発展する科学技術と憲法学

東京理科大学　教養教育研究院　野田キャンパス教養部　講師　田中（たなか）　美里（みさと）

はじめに

私たちの社会は，いまや，高度に発展した情報技術を抜きにしては成り立たない．筆者自身にとっても，Amazon などのショッピングサイトや，Facebook などの SNS の利用は，もはや生活の一部となっている．

今日の情報技術において，これもまた欠かせない存在となっているのが AI の存在であろう．AI とは，人間の知的営みをコンピュータに行わせる技術だが，本稿ではとくに，ある情報を基にして他の情報を推測するという活動を人間に代わって行うものに着目する．たとえば前述の Amazon を例にとってみると，筆者が日々好んで購入している物や閲覧している物の情報から，次に筆者が購入する可能性の高いものを AI が予測し，「おすすめ」が示される．SNS でも同様で，Facebook を開くと多くの広告が表示されるが，この広告のパーソナライズも AI による仕事である．

インターネットという大海の中でいちいち時間や労力をかけて探し出さなくても，気に入りそうな情報を見せてくれる機能はたしかに便利である．しかし，AI の利活用について懸念される点もあり，便利だからといってどこまでも AI の利用を拡大し続ければ良いということにもならないだろう．

他方でまた，懸念されることがあるからといって，AI の開発を一切止めよということも，極端だろう．たとえば，車には殺傷能力があるからといって，私たちは車のある便利な生活を捨てなかった．それは，交通ルールを整備するなどの方法によって，生命や安全を守るということと車のある便利な暮らしの双方を実現できると考えたからであろう．先端科学技術でも同様のことを考える必要があるように思われる．

以下では，まず，AI の利活用によって，どのような権利や価値が傷つけられる危険性があるのかを論じ，その後，筆者の専門である憲法学の観点から，問題解決の際の課題を見ることとしたい．

プライバシー侵害の危険

AI の活動に欠かせないのが，大量の情報である．ある人物に関する情報を大量に収集し，それらの情報を相互に関連付けて解析することで，AI は，その人が次にとる可能性の高い行動を予測する．この情報の収集・利用において，プライバシー侵害の危険がある．

プライバシー侵害というと，私たちが，誰の目にも触れないようにひた隠しにしている情報が AI に暴露されているのかと思われるかもしれないが，そうではない．AI が収集し，解析に用いている情報は，たとえば，私たちが SNS アカウントに入力している情報であったり，どこかのサイトに自分で書き込んだコメントであったり，何かのサイトや動画を閲覧した事実であったりする．これらの情報は，私たちがひた隠しにしているものかといえばそうではない．どちらかというと，自分から情報を提供しているという方が正しいかもしれない．この状況のどこの部分で，プライバシー侵害は生じているのだろうか．

憲法学においても，少し前までは，「プライバシー」とは，プライベートな事柄（たとえば，恋人同士の間でのささやきなど）を，本人の同意なく世間に公開されてしまわない利益を意味するものと理解されていた．しかし，今日では，私たちが秘密にしている事柄が暴かれてしまう時にプライバシー侵害が生じると考えるだけでなく，氏名や住所など，日常生活の中で他人に頻繁に公開している情報であっても（Amazon で購入する際には住所等の情報を渡す必要がある），その情報が，もともと聞いていた目的と異なる目的に使用されたり，知らない相手に渡ってしまったりすることがあれば，プライバシー侵害が生じると考えられている．このような考え方を憲法学では，「自己情報コントロール権」としてのプライバシーと呼んでいる．

私たちは，自分に関わる情報（自己情報）を一切明かさずに生きているわけではなく，社会生活の中で，自己情報を与えたり与えなかったりしている．たとえば，この人にはこの情報を知られてもよい，知っていてほしいと思う，信頼できる相手方（恋人や親友など）

に対しては，あえて秘密を共有することもある．一方，この人とはそこまで深い間柄ではないと思う人（電車で隣に座っただけの人など）に対しては，自己情報を多くは開示しないように気をつける．このように，自己情報の開示・不開示には，人と人との間の関係性の深さを調整する機能があり，だからこそ，私たちは，誰かが一生懸命に秘密にしていることを，無理矢理に暴こうとはしないのだと考えられる（誰かが何かを秘密にしているということは，その人にとって，私は，その秘密を共有したいと思うような間柄ではないことを意味するから，それを無視して，その秘密だけを奪取することは，その人の人間関係のあり方を否定することになる）．

「自己情報コントロール権」は，自己情報の開示・不開示が，上記のような機能を持っていることに着目し，この機能が健全に維持されていることを「プライバシー」として考えるものである．この考え方からは，いま問題になっている情報が，仮にひた隠しにされているものではないとしても，本人の同意なくして，その人に関わる情報を取得・利用することは，プライバシーを侵害することとなる．

さて，オンラインサイトを利用する際，そのサイトがどのような情報を，どのような目的のために取得・利用するかは，利用規約等の形で私たちに提示され，私たちは，それに対して同意を与えている．それでは，問題はどこにあるかというと，これが「一応の」同意であって，真の同意とは言いがたいことである．利用規約は長文で書かれ，現実的にはとても精読できるものではないし，サービスの提供と引き換えに同意を求められるものであるために，サービスを利用したければ，利用規約の中身に不満があろうとも，同意せざるを得ない．このような状況では，私たちは，誰に対して，自分のどのような情報を手渡すべきか，吟味できているとは言えず，自己情報に対するコントロールが奪われている状態にあるのである．

このように，AI による解析の対象となる情報の収集・利用について，プライバシー侵害の危険がある．

自律的な決定の妨げとなる危険性

次に，AI が情報を解析し，私たちに何かの情報を提示するときのことを考えてみよう．この段階については，AI のプロファイリングによって，私たちの自律的な決定が妨げられている危険性を指摘することができる．この自律的な決定が妨げられていることの影響は，私たち個人の日常生活における判断と，社会全体での民主的な判断との両方に及ぶ．順に見ていこう．

今日の情報技術の下では，AI によって非常に高い精度でのプロファイリングが可能になっている．たとえば，ある人がどのようなサイト，どのような商品のページを閲覧したかということはもちろん，そのページを眺めていた時間や，どのくらいの速さでスクロールをし，どこでその手を止めたかなどの情報を，追跡しながら収集・解析することで，学生かどうか，どのような性的指向を持っているのか，妊娠した女性なのかどうかなど，ある人の個人像を浮かび上がらせるのである．そしてここで現れてきた人物像に従って，次に私たちが取るであろう行動が予測され，それに沿った行動をとるよう「おすすめ」される．

これは，個人の不快感にとどまる問題ではない．たとえば，ある人がどのようなサイトを見ていたのか，どの人のどの投稿を長く見つめていたのか，何に「いいね」をしていたかによって，私たちの思想が推測され，それが就職活動等の場面で判断材料に含められるという未来も十分予測される（すでにいくつかの企業が AI による判断を人事に部分的に用いている）．

次に，プロファイリングが民主的な判断に影響を及ぼしたケースとして，ケンブリッジアナリティカ事件を紹介したい．この事件は，ケンブリッジアナリティカ社が，Facebook を通して集めた個人情報から個人の性格分析を行い，この情報を用いてマイクロターゲティングしながら，契約している政治家に有利な広告を「狙い撃ち」して流していたとされる事件である．そしてこの広告が，トランプ大統領やイギリスの EU 離脱派の勝利に大きな影響を与えたと言われている．ここで分析に用いられた情報は性格診断ゲームのようなものを通して集められたもので，一応の個人の同意を得て取得されたものであるものの，このゲームをすることが自分の後の投票行動に影響を及ぼすことになることを認識していた人は決して多くはないだろう．

ここまでの話に共通する問題は，私たちは，今までの自分とは違う行動をとる可能性が奪われているのではないか，つまり，これまで好んで買ってきたものを繰り返し買い，これまでの自分の考え方や好みに合った企業にしか就職できず，これまでの行動から分析された自分の性格からすれば好ましく感じられる可能性の高い政治的意見にばかり触れるよう，仕向けられているのではないか，ということである．

この問題は，AI に固有の問題ではないかもしれない．たとえば，新橋など，サラリーマンが多いとされる地域でサラリーマン向けの広告を配る方が，学生街

で同じ広告を配るよりも効率的だ，という意味でのターゲティングは，古くから用いられてきた方法である．それでは，AI の問題はどこにあるのだろうか．

様々な観点からの検討がされるべきであろうが，ひとまず指摘できるのは，プロファイリングの基礎とされている情報は，目や手の動きなど，私たちが無自覚にしている行動に関するものも多く，どのような情報がどのように関連付いて，行動の予測につながっているのかは，本人からは分からないことであろう．しかも AI が情報解析のために用いるアルゴリズムは非常に複雑なもので，そこに大量の情報が入力されていくため，この情報解析の全容は人間にはもはや把握することはできないものと思われる．

この点について，日本の個人情報保護法制が「お手本」としている，EU の「一般データ保護規則（GDPR）」では，プロファイリングに対して異議を申し立てる権利を定めており，将来の日本で，プロファイリングに対して法的対処がとられる可能性もある．

認識や価値観の再生産の問題

最後に，生成 AI に特に強く現れる特徴として，従来の社会で共有されてきた認識や価値観などを繰り返し再生産していく側面を指摘しておきたい．

生成 AI は，ある一定の時期までに集めた大量の情報を基に，全く新しい情報をその場で作り出す．これは，人間が文章を書く過程に似ている部分もあり，たとえば，この原稿を書くまでの間に得た知識を基礎に，私はこの文章を書いている．それでは何が違うかといえば，生成 AI は，「一般的に受け入れられている」「常識的な」回答をするということと，膨大な情報を忘れることなく永遠に記憶しているということである．

AI が「餌」として食べている情報は，特定の誰かから得られるものではなく，世界中の多くの人が発信しているものであり，それゆえに，AI の表現活動の基となっている思考は平均化されていて，「常識的」である．しかし，私たち人間は，時に，常識とはかけ離れた意見を言ったり聞いたりしながら，試行錯誤を繰り返してきたはずである．何かの情報を生成 AI に聞いてみて，そこで得られた情報に満足してしまうのでは，これまで常識的とされてきた考え方や情報をそのままに受け入れ，再生産することに繋がる．

また，膨大な情報を永遠に記憶しているということも良いこと尽くめとは言い難い．たとえば，本稿を執筆している現在，「日本で起きた重大犯罪の被告人を教えて」と生成 AI に問うと，被告人の姓名や事件の詳細が次々に表示される．しかし，私たち人間は，記憶できる情報の量に限界があり，これまで起きた事件を事細かにすべて覚えていることはない．このような「忘れてしまう」という一種の能力の欠如が，一度は失敗してしまった人間を許し，社会の一員として再び受け入れることを可能にしているように思われる．そうであるとすれば，忘れることをしない生成 AI が，一定の人々の社会復帰を困難にするということも懸念される．

この点，日本の最高裁判所も，自身が過去に犯した犯罪についての検索結果を検索エンジンが表示することを問題とした事件において，「当該事実を公表されない法的利益」が「当該 URL 等情報を検索結果として提供する理由」よりも優越する場合には，検索事業者に対して当該 URL 等情報の検索結果の削除を請求できるとしている．ここには，いわゆる「忘れられる権利」に近い発想を読み取ることもでき，この観点からは，たとえば，生成 AI を用いるにしても，用いられる情報は一定期間で刷新されるなどの機能を埋め込んでおく必要があるかもしれない．

法的な解決策の困難？

AI にこれまで見てきたような問題点があるとして，それでは，私たちはその問題をどのように解決すればよいのだろうか．

国内で何か問題が生じたとき，原因となっている行為を法的に規制するという方法が考えられる．国内で殺人や窃盗などが起きないようにするために，刑法で，それらの行為をした者への法的な制裁を定めることで，殺人や窃盗を禁止するというイメージである．しかしながら，高度に専門的な先端技術の開発・利用については法的規制の難しさが頻繁に指摘される．

たとえば，AI の技術，あるいは，そこで用いられるアルゴリズムなどについて，正確な説明ができる者は，専門家であれば少なくないだろうが，私たちの民主的な代表である国会議員の中には，そのような専門家はほとんどいない．そのため，そもそも，AI の活動を構成する一連の技術のうち，どこを規制すれば効果的に問題を解決できるのか分からないという事態が生じる．このような事情から，専門的な先端技術について法的規制は難しい，あるいは何とか法規制を作っても，その技術の開発・運用の実態とはかけ離れた内容になってしまうなど，なかなかうまく機能しないこ

とが指摘されてきた．

法が果たすべき役割はあるか？それは何か？

それでは，先端技術について法が何かの役割を果たすことは出来ないということになるのだろうか．この結論に飛びつく前に，もう一度慎重に考えてみよう．

そもそも，なぜ，これまでの規制には法が用いられてきたのだろうか．なぜ，法は私たちの代表者として選ばれた国会議員によって定められるべきものであると考えられてきたのだろうか．それは，規制が，複数の価値の衝突を調和させるためのものだからだろう．

このことを，AI との関係で考えてみよう．上述の通り，AI の利活用は場合によっては私たちのプライバシー権を侵害する可能性がある．しかし，私たちの人生や社会全体の発展にとって，必要な価値はプライバシー権だけではない．学者をはじめとした研究職の者たちが自由に研究すること（学問の自由）は，これもまた社会全体の発展に寄与する重要な価値であり，その成果として何かの技術を開発することもここに含まれる．このとき，学問の自由を重視してプライバシー権の保障の程度を下げるのか，あるいは逆にするのかを決める，ということが価値の調整である．

どのような価値をどのくらい強く守るべきかは，人によって様々な考え方がある部分で，だからこそ，私たち自身が選んだ代表による決断でなければ納得がいかない，あるいは，代表による決断に納得がいかないならば，次回の選挙では他の代表を選ぶことで，異なった価値の調整を図りたい．このような私たちの気持ちが，ある行為を規制するときに，法という方法を選んできたことの基礎にあるはずである．

そして，このような価値の調整は，必ずしも，技術の発展や変容に敏感に反応するものではない．古くからある法規制として殺人罪を考えてみよう．ある人が包丁で誰かを刺し殺せば，この人は殺人罪に問われる．このとき用いられた道具が包丁ではなく，最新の技術を複雑に用いて開発された毒薬であったら，殺人罪が適用できなくなるだろうか．おそらく，そのようなことはないだろう．この殺人の規制において重要なのは，殺人という行為が，他の人の生命に対する権利を侵害する危険な行為であり，それゆえに「殺人の自由」は認められないという価値判断である．このとき，この最新の毒薬の中のどのような成分がどのように人体に作用し，死という結果を招いたかということについて，細部まで理解していなければ，この毒による殺人を罪として考えることが出来なくなるわけではない．

つまり，「法」が負うべき役割としてとくに重要なのは，どのような活動がなぜ危険だと考えられ，規制の対象となるべきかを定めるというものであり，そうであるとすれば，あるルールの隅々まで法律が定めることができないならば，それをもって法がルール制定に関わることを諦めるべきだということにはならないように思われる．

この点について，たとえば GDPR の規定は，AI のプロファイリングによって自身の自律的な生活や人生が阻害されたと考える人に対して，プロファイリングへの異議を申し立てる権利を認めているが，この規定の意義は，AI によって自律的な生活が阻害されることは私たちの「権利」を侵害していると考えるべきだという価値判断を示していること，それによって，その権利を用いて個人が裁判所でそのことをより具体的に争うための道を開いたという部分にあるように思われ，この規定がプロファイリングという技術の細部に至るまで細かく制約を定めていないからといって，その意義が失われることはない．

おわりに

本稿では，AI によって私たちの生活や人生の中で重要と思われる価値が傷つけられている，あるいはこれから傷つけられる可能性があることを指摘し，それについて，法はどのような役割を果たすことができるかということを見た．そして，法の最も重要な役割は，社会に多様に存在する価値の衝突を正面から見つめ，調整を試みることではないかと指摘した．残念ながら，これまでの日本では，AI をはじめとする先端的な情報技術の開発や利用において，どのような価値を優先的に守るべきかということをめぐる議論が十分になされてきたとは言いがたい．いまこそ，価値という難問に向き合わねばならないのではないだろうか．

[参考文献]

- 山本龍彦（編）『AI と憲法』（日経 BP マーケティング，2018）
- 生貝直人『情報社会と共同規制』（勁草書房，2011）