イントロダクション：プライバシーの新たな視点

リネット・テイラー、ルチアーノ・フロリディ、バート・ファン・デル・スルート

出典：

Linnet Taylor, Luciano Floridi, and Bart van der Sloot, “Introduction: A New Perspective on Privacy,” in Linnet Taylor, Luciano Floridi, and Bart van der Sloot eds. *Group Privacy New Challenges of Data Technologies*, 2017, pp. 1-12.

キーワード：

・集団 Collectives
・グループ・プライバシー Group Privacy
・プライバシー権 Right to Privacy
・関係的プライバシー Relational Privacy
・ネットワーク効果 Network effects
・一般データ保護規定 GDPR
・プロファイリング Profiling
・アルゴリズム Algorithms

要旨

本稿は、論文集『グループ・プライバシー　データ技術の新たな挑戦』の第 1 章にあたるイントロダクションの要約である。著者は論文集の共編者 3 名で、テイラーとファン・デル・スルートはオランダのティルブルグ大学所属の法学者、フロリディはオックスフォードインターネット研究所 Oxford Internet Institute 所属の情報哲学者、情報倫理学者である。

著者らによれば、近年登場した新たなデータ分析技術は集団を主な分析対象としており、したがって、個人に焦点を当てた既存の法的・倫理的パラダイムは修正・拡張されねばならないという。本論文集では、こうした修正の試みとして、グループ・プライバシーを「彼らのプライバシーtheir privacy」ではなく「グループのプライバシーits privacy」として捉える観点が提案される[1]。イントロダクションでは、グループ・プライバシーに関連する哲学的・倫理的・法的事項が概観され、論文集の課題が設定される。

---

[1] 論文集の第 5 章にあたるフロリディの論考ではこの主張がより詳細に展開されている。内容については以下の紹介を参照されたい(http://www.ethics.bun.kyoto-u.ac.jp/wp/wp-content/uploads/2020/12/14716352b4d14ac0d44f044f9d4b0d5f.pdf)。

1. 本書の計画と端緒

本書は、新たに登場したデータ分析技術に対し、グループ・プライバシー〔についての考察〕が不十分である、という認識から始まった分野横断的な議論の産物である。ビッグデータ時代にあって、データ分析技術は個人ではなく集団を対象としており、そこで対象となる集団もますますグローバルなものになってきている。

したがって、個人に焦点を当てたプライバシー論は、現実の技術的状況に注意を払うため、修正・拡張される必要がある。このことを議論の出発点として、我々は、現在のプライバシー理解、データ保護理解にかんする新たな問題を提起する。この計画のひとつの出発点となったのは、グループ・プライバシーが個人のプライバシー、あるいは個人の利益の集合としてしか理解されてこなかったことである。我々の中心的問いは、「彼らのプライバシー」から「グループのプライバシー」へと移行することは可能なのか、できるとすればいかにしてか、ということである。

この問いに答えるためには、はじめに、「グループ」というときになにが意味されているか理解していなければならない。本書の寄稿者たちは、多様で様々なグルーピング――政治的集団、アルゴリズムによるグルーピング、民族的グルーピングなど――を提示している。こうしたコンセンサスの欠如は、ひとつには、本書の学際的性格からきている。というのも、法学者はグループについて哲学者とは違った仕方で考えるし、哲学者もまた社会科学者とは違った仕方で考えるからである。既存のプライバシー論がビッグデータを前にして不適切であることを考えれば、分野横断的な議論こそが現行のプライバシー定義の限界を超える助けとなるだろう。こうした探求のため、本書は学際的な視点を提供する。

本書には、法哲学、情報倫理学、人権、コンピューター科学、社会学、地理学の分野が含まれる。使用されるケーススタディには、アフリカの衛星データ、ヒトゲノム、ソーシャルネットワークが含まれる。これらの共通点は、いずれも一世紀前には存在しなかったデータタイプ――位置情報や携帯電話の記録――を扱い、新たな分析の方法――クラウドコンピューティングや機械学習――を用いているということである。

2. 新たなデータ技術とデータ実践

本書が焦点を当てる新たなデータ分析技術は、高所得国で利用可能なツール、アプリケーションから、低所得国でも使用される技術まで様々である。現在、世界中で、デジタル化(digitization)とデータ化(datafication)がデータ分析を進歩させている。

ビッグデータが提供する「神の目」は、デジタル技術から得られる人々の行動データによって生じている。この種のデータは、はじめからデジタル形式であり、しばしばユーザーが気づかないまま記録される。携帯電話やインターネットのようなデジタルコミュニケーション技術の使用、クレジットカードの取引、監視カメラなど、様々な仕方でデータは生み出される。また、これらのデータを伝達、合体させるシステムによっても新たなデータセット

が作り出される。ほかに注目に値するのは、地理情報の登場である。地理情報、とりわけスマートフォンから得られる活動データは、人々の移動と所在のデータを視覚化・モニタリングするまったく新たな方法をもたらし、様々な領域で重要視されている。

「神の目」の利用法は多種多様であり、ケア――人権保護や医療――にもコントロール――安全保障やテロ対策――にも用いられる。ビッグデータが様々なセクターで大きな関心を集めている最大の理由は、それがプロファイリングやナッジなどの仕方で、人々の行動を変化させることにある。新たなデータソースは、分析や理解のためだけでなく、人々に影響をおよぼすための実践の道具としても考えられているのである。

3. 個人を越えて

ビッグデータ分析においては、個人はもはや中心的な分析対象ではない。データは特定の個人や小さなグループではなく、巨大で漠然としたグループを対象として収集される。データは、グループのプロファイルに基づいて分析され、分析結果はしばしば政策といった大きな規模で用いられる。過去長い間、技術とコストの問題から、処理できるデータ量には限界があり、結果として、データ分析の影響を受けるのは個人あるいは小さなグループに限られていた。このため、法的・倫理的規範も個人に焦点を合わせ発展してきた。しかし、ビッグデータ分析の登場が大きな変化をもたらした。ビッグデータ分析は、ここ数十年の間に発展してきた社会的、法的、倫理的実践と理論の土台そのものに問題を投げかけているのである。

本書の寄稿者たちが指摘しているように、現行のデータ処理ガイドラインは特定可能な個人についての情報に注目している。たとえば、OECD（経済協力開発機構）のガイドラインは、個人データ(personal data)を、特定可能な個人にかんする情報と定義している。特定可能な個人の情報への注目は、伝統的なデータ処理に対してはいまだ有効であるが、カテゴリーあるいはグループについての情報への注目によって補完される必要がある。

現在支配的な社会的、法的、倫理的パラダイムは主に個人の利益と危害に焦点を当てており、結果として、プライバシーあるいはデータ保護は個人の利益の問題だと考えられている。しかし、ビッグデータ時代にあっては、政策などの様々な決定はプロファイルやパターンに基づいてなされており、良かれ悪しかれグループに影響する。それゆえ、個人の利益だけでなく、グループの利益にも注目しなければならないのだ。

また、現行のパラダイムは、個人が個人のデータをコントロールするという考えに焦点を当てている。たとえば、「インフォームド・コンセント」の概念によれば、データ主体の個人の同意がない限りデータを収集、分析、使用してはならないと説明される。問題は、ビッグデータ時代においても個人のコントロールへの注目が妥当であるのかということである。というのも、個人が自身にかんするすべてのデータ収集・分析を認識し、評価することは急速に難しくなってきているからである。

以上のように、個人、個人データ、個人の利益、そしてインフォームド・コンセントへの注目は狭すぎるのであり、より広いデータ使用を考慮に入れたプライバシー解釈によって

補完されねばならない。本書が試みるのは、グループ・プライバシーという考えを概念化するための基礎を定め、議論の次元を〔グループにまで〕高めることである。

4. グループ・プライバシーを概念化する

グループ・プライバシーについて論じる際の大きな難点の一つは、グループの本性を説明することである。一般的な考えによれば、はじめにグループを特定して、そのあとでグループの権利について論じることが可能になるとされる。これは、「事物」をはじめに特定せねばならず、それによって「性質」を特定できる、という暗黙の想定である。このアプローチは一般的には誤りではないが、グループの事例では、不必要な困難を生み出してしまうため役に立たない。グループは普通、多様で流動的である。たとえば、あるバスにのっている人々というグループは、バス停ごとに変化を繰り返す。このようなグループの不確実性から、真に存在するのは個人だけであり、それゆえグループ・プライバシーはグループを構成する個人のプライバシーの総計にすぎない、と結論されるかもしれない。この推論の問題点は、グループは「所与」のものではないということである。民族集団のように、所与のものとみえるグループの場合でさえ、そのグループに誰が属するかは特定の性質の選択によって決まる。それゆえ、属性が最初にあって、それにしたがってグループが構成されるのだと考えるほうがはるかに理に適っている。また、プライバシーの場合には、なんらかの性質――たとえば「ムスリム」――を選択してグループを作り出すデジタル技術が、そのグループのプライバシーを脅かすということがありうる。デジタル技術は、集団化と類型化を通じてグループを決定しているのである。

たとえば「十代と退職した人々」のように、いくつかの属性はきわめて直観的に思えるので、我々は、我々がグループを作り出しているのではなく、単に世界のありようを記述しているだけだ、という印象を受けてしまう。しかし、グループ・プライバシーの場合、グループを作り出す技術と独立にグループが存在して、彼らにプライバシー侵害が起きるのだ、と考えるのは誤りである。アルゴリズムやビッグデータなどのデジタル技術は、情報管理の実践や政策と同じく、特定の目的にしたがって、特定の性質を選択することによってグループを設計している。このことは、グループがなぜ動的であるのかを説明するだろう――目的が変われば、関連する性質の組み合わせが変わり、異なる個人の組み合わせが得られるのである。つまり、グルーピングの活動が先にあって、その結果としてグループが存在するのであって、その逆ではないのである。このアプローチに基づけば、グループのプライバシーを尊重しない目的に基づいたプロファイリングは、そのプロファイリングが設計するグループのプライバシーをすでに侵害している、と説明することができる。

存在論についての問題に戻ると、本書において、読者は2種類の存在論に出会うだろう。一方は、個人に基礎を置いた、主体基底的アプローチを支持する。この場合は、グループ・プライバシーは「彼らの」プライバシーとして現れる傾向にある。この考えによれば、グループ・プライバシーが存在するとすれば、それはグループの構成員のプライバシーの集合と

して分析される。他方の存在論は性質に基礎を置いた、述語基底的アプローチを支持する。この考えによれば、グループ・プライバシーは、「グループの」プライバシーとして考えられるだろう。つまり、グループ・プライバシーは、単なる構成員のプライバシーの集合を超えた、創発的な性質として分析されるのである。

5. 法学分野におけるグループ・プライバシーの取り組み

法学の文脈におけるグループの位置づけは複雑である。グループの権利が法的枠組みそのもの、あるいは少なくとも人権の枠組みの起源だと論じられることもある。一般に認められた最初の基本的権利は宗教の自由であったが、これは宗教的マイノリティ集団に認められた権利であった。

同様に、第二次大戦後、国際法において人権がはじめて成文化されたときも、焦点が当てられたのはグループであった。世界人権宣言に代表されるこれらの文書は、立法者が制限することのできない最小限の自由を定めたものであるが、個人のみならず、グループや法人もその対象であった。

にもかかわらず、次第に、ほとんどの人権の枠組みで、焦点はグループから個人へと移っていった。とりわけ顕著なのは、欧州人権条約である。欧州人権裁判所は、2002 年までの長きにわたり、法人はプライバシー権の侵害を訴えられないとしていた。それは、プライバシーは本質的に個人的価値と結びつくものであり、プライバシー権の侵害を訴えられるのは自然人だけだと考えられたからだった。

それでも、マイノリティの権利、未来世代の権利などの観念の発展は存在した。こうしたグループの権利は、第三世代の権利とよばれ、古典的な市民的自由、政治的自由のような個人的権利の射程を超えたものである。

最後に、プライバシー論の文献では、ときおりグループ・プライバシーについて論じられた。いわゆる「関係的プライバシー」や「家族のプライバシー」は、しばしばグループのプライバシー権であるとみなされてきた。しかし、この場合でも、個別の自然人に対して関係に参与する権利や家族の絆を深める権利が認められているのであって、グループや家族に権利が与えられるのではない。また、ある個人のプライバシーの喪失が他者のプライバシーに対しても影響をおよぼしうるという、いわゆる「ネットワーク効果」も注目を集めてきた。たとえば、遺伝性疾患を抱える人の遺伝子データが流出してしまった場合、その人の家族にまでその被害が波及しかねないという例が挙げられる。

プライバシーは、常々人格権と結びつけられてきた。おそらく、この 2 つの権利の間にはじめて明確な区別を引いたのは、スティグ・ストレムホルムであろう[2]。ストレムホルムによれば、プライバシー権がもっぱらアメリカの概念であるのに対して、人格権は、ドイツやフランスなどの国々で長い歴史を持つ、ヨーロッパの鍵概念である。2 つの概念の間の重要

[2] Stig Strömholm(1967) ‘Rights of privacy and rights of the personality: a comparative survey.’

な差異は、プライバシー権が放っておかれる権利、つまり消極的権利と解されるのに対して、人格権は、自分自身を公的文脈で表現し、アイデンティティと人格を発展させる権利をも含んでいるということにある。欧州人権裁判所は、欧州人権宣言 8 条を消極的なプライバシー権ではなく人格権として解釈するようになってきており、結果として、プライバシー権の適用範囲が大きく拡大した。

欧州人権裁判所の判断は、アイデンティティと個人の特定(identification)を、文脈的で社会に埋め込まれたものと扱い、結果として、特定の社会的、経済的、政治的グルーピングの中で表現されるものとして扱っている。しかし、新たなデータ技術は、個人ではなく、なんらかの性質によって集団化されたグループに注目している。このような状況で、人々がいかに個人の特定を主張しうるか、あるいはそれに抵抗しうるかはあきらかでない。データ分析がアルゴリズムによって自動化され、正確になればなるほど、プロファイリングという名のグルーピングも正確になっていく。アルゴリズム社会が発展する中、データの悪用や濫用を防ぐためには、グループ・プライバシーに注目する必要があるだろう。

正確なデータがもたらすこうした問題は、コミュニケーション技術にかんする予測不可能性と不確実性によって歯止めをかけられている。たとえば、低所得国では、一つの携帯電話を複数人が利用することがあり、単一のデータ分析プロファイルが幾人もの人の活動を反映してしまうことになる。

このような実践は、正確なプロファイリングに依拠する干渉を回避する可能性を持っているが、一方で、プロファイリングが貸し付け信用のような重大な判断を決定する場合には、人々に悪い影響をおよぼすこともありうる。いずれにせよ明らかなのは、個人のアイデンティティとグループのアイデンティティの間には、哲学的にも実践的にも、複雑かつ高度に文脈的な関係が存するということである。

6. 結論：「彼らのプライバシー」から「グループのプライバシー」へ

本書は、グループ・プライバシーの観念を様々な方向にたぐりよせようとする対話であり、問題に対する最終的解答を意図したものではない。

デジタル技術に対応して、我々は、多くの社会的・倫理的問題に関する見解をアップグレードしてきた。我々は物理的プライバシーから情報的プライバシーへと関心を拡張させてきたが、更に、プライバシーの主体についても考えを拡張しなければならないだろう。グループ・プライバシーの十全な理解は、我々の時代の難問に倫理的・法的に取り組むために必須である。本書がこうした概念的仕事に貢献してくれることを祈る。

（鈴木　英仁）