

プライバシーの権利を考える

山本龍彦

出典・凡例

本稿は、山本龍彦『プライバシーの権利を考える』（信山社、2017年）所収の諸論文のうち、現代のデータ倫理にとってとくに重要と思われる第1章、第2章、第3章、第6章、第12章の要約をまとめたものである。

外国語の翻訳については原則として著者の訳に従っており、原語を付すために()を用いた。とくに重要と思われる箇所には下線を施した。

1 プライバシーの権利（P. 3-21）

I はじめに

本稿は「常に変化する地形」とも喩えられるプライバシーの権利の変容について考察することを目的とする。

II プライバシーの権利の変容

プライバシー権論は、ウォーレンとブランダイスによる私生活秘匿のための権利（第1期）、ウェットな自己情報コントロール権（第2期）、システム・コントロールとしての権利（第3期）という展開を辿った。いわゆるイエロー・ジャーナリズム等による私生活への侵害に対する権利としてプライバシーの権利が提唱され、1960年代のアラン・ウェスティンとチャールズ・フリードの論文により第2期に移行した。この時期には、コンピュータ等の実用化や科学技術の発展といったプライバシーをめぐる状況の変化に応じ、プライバシーの権利の定式を変える必要があると提唱された。ウェスティンによればプライバシーの権利とは「自己に関する情報を、いつ、どのように、どの範囲で他者に伝達するかを自ら決定するという個人、集団または組織の要求」であり、フリードによれば「自己に関する情報のコントロール」である。こうしたウェットな自己情報コントロール権としてのプライバシー権論は、佐藤幸治によって日本にも広められた。1990年代後半になると、情報の連結可能性・検索可能性・解析可能性の飛躍的な向上や、個人のアイデンティティ形成におけるデータベースの基盤化を背景として、データベースや情報システムに対するコントロール権としてプライバシーを理解する立

場が提唱された。この立場はプライバシーという主観的利益を保護しつつも、構造やアーキテクチャ全体をコントロールするという側面が強調される（たとえば、適切な第三者機関が設置されているかといった組織法的審査）。これらのプライバシー権論のうち、第1期および第2期のものは日本の裁判所にも受容されたと考えられる。また、第3期のものと親和的な判例として住基ネット事件判決が挙げられる。

III 第3期プライバシー権論の課題と克服可能性

第3期のプライバシー権論には技術論的課題と権利論的課題がある。前者は、情報技術に関する専門知を有しない裁判官に構造審査をなすかという問題であるが、監査機関等の組織法的審査を行うことでその役割を果たすことが可能である。後者の課題には、2つのアプローチがある。一つは、プライバシーの「社会公共的なもの」を指摘するアプローチである。これは、情報システムの構築やその前提たる情報処理が社会全体に及ぼす影響を権利の「侵害」に参入することでプライバシー権の保護法益論および侵害論の突破口を見出すアプローチといえる。いま一つのアプローチは、プライバシー権を予防的ルールとして捉えるものである。これによれば、ミランダ・ルールのように、核心的な憲法価値を実効的に保護するために、あるいは将来生じうる核心的憲法価値の侵害を未然に防ぐために設定された政策的で戦略的なルールとしての「権利」としてプライバシー権を理解することができる。

IV 結語に代えて——多元的・文脈依存的プライバシー権論へ

プライバシー権論は前述のような変遷を見せたが、だからといって第2期以前に保護された利益が重要性を失うわけではなく、むしろプライバシーの多様性を示唆するものである。日本の憲法学においては「自己情報コントロール権」について一定の共通理解が形成されつつあることから、包摂的定義を前提に、多元的で文脈依存的なプライバシー権論を展開していくべきである。

2 プライバシー——核心はあるのか (PP. 23-46)

I はじめに

本稿は、プライバシーをもっぱら個人主義的観点から捉える見解を批判した上で、プライバシーの社会的な文脈を救済することを試みる。その目的は、第一にプライバシーに核心はあるのかという理論的難題に応答するという点にあり、第二に「自己情報コントロール権」説の再構成への足がかりを作る点にある。

II プライバシーの個人的な文脈

プライバシーは個人主義的な価値をいうのであって、共同体や社会はその敵であるという理解が、プライバシーに関する「一般的」で「支配的」な見方とされる。アメリカでは、プライバシーを「1人で放っておいてもらう権利」と定式化したウォーレンとブランダイスに影響を受けた不法行為法学者および裁判所がプライバシーを個人的権利 personal right として性格づけた。1960年代に情報技術を中心とする科学技術の進展を受けてプライバシーを「情報プライバシー」として再構成する見解が有力となった（アラン・ウェスティンやチャールズ・フリードなど）が、ここでも個人主義的傾向は維持された。こうした個人主義的傾向は、フリードの影響を受けた佐藤幸治が通説を形成した日本のプライバシー論にも受け継がれた。しかしこの傾向には、現代の高度情報化社会が提起する諸問題にうまく適応できないという課題がある。すなわち、①コンピュータによる情報処理に関心を示せていないという点、②本来的に保護すべき情報カテゴリーが狭いという点、③データベースにおける構造上の問題や抽象的な侵害を捉えきれない点、④データベース等の制度的・構造的な改革という救済手段に焦点を当てられていない点、などである。

III プライバシーの社会的な文脈

こうした課題を克服するためには——表現の自由における民主主義的価値と類比できるように——、プライバシーの社会的・客観的側面（＝「他者」）に目を向ける必要がある。その際、2つのアプローチが考えられる。一つは、忘却された「他者」の痕跡を過去のテキストに探すものであり、具体的にはハンナ・アーレントやウォーレンおよびブランダイス等の議論が参照される。アーレントによれば、プライバシー (privacy) は「なにものかを奪われている (deprived) 状態」を含意しており、生活や必要性から切り離された「自由な公的空間」において「政治＝活動」を行うための前提を成す生物としての必要性にもとづく空間・状態として位置づけられる。このように、プライバシーということばには、個人主義的理解とは異なる「他者」の存在が埋め込まれているといえる。また、アメリカにおいてプライバシー権論を展開し

たウォーレン・ブランドイスやウェスティンの議論においても、プライバシーが「民主主義」という価値に資する可能性を指摘していたことから、社会的側面を看取していたと読むことができる。プライバシーの社会的側面に着目するもう一方のアプローチは、現代の論者の議論を借りるものである。ここでは、3つの段階に分けて議論が紹介される。第一は、ロバート・ポストの議論である。ポストによれば、プライバシー（特に不法行為法上のそれ）は「単に共同体の要求に対して個人の利益を維持するものではなく、……個人と共同体の双方を構成する礼節さのルール (civility rules) を保障するものであり、プライバシー侵害の不法行為法は、共同体における「品位の限界 (limits of decency)」 (= 「礼節さのルール」) の維持や管理と深く関連している。第二の議論は、プリシラ・リーガンのものである。リーガンは、従来のプライバシー論は「個人に対するプライバシーの重要性を強調し過ぎて、プライバシーがもつより広範な社会的重要性を承認し損なってきた」と述べ、その社会的重要性の根拠を①共有価値 (common value)、②公共的価値 (public value)、③集合的価値 (collective value) の3つに求めた。第3の議論は、アニタ・アレン、ジェド・ルーベンフェルド、ポール・シュワルツらのものである。彼らの議論は、第2のものをそれぞれのかたちでさらに発展させたものとして位置づけられる。

IV 結語に代えて

以上のようなプライバシーの社会的側面に着目したアメリカの議論を踏まえると、日本におけるプライバシー権論はどのように映るか。日本においてはアメリカと異なりプライバシーについて「自己情報コントロール権」と捉える見解が通説化しているため、プライバシーの核心的価値は大きな問題とならない。むしろ、個別の問題状況や制約主体の性質に応じて、自己情報コントロール権の有する複数の価値——人格的価値、関係性構築に係わる価値、共同体構成的な価値、民主主義的価値、反全体主義的価値、等々——に着目すべきである。重要なのは、ある特定の文脈において、「自己情報コントロール権」が保障する多種多様な価値のうち、どれを（どれとどれを）考慮すべきかである。

3 データベース社会におけるプライバシーと個人情報保護 (PP. 47-64)

I はじめに

本稿の目的は、データベース社会を特徴づける新たな「プライバシーの問題」を明確化し、データベース社会によって生じるこうした「問題」に見合った違憲審査のあり方を提示する点にある。

II データベース問題と、その処方箋

比喩的には、伝統的なプライバシー問題が「激痛 (acute pain)」にかかわるものであるとすれば、データベースが提起する新しいプライバシー問題は「鈍痛 (dull pain)」にかかわる。前者は、たとえばイエロー・ジャーナリズムによる私生活上の秘密の公開・暴露や、親密圏における基本的人間関係への具体的・直接的阻害によって引き起こされる。他方、高度にネットワーク化されたデータベースにあっては、我々は自分の情報がどのように扱われるかを正確に知ることができず、こうした「不確実性」がもたらす実質的不安は、「鈍痛」として我々の行動に様々な影響を与えうる。

こうした「激痛」と「鈍痛」の違いは、従来の裁判例や学説において等閑視され、“すれ違い”を生んできたように思われる。

たとえば、裁判例においては個人情報の取得時に着目して合憲性を審査してきた。指紋押捺制度の合憲性を争った平成7年最高裁判決（最判平7・12・15刑集49巻10号842頁）は違憲審査のポイントをもっぱら指紋押捺の瞬間に置いていた。しかし、指紋押捺制度の現代的問題の核心は、指紋押捺によって生じる羞恥心や屈辱感にあるというよりも、その情報がデジタル化され、データベースに組み込まれた後の利用のされ方や、利用状況の不確実性に基づく実質的不安にある。また、録画機能付きテレビカメラ監視の合憲性を争った昭和63年の山谷テレビカメラ監視事件判決（東京高判昭63・4・1東高刑時報39巻1～4号8頁）や、Nシステムの合憲性を扱った平成13年東京地裁判決（東京地判平13・2・6判時1748号144頁）においても、同様の“すれ違い”が生じている。これらの裁判例はいずれも「データベース」が問題であったにもかかわらず、審査のポイントをもっぱら情報の取得場面に置いてきた、といえる（取得時中心主義）。

さらに、上記のような“すれ違い”は学説においても見られる。日本憲法学のプライバシー権論において通説的立場である自己情報コントロール権説は、フリードの議論を前提としているが、彼の議論は人間関係の形成にとって重要な情報をコントロールすることが核心とされ、センシティブ情報の盗取などが問題とされた。これを引き継いだ日本の自己情報コントロール権

説は、データベース問題ないし「鈍痛」に対応する具体的な憲法ドクトリンを提示しきれていない。収集された情報が、外延情報であるとの理由で緩やかな審査に服するとすれば、どう保存され、どのように取り扱われるかがわからないという問題の核心を突くことはできず、データベース問題とは”すれ違った”審査となる可能性が高い。

Ⅲ 住基ネット判決と構造審査——構造論的転回？

こうした裁判例や学説の状況のなかで、平成20年の住基ネット合憲判決（最判平20・3・6民集62巻3号665頁）は、データベース問題を意識するような審査手法を導入した。本判決は、情報の個別具体的な処理に着目した緩やかな目的・手段審査を行うのではなく、住基ネットのシステム構造全体に目を向け、その堅牢性や健全性を審査した。この判決は、情報組み込みという未だ「実害」ないし「具体的害悪」が発生していない段階で、権利が侵害されうるとした点が注目される。ただし、現在の高度情報技術を踏まえれば、少なくともネットワーク型データベースは構築・運用それ自体が自己情報コントロール権への「侵害」になりうるものと解し、構造審査はむしろ「正当化」の場面で行うべきであると思われる。

また、情報技術の専門家ではない裁判所が構造審査をなしうるかという問題も存在する。しかし、政策決定者ないし立法者が、データベース問題を踏まえた構造のデザインを行うとは限らず、また警察保有のデータベースのように個人情報保護法の及ばないデータベースも存在している以上、裁判所が審査を行う必要がある。さらに、規範の明確性や組織・手続き法上の予防措置の有無といった構造については、裁判所も判断能力があるといえる。ただし、直接的・常態的な審査は、個別的情報処理を捕捉することは外部からは難しい以上、監査機関が行うのがふさわしい。

さらに、プライバシー権論の構造論的転回については、個人の人格的生存に対する「具体的害悪」が生じる前の「鈍痛」が憲法上の権利の侵害として認められるかという問題が提起されている。これに対してはまず、データベースへの組み込みによって受ける「鈍痛」は、たとえば靖国神社参拝事件等で宗教的少数派が受けるそれよりも実質的なものだといえる。技術発展によって無数の「可能性の束」がもたらされ、それが個人の全人格的把握や、個人の脱構築不可能性まで帰結するような「可能性の質」であるとすれば、個人の自律的生が影響を受ける可能性があるため、不確実な構造のもたらす「不安」は、権利侵害と叫ぶほどの実態を有している。また、データベースへの情報組み込みやそのための情報取得が個人の自律的生に与える影響が間接的で微視的だとしても、データベースが作り出す「警戒的」な「雰囲気」が民主主義に与える否定的な影響は小さくない。プライバシーの権利には、「反全体主義」的な権利としての側面や、政治的討議空間の「前提条件」としての側面という社会公共的利益があるといえるからである。

IV おわりに

データベース問題に特有の「鈍痛」を「侵害」として捉えることは、自己情報コントロール権という考え方それ自体の放棄は導かないが、多様な価値ないし利益と結びついており、状況や文脈によってその背景的価値の組み合わせを変えるものであるから、可能なかぎり包括的に理解すべきである。この点で、「自己に関する情報を、いつ、どのように、いかなる範囲で他者に開示するのかを自ら決定する」というウェスティンの定義が有用である。

さらに重要なのは、侵害概念である。本稿の検討からすれば、国家によるデータベース構築を前提とした情報取得行為を問題にする場合には、その「侵害」を、取得後に起こりうる無数の侵害可能性を織り込む形で、またその可能性によって生じる実質的不安や民主主義への否定的影響を織り込む形で査定し、かかる侵害形式に見合った審査——すなわち構造審査——を用いるべきである。もっとも、侵害の度合いや構造審査の「場所」は、状況や文脈によって異なりうる。たとえば、①既存データベースの「ネットワーク化」が問題になる場合、まずネットワークシステムそのものの合憲性が審査され、厳格な構造審査が正当化の段階で行われることになる。その上で、別途、このシステムによって行政機関間で新たに行われることになった情報のやりとりが、情報のセンシティブ性に応じた審査基準によって審査されることとなる。次に、②新規のデータベース化が問題となる場合には、構造審査はやはり正当化の場面で行われるべきであるが、予定されるネットワークの規模と情報のセンシティブによって、かかる審査の厳格度が変わってくる。最後に、③データベース化を前提としない個別的信息収集が問題になる場合には、構造審査が侵害の度合いを査定するものとして行われるべきと考える。

6 予測的ポリシングと憲法——警察によるビッグデータ 利用とデータマイニング (PP. 99-121)

I はじめに

本稿は、ビッグデータ革命により影響を受け始めているとされる警察の法執行ないし犯罪予防の領域に焦点を当て、そこでのビッグデータ利用、とりわけ、これを前提としたデータマイニングおよびその適用——いわゆる予測的ポリシング (predictive policing)——の（憲）法的問題を考察することを目的とする。

II 何が問題なのか？

予測的ポリシングの実例として、「エリア」に着目した予測と「個人」に着目した予測が挙げられる。「エリア」に着目した予測とは、たとえば、過去の膨大な犯罪データから一定のパターンを抽出・発見し、犯罪が発生しやすい場所と時間 (hot spots) に警察資源を効率的に配分することで、予算削減および効果的なポリシングを実現するものである。「個人」に着目した予測とは、たとえば、シカゴ警察は「便宜告知プログラム (Custom Notification Program)」を導入し、暴行犯の実行者と犠牲者を予測するアルゴリズムをもとに捜査活動を行っていると言われる。

本稿は「ビッグデータ」という言葉を「小規模ではなしえないことを大きな規模で実行し、新たな知の抽出や価値の創出によって、市場、組織、さらには市民と政府との関係などを変えるデータ」というような、技術的観点に社会的観点を加味した定義で用いる。また、「データマイニング」は「データから知識を掘り当てること」を意味するが、「データのなかに隠れたパターンと微妙な関係性を明らかにし、将来の結果予測を可能にする規則性を推論するために、統計学的分析やモデリングのようなデータベース技術と技巧を適用すること」といった定義で用いる。

上記の定義から明らかなように、データマイニングそれ自体は個人の権利利益と直接関係するわけではないが、そこで抽出・発見されたパターン等が、個人識別情報を含むデータベースに「適用」される段階においてデータマイニングと特定個人の関係が結ばれる。こうした「適用」によって特定個人の傾向や属性が割り出される。警察が具体的に介入するのは「適用」の後であり、介入が法的問題となることは疑い得ない。だが、「適用」段階においても、法的検討の余地があるのではないか。

第1に、プライバシーの権利との関係において問題となる。「宴のあと」事件判決に従い、私生活ないし私事を密かに覗き見る行為がプライバシー権の侵害を構成するとすれば、データマイニング結果の「適用」は、既に保有している断片的個人情報からは明らかにならなかった

情報主体の私事を新たに知ろうとする行為——データ媒介的覗き見——として、プライバシー権を侵害するものと考えられることができる。

第2に、憲法13条が謳う個人の尊重原理ないし個人の尊厳原理との関係で問題となる。データマイニング結果を用いた個人の傾向把握ないし行動予測は、本人が自らの自由意思に基づいて選択し、行動する前にその個人を統計的に「判断」しており、個人の自律的・主体的な判断・選択や実際の努力を捨象し、当該個人をいかなる者かを決めつけていることから、自律的な個人としての主体性を否定するものといえる。また、こうした予測は、行動の前段階である内心領域の動向を覗き見る行為ともいえることから、憲法19条によって保障される思想・良心の自由と抵触しうる。

こうした侵害について裁判所の統制が及ぶのはデータセットの「適用」後の警察官による「介入」の段階であるが、実際にはデータマイニングによる不可視的な標的化によっても個人の行動が萎縮しうる。このような観点からすれば、「適用」の段階に法的問題を見出し、適切に統制していく必要性は高いと思われる。

III どのように統制すべきか？

では、どのような統制が考えられるか。ひとつは、データセットの「適用」について個別に同意を得るアプローチである。しかし、こうした同意を得るためには警察が情報主体に対して事前に告知する必要があるところ、これでは捜査上の秘密等が漏洩し、公共の安全と秩序の維持に重大な支障を来すおそれがある。また、ビッグデータ収集においては対象となる主体が膨大であり、全員について個別的に同意を得ることは現実的に困難である。

IV 結語に代えて

統制のもうひとつの方法は、法律の制定による集合的同意の方法である。データセットの「適用」が憲法上の価値と抵触する可能性があることからすれば、少なくとも法律という形式をとる必要がある（いわゆる法律の留保論）。また、情報主体本人によるコントロールに代わって適切な運用を担保するための仕組み・構造を組み込む必要がある。これには、情報の外部流出等に対して厳罰を科すことや、関係者へのリテラシー教育、監視機関の専門性の高度化といった内容が含まれる。監視機関の充実、透明性確保という観点からも重要である。

12 ビッグデータ社会とプロファイリング (PP. 257-277)

I はじめに

EU が GDPR においてプロファイリングの定義を示したように、プロファイリングは個人情報保護にとって喫緊の課題となりつつある。本論文は、EU のこうした取り組みがもつ現代的意義を明らかにし、未だ情報漏洩や第三者提供と言った「古典的論点」に執着する日本の個人情報・プライバシー保護法制の課題を明らかにすることを目的とする。

II 現代的なプロファイリングとは

現代的なプロファイリングには、①データ量の大きさ、②手続きの自動性、③科学的信憑性、④意外性（予測困難性）、⑤項目の広範性・細目性といった特徴がある。こうしたプロファイリングは、公的部門ではとくに警察による犯罪予防や航空機の搭乗拒否リストの作成において用いられ、民間部門ではターゲティング広告や保険、雇用、教育等において用いられる。さらに、SNS やポータルサイトにおけるニュースフィードの生成、選挙における利用が問題となっている。

現代的なプロファイリングには、次のような問題点があると考えられる：①プライバシー権の侵害、②内心の自由の侵害、③選挙権の侵害／選挙の公正の揺らぎ／民主主義の弱体化、④平等原則および個人の尊重原理との抵触、である。

III GDPR におけるプロファイリング規制と権利

EU は、これらのリスクに早くから気づき、GDPR においてプロファイリングに関する特別の規定を設けるに至った。GDPR は、プロファイリングを「自然人に関する特定の個人的側面を評価するために、特に、当該自然人の職務遂行能力、経済状況、健康、個人的選好、関心、信頼性、行動、位置もしくは動向を分析または予測するために、個人データを用いて行うあらゆる形式の自動化された個人データ処理」と定義したうえで、プロファイリングに対して異議を述べる権利を認めた。また GDPR はさらにすすんで、プロファイリングのような自動処理のみに基づいて、本人に法的効果を与える、あるいはそれと同程度本人に重要な影響を与える決定を下されない権利を主体に認めた。このように、GDPR は、人生の重要場面において、個人の能力的側面等がアルゴリズムの確率的判断のみによって自動的に評価・決定されるという社会をディストピアとして峻拒し、これを抑止しようと試みているといえる。いかなるデータ

処理がプロファイリングにあたるか等については、今後欧州データ保護ボード (European Data Protection Board) の指針等によって具体化されていくと考えられる。

IV 結語に代えて

人工知能の急速な発達には、確率的判断によって排除される集団を生むなど、近代立憲主義の基底的価値を揺るがしかねない問題を提起しうる。EU やアメリカはこうした問題に真剣に取り組み始めている。しかし、日本では、改正個人情報保護法がプロファイリングを問題にすることはなく、情報漏洩や第三者提供といった点に議論の焦点が置かれている。高度情報化社会において本質的に問題なのは人々が知らぬ間に個人的側面を曝かれるというプロファイリングである以上、第三者提供等への対策という外堀ではなく、プロファイリング対策という本丸を守る必要がある。そこでは、①プロファイリングそれ自体の規制と、プロファイリング結果の利用規制とのバランス、また、②プロファイリングの公正さとその正確性とのバランスに関する議論を深化させる必要があるだろう。

(松本 有平)