資料２

# 犯罪予防や安全確保のためのカメラ画像利用に関する有識者検討会
# プライバシー権からのコメント

慶應義塾大学法科大学院　教授
山本龍彦

# Ⅰ．プライバシーの権利の展開

## 1．【第1期】古典的プライバシー権（私生活秘匿権）

※ワレン＆ブランダイス「プライバシーの権利」（1890年）
→イエロー・ジャーナリズムの氾濫（背景：写真技術、印刷技術の向上）
→私生活を守る必要（let me be alone）
→私生活上の秘密を公表・暴露されない権利

☆**「宴のあと」事件判決**（1964年　ワレン＆ブランダイス論文から70年以上）

→「私生活をみだりに公開されない権利」（不特定多数に私事を暴露されない権利）

※「今日のマスコミュニケーションの発達した社会では個人の尊厳を保ち幸福追求を保障するうえにおいて必要不可欠なもの」（憲法の価値原理と紐づいた権利として位置付けられる→憲法の理解が私法上のプライバシー権理解にも一定の影響を与えうる）

## 2.【第2期】自己情報コントロール権（情報自己決定権）

→1960年代にアメリカにおいて「情報論的転回」が起こる

→日本では佐藤幸治「プライヴァシーの権利（その公法的側面）の憲法論的考察」（1970年）以降、通説化

・背　景　①コンピュータ技術の発達

②生活実態との適合性

→秘密は「隠す」だけなのか？

→選択的に開示しているのではないか？

→誰に何を見せるのかをコントロールしながら生きている

→このコントロールが奪われたとき、私たちはまともな社会的生活を送ることができるのか？（家族に見せる情報、友人に見せる情報、同僚に見せ情報、国家に見せる情報）

・なぜ「プライバシー（権）」が必要か？

→自律的に生きること（人間関係の主体的な形成）、不当な選別からの自由、自由に生きること（萎縮効果の除去）、健全な民主主義の維持

〇前科照会事件（1981年：最判昭和56年4月14日民集35巻3号620頁）

「前科等のある者もこれをみだりに公開されないという法律上の保護に値する利益を有する」
→前科情報〔非私生活情報〕の特定第三者に対する「開示」。
※1　ドイツ憲法裁判所による国勢調査判決は1983年（BVerfGE 65, 1）。
※2　京都府学連事件？　ノンフィクション逆転事件？　石に泳ぐ魚事件？　カレー事件法廷撮影事件？（隣人ネットワーク選択、witnessの「選択」の保障と関連したものと解する余地？）

〇江沢民講演会事件（2003年：最判平成15年9月12日民集57巻8号973頁）

「プライバシーに係る情報の適切な管理についての合理的な期待を裏切るものであり，X らのプライバシーを侵害するものとして不法行為を構成する」。「〔単純〕個人情報についても，本人が，自己の欲しない他者にはみだりにこれを開示されたくないと考えることは自然なことであり，そのことへの期待は保護されるべきものである」。「X らの意思に基づかずにみだりにこれを他者に開示することは許されない」。

〇ベネッセ事件（最高裁2017年：平成29年10月23日判時2351号7頁、差戻し後の控訴審2019年：大阪高判令和元年11月20日判時2448号28頁）

・最高裁：「原審は、……プライバシーの侵害によるXの精神的損害の有無及びその程度等について十分に審理することなく、不快感等を超える損害の発生についての主張、立証がされていないということのみから直ちにXの請求を棄却すべきものとしたものである。そうすると、原審の判断には、不法行為における損害に関する法令の解釈適用を誤った結果、上記の点について審理を尽くさなかった違法があるといわざるを得ない」。

・差戻審：「個人情報が外部に漏えいしてプライバシーが侵害された場合に、当該被漏えい者が精神的苦痛を被ったか否か及び被った精神的損害を慰藉するに相当な額を検討するに当たっては、流出した個人情報の内容、流出した範囲、実害の有無、個人情報を管理していた者による対応措置の内容等、本件において顕れた事情を総合的に考慮して判断すべきである。」「具体的に名簿利用による勧誘や電話により日常生活に支障を及ぼすなどの損害が発生したときには、それが本件漏えいと相当因果関係のある損害であることを立証して損害賠償請求できることはもちろん、それに至らない場合であっても、本件個人情報を利用する他人の範囲を控訴人が自らコントロールできない事態が生じていること自体が具体的な損害であり、控訴人において予め本件個人情報が名簿業者に転々流通することを許容もしていないのであるから、上記のような現状にあること自体をもって損害と認められるべきである」

→権利侵害について論じたものではなく、あくまでも損害（harm）の有無について論じたものである。しかし、「コントロール」の利益を示唆するものとして注目される。

## ○DNA抹消命令判決（名古屋地判令和3年1月18日）

「DNA型（・・・あくまで人を識別するための限られた情報としてのデータである。）についても、基本的には識別性、検索性を有するものとして、少なくとも指紋と同程度には保護されるべき情報であるため、何人もみだりにDNA型を採取されない自由を有すると解される」

「指紋及びDNA型は、・・・秘匿性の高い情報とはいい難く、これと同程度に慎重に扱わねばならない情報とまではいえないが、・・・万人不同性、終生不変性ないしこれらに近い性質を有するもので、識別性、検索性を備えており、特定のもののみ登録・管理され、他者に対する開示が予定されていない情報という性質を有しており、氏名等に比べれば、より高い秘匿性が認められるべきものであり、それゆえ、公権力からみだりに取得されない自由が保障され、<u>みだりに利用されない自由</u>が保障されるものと解される」

「適正に管理・使用される限り、国民が、罪を犯すことなく、私生活を送る上では、格別の不利益があるともいい難いように思われる」が、「情報の漏出や、情報が誤って用いられるおそれがないとは断言できないものであり、また、継続的に保有されるとした場合に将来どのように使われるか分からないことによる一般的な不安の存在や被侵害意識が惹起され、結果として、国民の行動を萎縮させる効果がないともいえないことなどからすれば、何の不利益もないとはいい難いのであって、みだりに使用されない自由に対する侵害があるといわざるを得ない」

「保護法益を制約することが、犯罪捜査のための必要性があるといった公共の福祉の観点から容認できるかとの観点から比較衡量して検討する必要があり、その趣旨に従って指掌紋規則等も解釈されるべきである」（「少なくとも、当該被疑者との関係でより具体的な必要性が示されることを要する」）

「指紋、DNA型及び被疑者写真をみだりに使用されない利益を、より射程の広いプライバシー権や情報コントロール権等の一部として位置づける理解をするかはともかく、当該利益自体が人格権を基礎に置いているものと解するものは可能であるから、・・・被疑者であった者は、訴訟において、人格権に基づく妨害排除請求として抹消を請求できるものと解するのが相当である」

# 3.【第3期】アーキテクチャ志向型の自己情報コントロール権

→1990年代後半に入ると、焦点を個々の情報のコントロールから、情報システムの構造やアーキテクチャに置く「構造論的転回（structural turn」が起こる（Neil M. Richards）。

①IoT、クラウド、AIといった情報通信技術の劇的発展により、ネットワークとの接続状態が「自然」となり、情報収集が常態化した上、かかる情報の保存・分析・連携も極めて容易になったこと、

②「データ＝資源」との思考の下、情報管理者にはより多くの情報を収集し、分析しようとする誘因が絶えず働くようになった。
→こうした現況の下では、“収集後”の個人情報の取扱いを明確にし、情報管理の構造・アーキテクチャを適切かつ堅牢なものにしない限り、濫用・漏洩のリスクが常在することになり、個人がある情報のあり方を自ら「決定」したとしても、それとは異なる用い方等がされる不安・リスクが継続することになる（収集時の自己決定の形骸化・無意味化）。
→また、同意の機会が形式的に増やされることで、かえって自己決定の質が低下するという「同意のパラドクス」が生じる（同意疲れ）。自己決定の実質化には、ユーザーインターフェース（UI）やアーキテクチャ（信託制度、AIエージェントetc.）の工夫が求められる。
→個人情報を取り扱うシステム構造・アーキテクチャの適切性・堅牢性が、「自己決定」の実現にとって決定的に重要になると認識。
※　カブキアン（Ann Cavoukian）が1990年代の半ばに提唱した「プライバシー・バイ・デザイン（PbD）」も、構造論的転回と軌を同一にするものと言える。

→第2期自己情報コントロール権論との連続性・関連性を維持しながら、システム構造やアーキテクチャの重要性を強調するもの。すなわち、①第2期の議論が強調した情報に対する自己決定的要素を引き続き重視しつつ、②かかる決定を実効化するシステム構造やアーキテクチャの重要性を前景化したところに特徴。

〇住基ネット判決（2008年：最判平成20年3月6日民集62巻3号665頁）
「個人の私生活上の自由の一つとして、何人も、個人に関する情報をみだりに第三者に開示又は公表されない自由を有する」（憲法13条）
＋構造審査（システム構造に着目した具体的危険性の審査）

## 【第4期】「適正な自己情報の取扱いを受ける権利」（音無和展など）

・第3期との共通点
・第3期との相違点
※個人情報保護法35条5項（「必要がなくなったとき」）、33条1項・2項（「当該本人が請求した方法」）

# Ⅱ．検討スコープと関連したコメント

1．公共空間における顔認識技術の利用は、同意ベースの規制にはなじまない（代替ルートをとることが困難。店舗型利用との相違・差分）

2．顔認識技術付きのカメラ撮影によって、特定個人を網羅的・継続的に監視することが可能となる（個人の行動の網羅的・継続的把握について、GPS捜査判決〔最大判平成29・3・15〕は、他の要素も加味してではあるが、「強制処分」と解している）。

※憲法上、自由が保障された諸活動（表現活動、移動の自由etc.）などに対する萎縮効果が非常に強い（通常の防犯カメラと異なる性質を有する）。このことは、自由かつ民主的な社会に対しても影響を与える（個人的法益＆社会的法益）。

3．公共空間をどのようなものとしてデザインすべきかについては、個別の同意ではなく、集合的同意（社会的コンセンサス）によって決せられるべきである。基本的には、法律による規律になじむ（適切な規律の下での利用が重要であり、それが権威主義国家における監視との差分となる）。

４．誰を登録しておくのか（登録基準）、登録・保存期間等は、スティグマ（烙印）との関係で、比例性に関する慎重な判断が必要である（ノンフィクション「逆転」判決〔最判平成6・2・8〕は、「新しく形成している社会生活の平穏を害されその更生を妨げられない利益」を認め、「時の経過論」を導入した。さらにDNA抹消命令判決は「具体的な必要性」を要求）。
→原則的な基準設定（公開）。例外については倫理審査委員会等による承諾？

５．登録情報にいかなる属性情報を紐づけるかについても検討が必要（政治的な犯罪などの登録の是非、精神疾患等との紐づけなど）。
→紐づけを禁止する事項を抽出する必要？

６．判決等の結果次第で、登録状況を変更しなければならない場合もある（仮に無罪となった場合には、抹消する必要があろう）。必要な情報更新をどのように行うのかも検討しなければならない（法務省や警察機関との定期的な情報連携のあり方が問題となるが、その場合には、センシティブ情報を扱うことになるために特に慎重な検討が必要である）。
→定期的な情報連携は協定？（法律が望ましいが…）

7. 不審者予測については、機械学習の精度の点で誤登録の問題が生じやすい（スティグマのリスク）。不審者登録については、アルゴリズムの適切性・公平性を担保することが重要となる（例えば、多数派と異なる動きをする障害者が「不審者」と登録されることはないか）。不審者登録・検知の実施も、安全性確保等が特に必要な一部公共空間においては許容されるが、そこには比例性が求められよう。

8. ガバメントアクセスについては明確な基準を設けるべきである。また、登録情報を共有する範囲（提供先）、共有する際の基準などについても事前に決定しておくべきである（駅の間での共有のあり方についての検討）。

9. 上記4～8については、透明性が求められる（8については、一回的なものではなく、透明性レポートのようなものを定期的に出すことも求められるのではないか）。

10. 上記4～8については、その比例性・適切性・公平性を担保するための監視統制システムが必要である（倫理審査委員会等の内部的統制機関／認証等機関／個人情報保護委員会）。

11. 公共空間（一部の大規模ショッピングモールを含む）における商用目的での顔認識技術の利用は、利用者の同意を必要とすると考えるべきである。ショッピングモール等の管理者に対し、同意のもとで顔情報を事前に提供・登録した者のみが、商用目的での顔認識技術の対象となるべきである（もっとも、商用目的での顔認識カメラ撮影に同意していない者も、公益目的での顔認識カメラでの撮影については受忍せざるをえない場合がある。同一のカメラを用いる場合にも、公共用と商用とで技術的に切り分ける必要がある）。

→公共空間における顔認識技術の利用は、安全性確保など公益に大きく資するところがあり、一定の条件下では許容されると考えられる（安易な監視社会論ではなく、比例性にかなっているか、適切なガバナンスがデザインされているか、といった法律論が必要）。