールにおける移動・位置情報の管理（特に店舗などの場所への入退情報を名前、国民番号（またはパスポート番号）、電話番号と紐付けて蓄積・管理することでクラスターの特定を行う SafeEntry システム）とその環境について紹介した。その後、再び 2020 年 12 月初頭から 2021 年 2 月中旬まで、二度目のシンガポール滞在・在外研究の機会を得ることができたが、折しもこの時期は、シンガポールにおける情報管理政策の転換が起こった時期に重なっている。

・転換点 2021 年 1 月

この時期は、スマートフォン／専用トークンの近接通信機能（Bluetooth）を用いて接触者を特定する接触確認アプリ・TraceTogether¹⁾（以下、TT とする。）が大規模商業施設等の入退出要件として義務化されるとともに、ネガティブな側面として同アプリで得られた情報が（2020 年 3 月導入当初の政府による説明とは異なり）殺人事件の捜査（司法警察活動）へと転用されていたことが、国会答弁の中で明らかになった時期でもある。この転用が明らかになった 2021 年 1 月 4 日、時を同じくして TT のプライバシーポリシーが（刑事訴訟法の枠内ではあれ）司法警察活動への接触情報の転用を認める方向で改定されたことも、政府への不信に拍車をかける事態となった。

・背景 「耳を傾ける政府」

この背景には、2020 年 3 月の導入時点から、TT が、GPS を用いた位置情報監視やクレジットカード使用履歴を通じた行動履歴監視とは異なり、オプトイン方式など個人情報保護・プ

ライバシーに配慮した設計・利用のプロセスを強調していたことが挙げられる。2020 年選挙における野党躍進への苦慮から、政府与党が「耳を傾ける」ことをアピールし続けることで国民の信頼を確保してきたことも相まって、TT の転用事件は政府の変節を疑わせる事情となったことは想像に難くない。反面から見れば、長引く COVID19 対策への有効打を欠いたまま、長期の行動制限への不満の高まりに対処するために、政府としてとりうる方式の一つが、国民の自発性という外観を調達しやすい TT の事実上の義務化だったと見ることもできる。結果として、TT 自体への反対運動が SNS・ニュースメディアを通じて大きく拡散されるなど、「感染（接触）を通じた統治」の正統性を政府自ら揺らがせる結果となった²⁾。

・再転換 2021 年 6 月

しかし、事態のおよそ半年後の 2021 年 6 月になると、変異株の影響もあいまってシンガポールで再度の感染拡大が広がる中、TT と SafeEntry システムが統合され、アプリのダウンロードまたはトークンの所持が法的裏付けの元で義務化されることとなった。この背景には、TT の利用割合が国民の 90% を超え、与野党を通じた合意事項となったことがあげられる。これを受けて、種々の行動制限とともに、人の出入りが多いショッピングモール、職場、礼拝所、学校、教育機関などに加え、人が長時間密接している可能性が高い飲食店やスポーツジムなど幅広いエリアにおいて TT と SafeEntry が連動した強固な情報管理体制が敷かれることとなった³⁾。長期にわたって他国よりも厳しい行動制限が続く中、「よりまし」な選択肢として TT による負担の小さな監視を受け入れることで自由を確保したいという国民と政府との間の同床異夢といえる。

・「耳を傾ける政府」再び 2021 年 8 月

この一方で、TT については、むしろその機能が民間事業者によって過剰に利用されるデメリットを回避するための緩和措置が、2021 年 8 月に実施されたことも注目に値する⁴⁾。具体的には感染リスク情報についての通知を取りやめたことである。この通知は、必ずしも感染していることを示すものではなく（あくまでも強制的な隔離には至らない）一定期間の自己監視のために用いられるはずのものとされていたが、（ワクチン接種歴情報、すなわち本人を特定する）当該情報を民間事業者が入店を拒否するリスクの代理指標（proxy）として用いていたことが明らかになったことが背景にある⁵⁾。ここでは従来の対立構図が、垂直的な国家—個人関係から、水平的な私人間関係へとスライドしている。

このように TT をめぐる政府・民間事業者・個人の間の相互調整プロセスは、情報管理と安全管理のバランスを確保するために、どの主体が、どの情報について、いかなる条件のもとで収集・蓄積・利用・転用（外部提供）を可能にするか、また遮断（破棄）を行うべきか、アーキテクチャ設計・運用を通じてこれら協同をいかなる原理・価値の下で実現するか……これらの動的プロセスについての興味深い事例を提供してくれる。

さらに、これら位置情報・接触情報の問題を超えて、現在 EU 圏を中心に議論されている顔識別・顔認証技術による公共空間における監視についても、類似の構造を持つものとして大いに示唆を与えてくれる。この問題は、折しも本稿執筆時の 2021 年 8 月に JR が指名手配中容疑者、不審者に加えて重大犯罪の出所者・仮出所者に対し、顔識別技術を利用していた問題が明るみに出た本邦においても原理に遡った議論を呼ぶものであるだろう。

以下では、この問題を、公共空間における生体情報識別をめぐる問題と比較しながら、現下の問題状況の整理を中心に、政府・民間事業者・個人の間の相互調整プロセスの変容から把握する観点を紹介する。なお以下の記述については、2021 年度 4 月—5 月における東京大学大学院学際情報学府における講義「社会情報学基礎Ⅲ」で

の検討を元に行っている。紙幅の都合で省いた論点も含めて講義資料はウェブ上で閲覧可能であるため、あわせて確認されたい。

2. 公共空間における位置・移動情報／接触情報

(1) 公共空間における位置・移動情報の問題

位置・移動情報はその大半が、路上や訪れた場所など公共空間における行動の履歴を反映したものである。公共空間においては、人は誰からも見られ「う」るのであり、追跡され「う」るのだから、人々は、見られるリスクを予め受忍し、追跡されるコストを既に支払っているとも考える。実際、アメリカにおける状況を踏まえてローレンス・レッシングは、公共空間におけるプライバシーについて、伝統的な答えでは、と前置きしつつ「公共の場に出ることで、その人は自分について他人が知ることを隠したりコントロールしたりする権利を全て放棄したことになる」⁶⁾と述べる。元来、私生活上の平穏を中核に据えてきた「プライバシー」を公共空間において保護するというのは語義矛盾であるというわけだ。

もちろんレッシングの意図は、この伝統をインターネット空間の特性に則して（アメリカ憲法修正第 4 条を）「翻訳」することにある⁷⁾わけだが、日本においては捜査機関による公道上における写真撮影のケース（京都府学連事件⁸⁾）を皮切りに、私生活上の自由の一内容として「承諾なしに容貌・姿態を撮影されない権利」を継続的に保護の対象としてきた。この背後には、一見瑣末に見える位置・移動情報であっても、集積・結合が技術的に容易になれば（思想・信条、精神・身体に関する基本情報、その他重大な社会的差別の原因となる）センシティブな情報を構成することで、①構成された情報が蓄積・（内部）利用・（外部）提供されうる個別的风险に加え、②当該情報に基づく選別・処理への異議申立て機会・環境自体が奪われうる不可視のリスク⁹⁾を生み出すことが挙げられる。必ずしも技術に精通しているとは限らない裁判所がこれらのリスクについて直接に判断することは困難を伴うことから、証拠取得・証拠保全の必要性は緩やかに判断されてきたものの、上記の諸リスクが限定的なものであるべきである点について

は昭和 44 年判決の枠組みを念頭に明示的に判断されてきた傾向が見て取れる。

この傾向を理解するにあたっては、一つには保護されるべき私生活・私的空間の範囲を技術の高度化と相関する形で拡張してきた判断がある。つまり、捜査に用いられる技術の高度化・密行化¹⁰⁾とともに、単に現認するのみならず瞬間を固定し(写真撮影)、また長期的な運動を保存し(動画録画)¹¹⁾、あるいは肉眼よりも精緻化し(高解像度化)、あるいは事前に告知することなく長期にわたる移動・行動履歴を追跡する(GPS 監視)¹²⁾ことが可能になる技術的特性を念頭におけば、動静が逐一把握される「侵入」されうる(住居・書類及び所持品に準ずる)「私的領域」の範囲がその自然的性質上基本的には拡大することが導かれる¹³⁾。

(2) 民間事業者を通じた情報取得の問題

他方でこの傾向が、捜査機関にとっては私人(民間事業者)を通じた情報取得・蓄積・照合等によって回避される傾向を生んできたことも注目される。具体的には、捜査関係事項照会(刑事訴訟法 197 条 2 項)による情報取得が広範になされていたことが明らかになったカルチュア・コンビニエンス・クラブの事件(2019 年)により広く知られるところとなった、私人(民間事業者)の持つ情報への捜査機関による「便乗」現象である。憲法 35 条上の問題・令状による審査が回避される一方で、明文における事前・事後の情報管理の規律を欠くために不可視化のリスクが増大する。ここから、必要な範囲の限定やコストについての比例性等を、事後的に検証するプロセスの必要がより際立つことになる。

この点につき、私人(民間事業者)を通じた情報取得・照合の例として、アメリカにおける GPS 判決・Jones 判決(2012)¹⁴⁾後に出された Carpenter 判決(2018)¹⁵⁾が好例となる。本事件は、裁判所の開示命令(court order)を通じて強盗被疑者の基地局位置情報を携帯電話事業者から取得した事件であり、争点としては、携帯電話を保有することで事業者に提供することになる基地局位置情報については、①捜査機関による捜査との関係で保護されるべきプライバシーに属するか(修正第 4 条該当性)、②また携帯

電話事業者から捜査機関へと開示されうる危険・リスクを任意で負担したものと見えるか(第三者法理)が問題となった。

注目すべきは、①について裁判所が、現代社会における携帯電話保有の位置付けとともに、技術的な追跡のためのコストと反比例したプライバシー保護の必要性の増大を提示している点である。要約すれば、おおよそ以下の通りである。(ア)デジタル時代以前、法執行機関は被疑者を短期間追跡してきたが、長期間の追跡を行うことは困難かつ高コストであったため、ほとんど実行不可能であった¹⁶⁾。それゆえに、社会は法執行機関の捜査官が例えば個人の車両の逐次の動静を長期間・秘密裏に監視・記録することはないと期待していたし、実際に不可能だった。(イ)しかし、現代社会において基地局位置情報は、GPS 情報と同様に個人の個別の動静のみならず「家族、政治、仕事、宗教、性的関係」を明らかにし、個人の生活を監視する機会を提供する。ましてや車両等と異なり、携帯電話は否応なしに常に携帯せざるをえず、所有者を正確にフォローし続ける。さらに、(イ)の性質からは従来の判決が問題としていた商業取引で使用される小切手や預金口座とは異なる帰結を生み出す。現代社会への参加に当たって不可欠な携帯電話は、ネットワークを切らない限り情報が自動的に収集される技術的性質をもつ。この技術的差異とあわせて、(ア)の網羅的・長期的な収集状況(本情報については 5 年間の保有)に鑑みれば、プライバシーの合理的期待を放棄したとはみれず、②の開示リスクを任意で負担したものと評価できない。

(ア)では網羅的・長期的な捜査が民間事業者の情報収集を通じて低コストでなされうることが確認され、仮にそれが実行可能であるとすれば独自の規律が必要であることが示される。加えて、(イ)では技術的性質に照らし、(GPS よりも精度上劣るとはいえ)携帯端末の着信等に用いられる基地局エリア情報(行動履歴としては十分な基地局識別番号・端末識別番号・取得日時等)を取得されることを前提に、(GPS とは異なり)携帯端末所持者の個別の機能オフが不可能であることも加味して、プライバシーの合理的期待と第三者法理の不適用が判断されたも

のと考えられる。

(3) 複合問題としての TraceTogether (TT)

以上で見た問題は、TT を用いた接触情報についても一定の条件の下で当てはまる。

第1節で見たとおり、TT は直接に位置・移動情報を特定する技術的性質を有するものではないものの、国民番号・氏名等情報が集権的に管理されるハイブリッド型であることを加味すれば、第2節(1)で見た技術的特性からは、「家族、政治、仕事、宗教、性的関係」等の代理変数(proxy)として端末間接触情報は積極的に利用可能であり、現に接触情報についての保健省による聞き取り手続きと連動している。

さらに TT は、トークンについては技術的に、アプリについては法令上切断を禁じられており、情報を遮断すること(例えば電源切れについて対処しなかった不備等)についての積極的説明の負担は、所有者個人に帰されることとなる。ここから第2節(2)で見たとおり、技術的不可避性の問題も共有する。

最後に、TT は公衆衛生上の観点から行動制限と強く結びついた義務化へと舵を切ったにもかかわらず、警察活動へと秘密裏に転用され、その事態が明るみに出るとともにポリシーの改訂がなされていたという法律の留保に基づく監督規律潜脱が挙げられる。これは、まさに第2節(2)で見た民主主義的価値の潜脱の問題である。そもそも強制処分法定主義の根拠は一般的に、要件・手続の事前の正当な定めを求める自由主義的要請に加えて、国家法によってその定めに一応の正統性が付与されたとする民主主義的要請に求められる。そして後者の民主主義的要請については、行政警察活動においても代替的な補完が求められる。しかし TT については、その導入に際して行政上の政策として導入されるとともに、事後的にこの補完もなされないままに、個人化された「選択」によって事実上の運用が継続している状態にある。

もしも個人化された「選択」による自発的・事実的な運用に基づく迂回的な正統化が可能であるならば、正統化の概念は規律概念としての有用性を消尽させることになる。ここから、民間情報に「便乗」しつつも、個人の負担がごく小

さいながらも薄く広く浸透する(panvasive な¹⁷⁾) 捜査への規律を再設計する必要を迫る。

3. 公共空間におけるリアルタイム生体識別

(1) 識別(identification)と認証(authentication)

第2節では捜査機関における情報の取り扱いの中で、情報の種別としての位置・移動情報の規律を論じた。他方で、データの処理プロセス自体についての規律で近時欧州を中心に議論されているのが、公共的にアクセス可能な空間におけるリアルタイム生体識別である。特に警察活動での利用には、明示的に制限が課されている。以下では、2021年4月におけるAI規則案¹⁸⁾をベースに、リアルタイム生体識別の論点を整理する。

まず生体(biometric)情報とは、個人を他と区別する特有な身体・精神・振る舞いにかんする情報一般を指し、外延的には顔貌・容貌だけでなく歩行情報、指紋情報、DNA 情報、声帯情報、キーストロック、その他把握されうる行動信号を広く含むと理解される。ここで機能面から分節するならば、上記の通りデータの処理プロセスについての規律を問題とすることから、本人の認識に基づき本人確認のために用いられる認証(authentication)とは異なり、本人の認識の外で本人を他と区別して処理する識別(identification)こそが問題となる。言い換えれば、本人の認識如何にかかわらずに、一定の目的で本人についての情報を他と機械的(automated)に区別する処理(processing of personal data)一般を指す¹⁹⁾。物理的な顔認識(recognition)は認証・認識双方の前提であり、目的により認証・認識は区別される。

識別が問題となる理由は、人々を所定のカテゴリに当てはめることで気づかれることなく影響を与えてしまう点、透明性と正確性を欠くことで人々の権利・自由へのリスクをもたらす点、差別・不平等な取り扱いをもたらす点、人の尊厳を損なう点などに求められるのであり、形式的な同意は識別を正当化しない。もちろん識別は、生体情報以外でも生じるものの、生体情報は、その取得・採取が技術的に簡易かつ秘密裏にもなされうる傾向が高まっていることに加え、その情報が年月を通じた非可塑性を

保持するという特徴からより注目に値する²⁰⁾。

最後に、リアルタイム (real-time) 性とは、上記の生体情報の取得・比較・識別の処理が、(ほぼ) 瞬時に、あるいは大した遅延がなくなされることを指す。この点で、事後 (post) 的に行われる識別とは区別される。リアルタイムな処理は、事後 (post) 識別より一層、人々に監視されている感覚を与えることで間接的に行動を (事前に) 制限する点、そしてリアルタイムの介入に対してはチェックや修正の機会を (事前に) 欠く点が問題となる。このような問題から、リアルタイム生体識別は、一定の重大な犯罪の嫌疑がある場合について、原則として司法当局による事前の認可に基づいてのみ許容される。

(2) 「公共空間」の変容と残された課題

リアルタイム生体識別は多くの問題を含む。例えば本邦でも、警察保有の顔写真情報と防犯カメラ画像や SNS 上の顔画像とデータベースとを照合する運用がなされているが、他国では顔認識上の問題として既に、①自動処理を通じた誤判定リスクが薄く広がる問題と、②技術的問題としての人種間による誤判定リスクの不平等性の問題が生じている。

しかしより深刻な問題は、欧州データ保護監察機関が、AI 規則案の 2 日後に提出したプレスリリースにおいて、上記の生体識別が「個人の私生活に深く非民主的に (non-democratic) 侵入するリスクが極めて高い」²¹⁾と指摘した、民主的な価値毀損の問題である。

この問題は、上記の誤判定や誤認逮捕のリスクを超えて、ジョナサン・ジットレインが「インターネットの未来」(2008) で述べた「完全な執行 perfect enforcement」に近づく場合にこそ生じる。すなわち、精密に個人が識別されるときに物理的な公共空間のもつ「公共性」の蒸発リスクである²²⁾。言い換えれば、匿名的なままでコミュニケーションが可能となる「誰でもない」場所の消失により、個々人が政治的空間の中でお互いの立場を交換可能であると認める基礎を失ってしまうことにこそ問題の根があるのではない。国家が自らに求められる正統性が求められる権限の行使を回避する²³⁾ことで、COVID19 の中で起きている市民間の不和に見

られるように、諸リスクは個々人の間で調整すべき危害へと翻訳されることになる。

この問題は、単にアルゴリズム支配的なシステム (algorithmic system) の問題に限られない。より一般に、上記で論じてきた意味で、健全な相互作用を可能とする情報環境の構築と比較可能である。たとえば、ブロックチェーンを用い、製造者に永続的・自律的な制限を厳密に課す能力を与える耐改竄性に裏打ちされたスマートコントラクトの設計の中では、個々人の利用や創意工夫、あるいは修繕の可能性が閉ざされてしまう事態と比較できるし²⁴⁾、あるいはレッシングが「適切なフェアユースの余地を残したコード保護システムだけが議会の法の保護対象となる」²⁵⁾と宣言したデジタルコモンズと比較できる。契約の経済学の観点からは、リソースの利用価値が定まっておらず、リソースの投下先が確定的には決まっていない中における権限の非占有 (分配) の問題が現れる。

確かに監視は、個人化された私たち一人一人の一面において心地よい。しかし、その快さは (原理的にももちろんのこと) 集合的に見た私たちにとってなお善いものではない。自然的傾向としての不安の裏返しとしての監視の心地よさは、不安を統御する私たちにとってそうすべき (二階の) 理由を与えるものではない。紙幅が尽きたために論じ切れなかったものの、上記の状況依存のかつ状況適合的な私たちの傾向性を統御する民主主義の基盤となる価値として、公共空間を成立させる存在の匿名性の内容とともに、各種の情報 (価値) がある仕方で消尽することによって初めて成立する (公正な) 政治・競争環境について、いずれ別稿にて取り上げたい。

本研究は JSPS 科研費 JP20K13300 の助成を受けたものである。

註

- 1) TT は Bluetooth 方式の中でも、接触情報そのものは端末レベルで分散管理しながらも、国民番号・氏名・連絡先などの情報を中央サーバーで管理する、いわゆるハイブリッド方式を採用している。TT の情報取得方式は概ね下記の通りである。①登録時にユーザーの連絡先情報を取得する、②アプリの識別子と連絡先情報データベースを保管、③ユーザー陽性時に、過去 2 週間に接触した全識別子リストを自動アップロードする、④ DB 中の識別子をから接触ユーザーに保健省から電話／メールを行う。
- 2) この顛末については、Reuter 社の“Singapore COVID-19 contact-tracing data accessible to police” (2021 年 1 月 4 日) などで確認することができる。
- 3) 在シンガポール日本大使館「新型コロナウイルスの発生に関する注意喚起 (その 43)」 (2021 年 4 月 23 日 <https://www.sg.emb-japan.go.jp/files/100182789.pdf>) などを参照せよ。
- 4) StraitTimes “TraceTogether app’s possible Covid-19 exposure alert has been removed” などを参照せよ。なお、TT は本文に記載した個別通知を切ったとしても、シンガポール保健省が高リスク者と判断した場合には、個別に電話・SMS 通知を行うオペレーションがなされる点で不可避的である。この点で、日本の接触確認アプリとは異なる。
- 5) 後述するワクチン・パスポートの民間事業者への転用にまつわる不平等の問題と同様の事態が、ここでは現出している。
- 6) ローレンス・レッシング『CODE: 2.0』 (翔泳社、2007 年) 281 頁。
- 7) 同上。レッシングは続けて、「公共の場にいるときの各種事実は、法的には保護されていなくても、そうした事実を集めたり利用したりするコストの高さによって実質的に守られている。摩擦こそはプライバシーの最高の友というわけだ。」と確認する。本稿で問題にするように、問題はプライバシーを取り巻く環境依存的な「摩擦」の変容プロセスにある。
- 8) 最大判昭和 44 年 12 月 24 日刑集第 23 卷 12 号 1625 頁。
- 9) このほかにも P. Norberg のいう「プライバシーのパラドクス」、H. Nissenbaum のいう「透明性 (合理的無知) のパラドクス」などがある。ただし本稿では、いずれも自己の情報管理を放棄する環境的要因を指摘するものとして、本文②に含めることとする。この点につき、メグ・レタ・ジョーンズ『Ctrl+Z 忘れられる権利』 (勁草書房、2021 年) の第二章を参照。
- 10) 捜査密行の原則については、捜査比例の原則に反するという論拠に加え、一般的に罪証隠滅のおそれが認められる場合には強制処分により対処することが原則である上に、DNA 型情報などそもそも罪証隠滅が物理的に不可能な事例について、本原則は適用されない。久岡康成「捜査における手続保障——捜査の密行性概念の再批判——」刑法雑誌 27 卷 4 号 47 頁 (1987 年) および同氏による東京高判平成 28 年 8 月 23 日高裁判集 69 卷 1 号 16 頁の判例紹介 (立命館法学 378 号、2018 年) を参照せよ。
- 11) 最判平成 20 年 4 月 15 日刑集第 62 卷 5 号 1398 頁。
- 12) 最大判平成 29 年 3 月 15 日刑集第 71 卷 3 号 13 頁。なお現在の GPS 即位精度は 3-10m 程度であるものの、準天頂衛星に基づくと 20-30cm 程度となり、後者の精度によれば行動補足に加えて人の識別に使えることになる。宍戸ほか編著『AI と社会と法』 (有斐閣、2020 年) 第 9 章・佐藤一郎発言を参照せよ。
- 13) 稲谷龍彦『刑事手続におけるプライバシー保護』 (弘文堂、2017 年)。なお、警察保有のデータベースとして被疑者写真約 1100 万件、指紋約 1100 万件、DNA 情報 (被疑者 DNA 型記録、遺留 DNA 型記録、変死者 DNA 型記録、特異行方不明者等 DNA 型記録) 約 140 万件の保有が確認され、運用として対象者の死亡時、誤認逮捕であることが明らかになったときには「保管する必要がなくなったとき」にあたるとして削除されるものの、不起訴時や無罪判決を得た時にも削除されない (2021 年 5 月 11 日参院内閣委員会における質疑)。
- 14) United States v. Jones, 565 U. S. 400 (2012)。
- 15) Carpenter v. United States, 201 L. Ed. 2d 507, 2018 U.S. LEXIS 3844, 138 S. Ct. 2206, 86 U.S.L.W. 4491, 27 Fla. L. Weekly Fed. S 415, 2018 WL 3073916. 邦語による紹介として、尾崎愛美・亀井源太郎「基地局位置情報取得捜査と令状の要否——Carpenter v. United States 判決を契機として」情報法制研究 4 号 (2018 年) がある。
- 16) レッシング『コモンズ』 (翔泳社、2006 年) 282 頁を参照せよ。「現実空間では認められていた活動 (法がそれを保護しているからか、あるいはそれを追跡するコストが高すぎるために認められていた) がサイバー空間にますます移行するにつれて、その活動に対するコントロールは増してきた。」
- 17) Christopher Slobogin, “Panvasive Surveillance, Political Process Theory and the Nondelegation Doctrine” Georgetown Law Journal, Vol. 102, 2014, Vanderbilt Public Law Research Paper No. 14-13.
- 18) 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” (2021).

- 19) 高木浩光「個人情報保護から個人データ保護へ」情報法制研究 第2号 (2017)。高木によれば processing of personal data の規定そのものは、1980 年における欧州評議会「個人データの自動処理に係る個人の保護のための条約」に遡り、一般データ保護規則 (GDPR) (2016 年) におけるプロファイリング規制 (決定の自動処理規制) はこれを踏襲したものである。なお GDPR 上におけるプロファイリングが、日常用語としての属性推定を指すものでないことについても、同論考を参照せよ。
- 20) 捜査機関が警察官であることを秘して被疑者にコップ入り飲料を飲ませ、その唾液がついたコップを回収することで DNA 採取を行った事件 (東京高判平成 28 年 8 月 23 日高裁判集 69 卷 1 号 16 頁) を参照せよ。このケースでは、反実仮想的に意図に反する DNA 採取であったことに加え、留置に該当しないことから、令状主義の精神に反する強制処分に該当し、証拠排除された。
- 21) EUROPEAN DATA PROTECTION SUPERVISOR “Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary” (2021).
- 22) 2021 年 8 月に発表されたアップル社による (iCloud フォトライブラリーの同期システムに接続された) 児童虐待に関する写真の自動収集措置によってイメージされるように、①情報収集における panvasiveness の観点からは、本稿の関心からは、個別の被疑者に対する嫌疑に裏付けられた司法警察活動と行政警察活動、公安活動との差異を曖昧にする問題が指摘できる。もちろん②執行・運用のコストの観点からは、嫌疑者の全てが法執行の対象になるわけではないと一応は言える。しかし、①メッセージとして「全てが見られうる」ことがもたらす市民社会へのコストと、②「現に執行対象となった者が選ばれた偶然性」による法の正統性の揺らぎという二つの問題を惹起するおそれには各々対処する必要がある。次稿に続く問題提起として記す。
- 23) ショシャナ・ズボフの『監視資本主義』(東洋経済新聞社、2021 年) において着目されるべきは、9.11 後におけるグーグル社と国家安全保障局 (NSA) の間の常態的な官民協同を論じた (アメリカ例外主義に準えた) 「監視例外主義」であるだろう。さらにこの問題が自動化すれば、「アルゴリズムと共謀」の問題に通じる。前掲『AI と社会と法』第 2 章Ⅲの市川発言を参照せよ。
- 24) アーロン・ライト、プリマヴェーラ・デ・フィリッピ『ブロックチェーンと法』(弘文堂、2020 年) 231 頁。なおアーカイヴが有する生成力につき、ジャック・デリダ『アーカイヴの病』(法政大学出版局、2017 年) 26 頁も参照。「覚え書の技術一般としてのアーカイヴは、単にそれなしでも存在したか存在しているだろうと信じられるような、いずれにせよ存在するだろう過去のアーカイヴ化可能な内容の、貯蔵と保管の場所なのではない。そうではなく、アーカイヴ化するアーカイヴの技術的構造は、アーカイヴ化可能な内容の構造のことも、その出現自体において、そしてその未来との関係において決定するのである。アーカイヴ化は事件を、記録するのと同じほどに生み出す。」
- 25) レッシング『コモンズ』(翔泳社、2006 年) 388 頁。

(永石尚也・本学非常勤講師)