KGRI
Keio University Global Research Institute

KGRI Working Papers

No.5

「Comparative Law Research on the Personal Data Protection Law in Various Countries」

Version2.0

※仮訳（後日完全版を公表）

2024 年 3月

編集代表

山本龍彦

慶應義塾大学大学院法務研究科 教授

同グローバルリサーチインスティテュート 副所長

編集

飯田匡一

慶應義塾大学大学院法務研究科 研究員、弁護士

佐藤太樹

慶應義塾大学大学院法学研究科 博士課程

Keio University Global Research Institute

「Comparative Law Research on the Personal Data Protection Law in Various Countries」

【代表編者】

山本龍彦　（慶應義塾大学大学院法務研究科教授、KGRI 副所長）

【編者】

飯田匡一　（慶應義塾大学大学院法務研究科研究員、弁護士）

佐藤太樹　（慶應義塾大学大学院法学研究科博士課程）

【著者】

EU　　: Elaine Fahey　　（ロンドンシティ大学ロースクール教授）

ドイツ　: Meinhard Schröder　（パッサウ大学法学部教授）

スイス　: Florent Thouvenin　（チューリッヒ大学法学部教授）

　　: Samuel Mätzler　　（チューリッヒ大学大学院博士課程、スイス弁護士）

フランス: 小川有希子　　（帝京大学法学部助教）

タイ　　: Thitirat Thipsamritkul（タマサート大学法学部専任講師）

台湾　　: Chien-Liang Lee　　（中央研究院法律学研究所教授、同所長）

韓国　　: 尚知永　　（慶應義塾大学訪問研究員、韓国弁護士）

中国　　: 松田侑奈　　（KGRI 客員所員）

カナダ　: 山本健人　　（北九州市立大学法学部准教授）

アメリカ: Jesse W. Woo　　（コロンビア大学大学院修士課程、カリフォルニア州弁護士）

要旨

JST・ムーンショット型研究開発事業（目標 9）の「分散管理の法理」（課題推進者・山本龍彦慶應義塾大学教授）では、パーソナル AI を社会実装することで生ずる利点や課題を、法的観点から分析している。パーソナル AI とは、本人のプライバシー選好に基づいて本人のパーソナル・データを代行管理する AI である。これは、情報自己決定権（自己情報コントロール権）をバックアップするツールとして捉えることができる。

本研究は、EU・ドイツ・スイス・フランス・タイ・台湾・韓国・中国・カナダ・アメリカを対象に個人情報保護法制を比較研究するプロジェクトである。各国のレポート執筆者には、個人情報保護法において本人関与のための仕組み（削除請求権、アクセス権、同意、データポータビリティ権）がどのように規定されているのかについて調査を依頼した。特に憲法と個人情報保護法の関係性に注目しながら、情報自己決定権の意義と課題を検討した。

目次

＜質問項目（日本語）＞

1、憲法と個人情報保護制との関係性

① プライバシー権ないし情報自己決定権が、憲法上（条文または判例上）保障されているかどうか。またその際、プライバシー権と情報自己決定権との異同が意識されているかどうか。

② プライバシー権ないし情報自己決定権が憲法上の権利として保障されている場合、かかる権利が、個人情報保護法の目的規定のなかに読み込まれているかどうか。別言すると、個人情報保護法が、プライバシー権などの憲法的価値を実現する法令として位置付けられているかどうか。

2、個人情報保護法制の現状と課題

① 個人情報保護法を制定するにあたってモデルとした国はあるか。

② クッキー情報は個人情報保護法制における「個人データ（個人情報）」のなかに含まれているか。個人情報保護法上保護の対象となる「個人データ（個人情報）」の定義。

③ データ主体の権利と事業者の義務。

−(a) 利用停止請求権の範囲。例えば、日本の個人情報保護法では、令和二年の改正で利用停止請求権の範囲が拡大された。

−(b) 同意の位置付け（オプトイン方式かオプトアウト方式か）。本人の同意が要求される場面は。事業者が個人データを取得する場合に当該個人の同意を得ることが義務付けられているかどうか。また、個人データが第三者に提供される場合、当該個人の同意を得ることが義務付けられているかどうか。

−(c) ＜通知＝同意＞モデルの限界とその対策。個人の認知限界という観点から＜通知＝同意＞モデルの限界（同意疲れやプライバシーポリシーの流し読み）が予てから指摘されている。こうした課題に対して、各国の個人情報保護法制がどのように対応しているか（事業者に対して実効的な告知方法を義務付けるなど）。

−(d) 情報銀行や PDS(Personal Data Store)のように、パーソナル・データに対する本人の controllability を補助するための仕組みや制度はどのように社会実装されているか。

−(e) AI の利活用やプロファイリングの場面に特化したデータ保護の仕組みが存在するかどうか。

−(f) データ・ポータビリティ権は保障されているか。またこの権利は具体的にどのような場面で社会実装されているか。

④ 個人情報保護法を執行する監督機関の組織と権限（制裁や告訴の仕組み）。

⑤ 司法的救済の仕組み（訴訟要件、集団訴訟の可能性）

⑥ 研究・医薬品開発を目的とした診療データの二次利用。診療記録等を医薬品開発などの研究目的で利用する場合に、データ主体である患者の同意は要請されるのか。診療データを二次利用するにあたって、匿名加工などの一定の義務が課せられるか。

I. EU

Elaine Fahey（ロンドンシティ大学ロースクール教授）
Elaine.fahey.1@city.ac.uk
質問項目：EU のデータ・プライバシー

1. 憲法と個人情報保護制度との関係性

①プライバシー権ないし情報自己決定権の憲法上の位置づけ

欧州の個人情報保護制度は、個人が自分に関する個人データを管理できるべきであるという前提に基づいている。このような管理は多くの場合「情報自己決定権」[1] と呼ばれ、欧州連合基本権憲章 8 条に個人情報保護という基本権の論理的な根拠として位置づけられている。これは自分自身に関する情報のうち、誰に対し何の目的の下で公開されるかを決定するための個人の権利に関連するものとして理解されている。[2] 情報自己決定権は、EU 法に適用される概念の形態ではないデータ・プライバシーの自己管理とはある程度異なっている。監督を伴う分散化された執行体制を通じた権利の広範な行政化に支えられている独特の方向転換は、世界的にプライバシーに関する最も重要な分断の一つを生み出した。米国の法律はこれらの理想へとある程度移行しているものの、最終的には EU の価値観のアンチテーゼであるような価値観を今も支持し続けている（例えば、現在では米国内の 7 つの州がデータ・プライバシー法を制定している）。[3]

個人データを保護する権利は欧州連合の機能に関する条約 16 条と EU の一次法である EU 基本権憲章 8 条に明記されており、国家レベルでも EU レベルでも膨大な執行体制が整えられている。[4]

---

1 Kuner, Christopher and others (eds), The EU General Data Protection Regulation (GDPR): A Commentary(New York, 2020; online edn, Oxford Academic), https://doi.org/10.1093/oso/9780198826491.001.0001, 2023 年 6 月 30 日にアクセス。

2 P. Schwartz, “The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination”, The American Journal of Comparative Law, Vol. 37, No. 4, 1989, pp. 675-701

3 IAPP, “US State Privacy Legislation Tracker”, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/, 2023 年 6 月 26 日にアクセス。

4 Vogiatzoglou, Plixavra, and Peggy Valcke (eds), ‘Two Decades of Article 8 CFR: A Critical Exploration of the Fundamental Right to Personal Data Protection in EU Law’, Eleni Kosta, Ronald Leenes and Irene Kamara (eds), Research Handbook on EU Data Protection Law (Edward Elgar Publishing 2022) https://www.elgaronline.com/display/edcoll/9781800371675/9781800371675.00010.xml ; Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius (2019) The European Union general data protection

各加盟国にはデータ保護法の適用を監督するデータ保護機関（DPA）が設けられており、その違反に対する苦情を扱うとともに、以下に概説するとおり、膨大な範囲の手続きや救済措置が適用可能である。

憲章第 52 条（3）では、EU 基本権憲章と欧州基本権条約の両文書に対応する権利が含まれている限り、基本権憲章に規定されている権利の意味と範囲は欧州人権条約に規定されているものと同じであることとしている。しかし、この規定は EU 法がより広範な保護を提供することを妨げておらず、EU 法は特筆に値するようなプライバシーの理解を独自に深めている。欧州人権裁判所（ECtHR）では、個人情報が私生活の範囲に含まれるためにはプライバシーの要素も追加で必要としている。しかし、この点で EU 法は、ECHR 法と概念的にも実質的にも密接に結び付いているものの、自律的に幅広い範囲の権利を認めていると言えるものと考えられる。

② 個人情報保護制度の憲法上の意義

GDPR1 条（2）によると、同規則は「自然人の基本権や自由と、特に彼らの個人データが保護される権利」を守ることを目指している。EU 基本権憲章は、第 8 条において個人データの保護を提供している。EU 法ではリスボン条約以降 EU 基本権憲章が拘束力のある権利の源泉となっており、この中にはデータ保護権への言及も含まれている。基本権憲章が ECHR 法の影響を強く受けており、EU 法が現在も進行中であるその条約において EU の ECHR 加盟を定めていることから、ECHR 法は EU 法の基礎としてその重要な法源となっている。司法裁判所は、欧州のデータ保護法の進化に影響を与えるにあたり、EU 基本権憲章への依存を強めている。

↓

2. 個人情報保護法制の現状と課題

① 他国における法制度の影響

---

regulation: what it is and what it means, Information & Communications Technology Law, 28:1, 65-98, DOI: https://doi.org/10.1080/13600834.2019.1573501 ; Paul De Hert, Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Serge Gutwirth and others (eds), Reinventing Data Protection? (Spriner 2009) https://link.springer.com/book/10.1007/978-1-4020-9498-9#toc

複数の世界組織や国際組織が初のプライバシー条約を締結したと広く理解されている（例えば OECD または欧州評議会）が、欧州諸国はプライバシー保護規則をいち早く採択したことで特別な位置を占めている。例えば、スウェーデン、ドイツ、オーストリア、デンマーク、フランス、ルクセンブルクは、1970 年にドイツで世界初のデータ保護法が定められた後にプライバシー法を法制化している。[5] 1981 年 1 月には、世界発のデータ保護条約であり EU 法にも影響を与えた個人データの自動処理に関する個人の保護のための第 108 号条約を欧州評議会が採択している。ここで、他国が EU 法に与えた影響を辿るよりことも重要な点として、EU による GDPR という形を通じてプライバシーに関する世界基準を通じた他国の基準へ影響を与えるという EU の意図を指摘したい。[6]

②「個人データ」の定義と範囲

一般的にクッキー法として知られる ePrivacy 指令は 2002 年に成立し、2009 年に改正されているが、これは GDPR が発効すると同時に 2018 年にいわゆる ePrivacy 規則として成立させることを意図していたものの、まだ採択に至っていない。その後、2021 年に提案された ePrivacy 規則では、クッキー（ユーザーのブラウザーに由来する ID 識別子）の使用についてより厳しい規則を導入することを意図していた。GDPR の下では、クッキーID は個人データであると見なされている。クッキーに関する法律は、ブレグジット後の英国が GDPR に規定されている特定の重要な保護を排除することを同国が検討するための広範な根拠を提供している。

↓

③ データ主体の権利と事業者の義務

a) 個人データの削除権（例えば GDPR 第 17 条）または利用停止請求権

個人はその個人データを消去するようデータ管理者に依頼できる（例えば、データ処理の目的の下でデータが必要でなくなった場合）。画期的な判決であった 2014 年の判決 C-131/12 *Google Spain and Google* EU:C:2014:317 では、CJEU がいわゆる「忘れられる権利」を定めている。

---

5 Streinz, Thomas, The Evolution of European Data Law (January 18, 2021). Paul Craig and Gráinne de Búrca (eds), The Evolution of EU Law (OUP, 3rd edn 2021), 902-936, Available at SSRN: https://ssrn.com/abstract=3762971 or http://dx.doi.org/10.2139/ssrn.3762971; Graham Greenleaf, How far can Convention 108+ 'globalise'? Prospects for Asian accessions, Computer Law & Security Review, Volume 40, 2021, 105414, https://doi.org/10.1016/j.clsr.2020.105414.

6 E.g. 2017 Communication from the European Commission, 'Exchanging and Protecting Personal Data in a Globalised World' COM 2017 7 final.

この権利は、現在では GDPR17 条に明記されている。*Google v CNIL*（C-507/17）では、忘れられる権利の領域的範囲を裁判所が決定する必要に迫られ、EU 圏外の検索結果へのアクセスを防ぐ、あるいは少なくとも真剣に防ぐ措置と関連して、EU 全域での参照解除に関する一般規則を確立している。しかしながら、概念としては世界的に普及しており、そのような判例法は EU 法を象徴するものとして捉えられており、その実施、検索エンジンの透明性、公人などについては多くの論争を引き起こしている。[7]

b) 同意の位置付け（オプトイン方式かオプトアウト方式か）。

個人データの処理は一般的に禁止されており、法律により明示的に許可されている場合、またはデータ対象が処理について同意した場合を例外としている。個人データ処理について比較的よく知られた法的根拠の一つである一方で、同意は EU 一般データ保護規則（GDPR）で言及されている六つの根拠の一つに過ぎない。その他の根拠は契約、法的義務、データ対象の重大な利益、公益、正当な利益であり、GDPR6 条（1）に明記されている。妥当な法的同意の有効性の基本要件は第 7 条で定義されており、GDPR 前文 32 でさらに詳しく明記されている。同意は自由に与えられ、具体的で、十分な情報に基づいて行われ、明確でなければならない。自由意思に基づく同意を得るためには、その同意が自発的に与えられなくてはならない。判例 C-673/17 – *Planet 49 GmbH* ECLI:EU:C:2019:80 では、GDPR6 条（1）に関して、CJEU は同意が明瞭な肯定的行為により与えられなくてはならないと判示しており、この権利中心型の EU 法の見解が重要であるように見える。[8]

c) ＜通知＝同意＞モデルの限界とその対策。

上述のとおり、同意は GDPR の運用の中核を成す原則である。その個人主義と人間中心的なプライバシーの適用への注目がその運用を支配しており、ソロブが概説している原則のアンチテーゼであるとも論じることが可能である。

---

7 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf Vrabec, Helena U., 'The Right to Be Forgotten', Data Subject Rights under the GDPR (Oxford, 2021; online edn, Oxford Academic, 22 July 2021) 参照, https://doi.org/10.1093/oso/9780198868422.003.0006, 2023 年 5 月 22 日にアクセス。

8 Wiedemann, K. The ECJ's Decision in "Planet49" (Case C-673/17): A Cookie Monster or Much Ado About Nothing?. IIC 51, 543–553 (2020). https://doi.org/10.1007/s40319-020-00927-w

d) PDS（Personal Data Store）のように、 個人データに対する本人の controllability を補助するための仕組みや制度はどのように社会実装されているか。

パーソナルデータストア（PDS）は複雑な技術クラスを表すものであり、GDPR 下における責任に関連する数々の興味深い不確実性を提起している。個人データの特別なカテゴリの処理は、適用除外がない限り GDPR9 条（1）により禁止されているが、商業的な文脈ではこれは一般的に明示的な同意のことである。[9] 「自然人によって、純粋に個人的又は家庭的な活動の過程で行われる」、専門的または商業的な活動との関連性がない場合にデータ処理が発生する状況において、GDPR をかかる処理に適用されないようにする「個人的・家庭的な適用除外」は、狭く解釈されている。PDS は、GDPR 下において、プラットフォームそのものも自らの意図の下で利用者データを処理することにより商業的な目的を追求できるという課題を提起している。PDS は同意志向であり、利用者の同意の適切な取得を支援するための手段を提供できる可能性がある。[10] 全体的に、PDS の目的も類似しており、個人データの処理についてさらなる透明性や管理をもたらすことで個々の利用者に力を与えることを目指している。

e) AI の利活用やプロファイリングの場面に特化したデータ保護の仕組みが存在するかどうか（GDPR 第 21 条）。

GDPR22 条では、データ主体は自動的な処理またはプロファイリングのみに基づいて法的または重大な効果を伴う決定の対象とならない権利を有する。第 2 項で定められている条件に従って自動化された決定が例外的に許可される場合、データ管理者はデータ対象のために、人間による介入を得る権利、自らの視点を表現する権利、決定に異議を申し立てる権利など、適切な保護措置を講じなくてはならない（GDPR22 条（3））。

プロファイリングとは、「特に自然人の仕事における成績、経済的状況、健康、個人的嗜好、関心事、信頼性、行動、位置、または移動などに関する個人的側面を分析または予測する目的で、かかる自然人に関連する特定の側面を評価するための個人データの使用により構成される、あらゆる形態で行われる個人データの自動化された処理」のことである（LED3 条（4）、GDPR4 条（4））。

---

9 Janssen, Heleen and Cobbe, Jennifer and Norval, Chris and Singh, Jatinder, Decentralised Data Processing: Personal Data Stores and the GDPR (December 28, 2020). International Data Privacy Law, Volume 10, Issue 4 Pages 356–384, https://doi.org/10.1093/idpl/ipaa016 (28 December 2020).

10 Bodó, B. and Irion, K. and Janssen, H. and Giannopoulou, A. (2021). Personal data ordering in context: the interaction of meso-level data governance regimes with macro frameworks. Internet Policy Review,[online] 10(3). https://policyreview.info/articles/analysis/personal-data-ordering-context-interaction-meso-level-data-governance-regimes より入手可能 [2023 年 5 月 22 日にアクセス]。

そのため、プロファイリングはそれ自体が自動化された意思決定の一形態なのである。GDPR21 条では、データ主体が、第 6 条（e）または（f）に基づき、当人に関する個人データの処理について（それらの規定に基づいたプロファイリングを含む）、いつでも当人の特定の状況に関連する根拠により意義を申し立てる権利を有することを明記している。EU のデータ保護法は法律により体系的または個別に予測的な取り締まりのアプリケーションが提供されている場合においてそのようなアプリケーションの使用を防いでおらず、その一方で数々の但し書や条件が法律の確実性を損ねており、その有用性をさらに制限している可能性がある。[11]

f) データ・ポータビリティ権は保障されているか（例えば GDPR 第 20 条）。またこの権利は具体的にどのような場面で社会実装されているか。

GDPR20 条はデータ・ポータビリティ権を提供しているが、この概念の解釈が狭ければ個人にもたらされる利益が少なくなる一方で解釈が広ければデータ管理者にとって懸念事項となることから、その権利の行使にはまだ明確化する必要があると言われている。明確化されていないにもかかわらず、GDPR20 条は、オンライン上の評判など、統計上または分析上の目的に沿ってサービスプロバイダーが生成したデータの移転については対象外としている可能性がある。GDPR20 条の文言がデータ・ポータビリティ権の範囲をかなり制限してしまっていると主張されている。

データ・ポータビリティ権は生存している特定可能な個人のみが利用できることから、法人が GDPR20 条を行使することはできない。GDPR20 条によるデータ・ポータビリティ権はその曖昧さと、それに含まれている他のデータ主体の権利や自由などといった固有の限界により意図する結果を提供できない恐れがある。データ・ポータビリティ権には数々の示唆がある（例えば、市場へのアクセスの促進、高い切り替えコストの防止、市場における潜在的な競争を脅かすネットワーク効果の緩和）。[12]

④個人情報保護法を執行する監督機関の組織と権限（制裁や告訴の仕組み）。

11 Lynskey, Orla, ' Article 20 Right to data portability', in Christopher Kuner and others (eds), The EU General Data Protection Regulation (GDPR): A Commentary (New York, 2020; online edn, Oxford Academic), https://doi.org/10.1093/oso/9780198826491.003.0052, 2023 年 6 月 30 日にアクセス。

12 Peter Swire and Yianni Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' (2013) 72 Maryland Law Review 335.

GDPR75 条以降では、文献レビューで概説しているとおり、監督の仕組み、権限、および手続きについて膨大な数の規定が提供されている。判決 C-132/21 *Budapesti Elektromos Művek* ECLI:EU:C:2023:2 では、CJEU はそのような GDPR 救済条項の一貫した均質な適用を保証することは加盟国に委ねられることであるとしながらも、CFR47 条に違反しないことを保証するなどの保護措置を提供しなくてはならないとも述べている。

法定目的が公益にあり、データ主体の権利や自由の保護という分野で活動する非営利団体、組織、または協会は、データ主体を代表して DPA に苦情を申し立てたり、GDPR80 条に基づきデータ主体を代表して司法救済権や損害賠償を求める権利を行使できる。CJEU は最近、GDPR80 条（2）の下、国内法により消費者保護協会が GDPR 違反に関する法的手続きを取れると判示している（判決 C-319/20 *Meta Platforms Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände* ECLI:EU:C:2022:32）。

法務官は、判決 C-300/21 *UI v Österreichische Post* AG ECLI:EU:C:2022:756 において、GDPR82 条違反による非物質的損害の性質について問うている予備的問題に関して意見書を出している。中でも、AG は非物質的損害の賠償が、侵害の結果としてデータ主体が感じる可能性のある単なる取り乱しをその対象内に含めないものと結論付けている。

GDPR83 条（5）および（6）によると、GDPR の重大な違反により課すことができる罰金の上限は€2000 万または事業者の直近の会計年度における全世界の売上額の 4 パーセントのうち大きい方であり、2023 年における非常に重要な決定の対象となっている。[13]

⑤司法的救済の仕組み（訴訟要件、集団訴訟の可能性）

13 EDPB/ Irish Data Protection Commissioner decision as to Meta March 2023. 'Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation'を参照, https://edpb.europa.eu/system/files/2023-05/final_for_issue_ov_transfers_decision_12-05-23.pdf

GDPR 前文 143 で概説されており、また本稿でも概説するように、GDPR78 条の規制に関しては非常に幅広い範囲の司法救済措置が適用される。GDPR 下における監督当局は、GDPR 下における個人の権利の侵害に対する苦情を検討し、罰則が有効であるように管理者または処理者に非常に多額の上限額までの罰金という形で罰則を課すための権限が義務付けられている。その結果、そのような機関は加盟国の法律により独立した当局として設立され、任期が定められ、早期解任に対する法的保証があり、調査と決定に関する権限が委ねられている事項において完全な管轄権がなければならない。データ保護監督当局は EU 法において「法廷」である事に関する要件を満たさないため、彼らの決定事項は GDPR78 条に従った裁判所による司法審査を受けなければならない。第 77–79 条の目的は、国内法の下で存在している可能性のある他のいかなる救済にもかかわらず、国内法において効果的に果たされなければならない。

④個人情報保護法を執行する監督機関の組織と権限（制裁や告訴の仕組み）。

第 78 条（1）では、国内法の下において監督当局の法的拘束力のある判決に対し裁判所に上訴する機会が設けられていることを要求している。加えて、第 78 条（2）では苦情を受理した監督当局の無活動に対し司法的救済が用意されていることを義務付けている。[14]

判決を下すことを可能にするために問題に対する決定が必要であると判断する国内裁判所、または TFEU267 条に規定されている場合は、本規則を含む EU 法の解釈について予備的判決を下すように司法裁判所に要求しなければならない。[15] その国内裁判所は理事会の決定を無効であると宣言する権限を有していないものの、決定が無効であると見なすという司法裁判所の解釈のとおり TFEU267 条に従い、司法裁判所に妥当性の問題を付託する必要がある。

14 実際に、CJEU はそのような苦情を「相当の注意を払って」審査することは監督当局の義務であることを強調している。判決 C-362/14 Maximillian Schrems v Data Protection Commissioner ECLI:EU:C:2015:650, para 5.を参照。

15 判決 C-645/19 Facebook Ireland Ltd and Others v Gegevensbeschermingsautoriteit ECLI:EU:C:2021:483.

⑤司法的救済の仕組み（訴訟要件、集団訴訟の可能性）

GDPR により集まっている注目が増えた主な理由はその新たな制裁体制にあるが、これは EU 競争法に触発されているようである。DPD は違反を制裁する方法について概ね各加盟国の判断に委ねていたのに対し、GDPR では「効果的、比例的、かつ思いとどまらせるような罰則」を義務付けており、行政罰が事業者の全世界での年間売上額の最大 4 パーセントまでの額に上る場合があると規定している。

前述のとおり、法定目的が公益にあり、データ主体の権利や自由の保護という分野で活動する非営利団体、組織、または協会は、データ主体を代表して DPA に苦情を申し立てたり、GDPR80 条に基づきデータ主体を代表して司法救済権や損害賠償を求める権利を行使できる。

⑥研究・医薬品開発を目的とした診療データの二次利用

GDPR9 条（2）（g）では、「自然人及び健康に関するデータを一意に識別する目的での遺伝子データ、生体認証データの処理」が「追求される目的に釣り合うものでなければならず、データ保護の権利の本質を尊重し、データ主体の基本権および利益を保護するための適切かつ具体的な措置を提供しなければならない連邦法または加盟国の法律に基づき、実質的な公共の利益のために必要」であれば許容されることを規定している。

この条項と、研究目的での診療データの活用の関係性について、質問がある。診療記録等を医薬品開発などの研究目的で利用する場合に、データ主体である患者の同意は要請されるのか。診療データを二次利用するにあたって、同意の他に一定の義務が課せられるのか。

欧州保健データスペース（EHDP）における最近の動向についてもご教示いただきたい。

EU 一般データ保護規則 2016/679（GDPR）の運用には、データ保護の原則、個人データを処理するための法的根拠、データ主体に与えなくてはならない情報、データ主体の権利という四つの要素がある。

それぞれの要素に、利害のバランスが含まれる。研究者がヒト参加者と直接連絡を取る単独の研究では、セキュリティやデータ最小化の基準（すなわち、プロジェクトの目的に対して必要な期間のみデータを収集、分析、および保管すること）を満たし、データ主体にはプロジェクトについて完全に通知し、データ主体の権利が尊重されていなくてはならない。より複雑なデータ共有の方法は GDPR を通じて交渉することが難しいと言われている（例えば、元の同意が新たな処理に対し有効かどうか）。[16] データガバナンス法（DGA）と EU 一般データ保護規則（GDPR）と併せて、欧州保健データスペース（EHDS）の規制の提案は、欧州連合における診療データの利用に向けた新たな規制とガバナンスの枠組みを形成している。[17] 欧州データ戦略（European Strategy for Data）は、経済や社会でデータを利用可能にしつつ、データを生成しそれらを管理する個々人を保護するために、EU における単一のデータ市場を創出し、健康を含む複数の戦略的領域における共通の欧州データスペースを確立させることを目指している。[18] それでも、欧州のデータ保護法またはその欠如に見られるこれらの課題の権利中心型の性質は多くの議論を呼んでいる。[19]

プライバシーの決定については多大な議論が行われてきており、個人の選択が妥当であると認められるためにその選択の参考として必要な情報量についてはかなりの複雑性が伴う

---

[16] Townend, D. (2021). Privacy. In G. Laurie, E. Dove, A. Ganguli-Mitra, C. McMillan, E. Postan, N. Sethi, et al. (Eds.), *The Cambridge Handbook of Health Research Regulation* (Cambridge Law Handbooks, pp. 73-80). Cambridge: Cambridge University Press. doi:10.1017/9781108620024.010

[17] European Health Data Space." European Commission.; European Commission, "Proposal for a Regulation of the European parliament and of the Council on the European Health Data Space" COM/2022/197 FINAL, May 3, 2022 <https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en>（2023 年 7 月 1 日）。

[18] デジタルサービス法（DSA）では、オンライン・プラットフォームやオンライン検索エンジンが公衆衛生や未成年の保護、ならびに人の身体的および精神的健康に対する深刻な悪影響に対する保護について、設計、機能、および利用の観点からリスクを評価しなければならない。デジタル市場法（DMA）では、委員会は公衆衛生を根拠にゲートキーパーを免除しており、これまで禁止されていた個人データの処理を許可している。

[19] EDRi. "EU's proposed health data regulation ignored patients' privacy rights." EDRi. March 6, 2023. <https://edri.org/our-work/eu-proposed-health-data-regulation-ignores-patients-privacy- rights/>（2023 年 7 月 1 日にアクセス）。

.

（例えば、多くの最先端の生物医学研究の方法論）。[20] EHDS の前は、GDPR7 条（3）においてデータ主体にいつでも同意を撤回する権利があると定められていたものの、データ管理者の関連する義務が示されていなかった。EHDS は、診療データの二次利用について、開発・イノベーション活動、アルゴリズム及び AI 関連のプロジェクト、個別化医療への応用など、非科学的な正当化の理由を追加で導入している（EHDS34 条（1）f-g）。GDPR による規定をさらに発展された EHDS は診療データの二次利用に関する条項を定め、「社会の一般的利益」に貢献することを意図している。第 34 条では、アルゴリズムの訓練、試験、および評価について許可される目的を定めている。他の条項は、その他の目的（例えば科学研究、公衆衛生、健康関連の統計、教育活動、個別化医療の提供）に関連している。個人または社会全体にとって悪影響を及ぼす、または有害である活動のための二次利用は禁止されている。

α:データ主体のアクセス権（GDPR15 条）と GDPR15 条（h）の AI は、「第 22 条（1）および（4）に言及されるプロファイリングを含む自動化された意思決定の存在、ならびに少なくともそのような場合における、関係する論理に関する有意義な情報およびデータ主体にとってのそのような処理の重要性と想定される結果」について、管理者から確認を得る権利をデータ主体が有するものとしている。この条項における「有意義な情報（meaningful information）」の意味は何か？一般的に、一般人は AI のアルゴリズムを理解するための特別な能力または専門性を有していない。判例法やガイドラインの下で「有意義な情報」と見なされるような説明はどのようなものか？

医療データアクセス機関（HDABs）はデータ許可証を発行することで二次利用のための診療データへのアクセスを許可できる（開発、訓練、試験を支援するため、AI 法の下で健康領域における AI システムを検証するためなど）。[21]

---

[20] Townend, D. (2021). Privacy. In G. Laurie, E. Dove, A. Ganguli-Mitra, C. McMillan, E. Postan, N. Sethi, et al. (Eds.), *The Cambridge Handbook of Health Research Regulation* (Cambridge Law Handbooks, pp. 73-80). Cambridge: Cambridge University Press. doi:10.1017/9781108620024.010.

[21] Teodora Lalova Spinks, 'People Have the Power: Patient empowerment in the European Health Data Space proposal (Part I)'を参照。

https://www.law.kuleuven.be/citip/blog/people-have-the-power-patient-empowerment-in-the-european-health-data-space-proposal-part-i/ (accessed 1 July 2023); Tjaša Petročnik and Sofia Palmier 'The AI Act and European Health Data Space Proposal Seeing AI

すべてのデータ保護機関（DPA）の調査と、プライバシー関連の組織の専門家とのインタビューにより構成された 30 ヵ国（EU 加盟国 27 ヵ国と EFTA EEA 加盟国 3 ヵ国）で行われた実証研究からは、アクセス要求権の範囲に入りうる複数のタイプの潜在的な「有意義な情報」と、データ主体が被る影響に関する複数の情報タイプが評価されたが、これらの情報タイプのほとんどが実務において滅多に、またはまったく提供されていないことが明らかになっている。[22]

β) データ主体のアクセス権（GDPR15 条）、データ・ポータビリティ権、及び診療記録

データ主体のアクセス権（GDPR15 条）を行使することにより、データ主体は時分の診療記録または診療データを病院から取得できるか？これらの診療データはデータ・ポータビリティ権に含まれているか？

個別化医療サービスのための個別のアプリへと診療データを集約することも考えられる。そのような個別化医療サービスと欧州保健データスペース（EHDS）の関係性について伺いたい。

GDPR は第 20 条（1）においてデータ・ポータビリティ権を定義しており、個人には明確で簡単な方法によりその個人データを受領する権利と、それらのデータを元の管理者により妨げられることなく別の管理者へ送信する権利があることを明記している。EHDS の下では、データ・ポータビリティ権は EHDS3 条（8）に定められている。[23] これは、患者が複数の医療提供者の間で公共管理者または民間管理者が処理した一次診療データを交換し、それらへのアクセスを提供することを可能にするために、診療データの一次利用と結びついていると理解されている（薬局、病院、およびその他の医療現場、EHDS10 条（2）（o）（4））。[24]

---

to Ai with one another European Law' Blog 26/2023 < https://europeanlawblog.eu/2023/05/30/the-ai-act-and-european-health-data-space-proposal-seeing-ai-to-ai-with-each-other/>（2023 年 7 月 1 日にアクセス）。

[22] Bart Custers, Anne-Sophie Heijne, 'The right of access in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice' (2022) 46 Computer Law & Security Review' 105727.

[23] Florina Pop and Laura Grant 'Data portability in the European Health Data Space: Benefits, Risks, and Challenge' <https://www.eipa.eu/blog/data-portability-in-the-european-health-data-space/#> EUIA Blog（2023 年 7 月 1 日にアクセス）

[24] Teodora Lalova Spinks, 'People Have the Power: Patient empowerment in the European Health Data Space proposal (Part I)'を参照。
https://www.law.kuleuven.be/citip/blog/people-have-the-power-patient-empowerment-in-the-european-health-data-space-proposal-part-i/ （2023 年 7 月 1 日にアクセス）。

「電子診療データ（electronic health data）」の定義と前文 12 によると、GDPR とは異なり、EDHS における一次データ・ポータビリティは推論データも対象としている。

CJEU は、GDPR15 条（1）（c）において管理者に、データ主体が要求した場合に個人データの具体的な受領者の身元を公開することを義務付けているが、かかる要求が明らかに根拠がない、又は過剰である場合は例外とし、その場合は受領者のカテゴリに関する情報のみで十分であると判決 C-154/21, *RW v Österreichische Post*, 12 January 2023 において判示している。[25] 2023 年には、ニコラス・エミリウ法務官が判決 C-307/22 *FT v DW* の意見書において、GDPR12 条（5）と 15 条（3）が、データ主体にその個人データの複製を提供することをデータ管理者に要求するものであると解釈しなければならないとし、データ保護とは無関係な目的のための複製をデータ主体が要求している法的手続きまで関連付けている。[26] その訴訟事件では、治療ミスを疑った歯科医院の患者が、訴訟に向けた準備の過程で歯科医院が所有している彼に関するすべての診療記録の複製を無償で提供するよう歯科医院に要求している。

※本研究は、JST【ムーンショット型研究開発事業】グラント番号【JPMJMS2293】の支援を受けたものです。

[25] ECLI:EU:C:2023:3.

[26] ECLI:EU:C:2023:315

ドイツにおける個人データ保護法についてのレポート

マインハルト・シュレーダー＝アレクサンダー・フラマースベルガー
パッサウ大学

Question List/ Fragenkatalog

1. The Relationship between Constitutional Law and Personal Data Protection Law

①Constitutional Status of the Right to Privacy or the Right to Informational Self-Determination

"Is the right to privacy or the right to informational self-determination (i.e., the right to self-determination in the management of personal data; das Recht auf informationelle Selbstbestimmung) guaranteed as a constitutional right? If so, is the right to privacy interpreted to be different from the right to informational self-determination?"

a) プライバシーの権利

基本法 2 条 1 項は、次の言葉で始まる。「何人も、自己の人格を自由に発展させる権利を有する」。一般的な見解[1]によれば、これによって 2 つの独立した基本権が表現されている。つまり、一般的行為自由[2]と、一般的人格権[3]である。一般的行為自由が受け皿的な基本権としての機能しか持たず、より特別な自由権と比べて補充的なものであるのに対して[4]、一般的人格権は、判例の積み重ねのなかで特別な自由権と同等の権利へと発展してきた[5]。一般的人格権は、基本法 1 条 1 項に基づく人間の尊厳と、基本法 2 条 1 項から導かれる人格権が結びついて、常に「コンビネーション基本権」として引用される[6]。もっとも、ドグマーティク上、2 つの基本権が重畳的に適用されるわけではなく、基本法 1 条 1 項との結びつきは、単に解釈上の刺激として、また保障の範囲を明確化するものとして用いられるにすぎない[7]。一般的人格権に人間の尊厳が積み込まれることによって、基本法 2 条 1 項における当初の明確な成文化とは、いくぶん距離をおくこととなった。したがって、一般的人格権の実際の範囲は、コンビネーションのなかではじめて提示されうる。一般的人格権の保障内容は、人格の完全性、すなわち、行為とは区別されるところの存在である[8]。この基本権は、個性が退避する空間を各人に保障する。つまり、各人は「私事において放っておかれる」[9]、「自分自身に属する」[10]権利を有する。この権利は、ある程度までは、匿名性の権利も含んでいる[11]。レーバッハ判決において、連邦憲法裁判所はこのこと

[1] Andere Ansicht wohl *Kube*, in: HStR VII, § 148 Rn. 108.
[2] Die Garantie derselben ergibt sich vor allem aus einer historischen Auslegung – Art. 2 des Herrenchiemsee-Entwurfs lautete: „Jedermann hat die Freiheit, innerhalb der Schranken der Rechtsordnung und der guten Sitten alles zu tun, was anderen nicht schadet.", vgl. JbÖffR, NF Bd. 1 S. 55 – und aus einer systematischen Auslegung unter Berücksichtigung der weiten Schrankenregelung.
[3] BVerfGE 95, 267 (303); BVerfGE 6, 32 (36 f.); BVerfGE 80, 137 (152 f.).
[4] BVerfGE 85, 214 (217 f.); BVerfGE 148, 267 Rn. 38.
[5] BVerfGE 153, 182 Rn. 205; BVerfGE 118, 168 (183); BVerfGE 106, 28 (36).
[6] Im Anschluss an die zivilrechtliche Rechtsprechung BVerfGE 34, 269 (278); schon in der Lüth Entscheidung Art. 2 Abs. 1 GG mit Art. 1 GG in Verbindung bringend BVerfGE 6, 32 (41).
[7] BVerfGE 27, 344 (351); *Rixen*, in: Sachs, GG, 9. Aufl. 2021, Art. 2 Rn. 63.
[8] Vgl. *Rixen*, in: Sachs, GG, 9. Aufl. 2021, Art. 2 Rn. 59; siehe auch bereits *Dürig*, JR 1952, 259 (261).
[9] *Starck*, in: v. Mangoldt/Klein/Starck, GG, 7. Aufl. 2018, Art. 2 Abs. 1 Rn. 85.
[10] *Arndt*, NJW 1967, 1845 (1846).
[11] Vgl. dazu *Neumann-Duesberg*, Juristen-Jahrbuch VII, S. 138. Siehe auch *v. Mutius*, Anonymität als Element des

を明確に表現している。「何人も、原則として、自分の生活像の全体または生活における特定の出来事を、他人が公に描写してよいか、またどの程度まで描写してよいかを、自分で、かつひとりで決定することができる」[12]。

b) 情報的自己決定

1983 年の国勢調査判決において、連邦憲法裁判所は、基本法 1 条 1 項と結びついた 2 条 1 項の一般的人格権から、情報自己決定権を発展させた[13]。この際に連邦憲法裁判所は、一般的人格権のこれまでの具体化は、網羅的なものではないと述べた。つまり、一般的人格権には、技術発展が進展していくことにより新たな危険が生じる過程で、さらなる発展をみせる余地がある[14]。したがって、〔国勢調査判決において〕連邦憲法裁判所が「マイクロセンサス」[15]、「離婚文書」[16]、「医療記録」[17]、「レーバッハ」[18]および「依存症患者相談所」[19]といった〔国勢調査判決以前の〕諸裁判を参照指示することで示しているように、国勢調査判決以前にも、個人関連データの保護は存在していた。しかし、連邦憲法裁判所は、現代の情報技術がもたらす新たな危険の到来を利用して、情報的自己決定という形で人格権から特別な形態を導出し、そうすることで、技術革新に伴う一般的人格権の重要性の高まりを考慮する契機とした[20]。 情報自己決定権は一般的人格権から導き出されたものであるが、判例は、その独自性をますます強調している[21]。情報自己決定権は、もともとは一般的人格権から具現化されたものとして、憲法上の地位も有する。しかし、その導出とそれに伴う特有の保護方向のゆえに、憲法上で明示的に表れてはいない。

c) 差異

情報自己決定権は、一般的人格権から発展したものであるため、それらの差異というよりは、特殊性について言及しなければならない。一般的人格権は、個人の完全性に対する国家の介入からの保護を提供するものである。各人は、「自己決定的な方法で個性を発展させ、維持する」ことができなければならない[22]。このとき、一般的人格権は、人格の発展に関わる要素のうち――基本法の特別な自由の保障をすでに受けるものではないにせよ――人格を構成する重要性という点で、これらの自由保障にひけをとらないものだけを保護する[23]。したがって、一般的人格権には、例えば、自己の言葉に対する権利[24]、自己の記録や自己の肖像に対する権利[25]、さらに人間のセクシュアリティ[26]も含まれる。原則とし

allgemeinen Persönlichkeitsrechts – terminologische, rechtssystematische und normstrukturelle Grundfragen, in: Bäumler/v. Mutius, Anonymität im Internet, 2003, S. 12 ff. Siehe auch BGH, NJW-RR 2007, 619 (620).

12 BVerfGE 35, 202 (220).
13 BVerfGE 65, 1.
14 BVerfGE 65, 1 Rn. 152.
15 BVerfGE 27, 1 (6).
16 BVerfGE 27, 344 (350 f.).
17 BVerfGE 32, 373 (379).
18 BVerfGE 35, 202 (220).
19 BVerfGE 44, 353 (372 f.).
20 *Dreier*, in: Dreier, GG, 3. Aufl. 2015, Art. 2 I Rn. 79.
21 BVerfGE 115, 320 (341); BVerfGE 120, 351(360); BVerfGE 133, 277 Rn. 105; ebenso *Jarass*, in: Jarass/Pieroth, GG, 17. Aufl. 2022, Art. 2 Rn. 40.
22 BVerfGE 141, 186-220, Rn. 32; BVerfGE 35, 202 (220); BVerfGE 79, 256 (268); BVerfGE 90, 263 (270); BVerfGE 117, 202 (225).
23 BVerfGE 141, 186-220, Rn. 32; BVerfGE 79, 256 (268); BVerfGE 99, 185 (193); BVerfGE 120, 274 (303).
24 BVerfGE 34, 238 (246 ff.); hinsichtlich der Abgrenzung zu Art. 10 GG oder Art. 13 GG vergleiche etwa *Starck*, in: Mangoldt/Klein/Starck, GG, 7. Aufl. 2018, Art. 2 Abs. 1 Rn. 92.
25 BVerfGE 80, 367 (375).
26 BVerfGE 47, 46 (73 f.).

て、個人関連データの処理に対する保護も、これらの事例群に数えられる。すなわち、データが保護されるのは、そうしたデータから〔個人の〕人格が帰納的に推論されうるからである。自動化されたデータ処理によって、一般的人格権に特別な脅威が及ぶが、情報自己決定権という〔一般的人格権の〕特別な形態によって、こうした脅威への対応がなされた。この点で、一般的人格権と情報自己決定権は、主に事項的に関係するポイントの点で異なっており、抽象的な保護強度に関してさほど異なるところはない。それにもかかわらず、情報的自己決定は、現代のデータ処理に固有の危険に関して、保護領域の「側防と拡張」を行うものである。つまり、これにより、保護領域への潜在的な介入は、早くも危険が及びうる段階へと移行する[27]。実効的な基本権保護のために、判例は、個人関連データのあらゆる処理は介入を構成し、この点で「些細なデータ」はもはや存在しない、という意味において、情報的自己決定の保護領域を拡張している[28]。

以上をまとめると、情報的自己決定は、一般的人格権の独立した一形態として理解されるべきであり、その造形において、データ処理に関する特別な要請ないしそれに伴う危険に適合したものである。このような区別は、「忘れられる権利 I」に関する連邦憲法裁判所の説示においても支持されている。この事件で、連邦憲法裁判所は、オンライン・アーカイブにおける報道記事の保存に関する事実関係についての判断を求められた。連邦憲法裁判所は、一般的人格権と情報的自己決定を、関係者の保護の必要性に基づいて区別した。このように考えると、この事件における危険は、データ処理によってではなく、特定の情報を公に流布することによって現実のものとなる[29]。

② Constitutional Significance of the Personal Data Protection Law

"If the right to privacy or the right to informational self-determination is constitutionally protected in any sense, is such right defined or stipulated as a purpose or guiding principle of the personal data protection law? In other words, is the personal data protection law characterized as a statute that implements constitutional values or norms such as the right to privacy?"

GDPR の 1 条 2 項において、GDPR は、規則の目標が、自然人の基本権、とりわけ個人関連データの保護の権利を保護することであると明示的に定めている。ここで重要なのは、GDPR が個人関連データの保護のみを目標としているのではないということである。これは、GDPR の 1 条 2 項後段における「特に」という言葉ですでに表現されている〔GDPR1 条 2 項後段は、「……特に、自然人の個人関連データの保護の権利を保護する」と規定する〕。むしろ GDPR は、基本権が全体として保護されるべきものであるとしている。これは、実効的なデータ保護は、様々な基本権が保護されてはじめて保障されうるという事情も考慮に入れたものである[30]。

欧州の基本権の観点からすれば、GDPR は、特に EU 基本権憲章 7 条および 8 条を実現している[31]。関連する憲法上の立場を保護するというデータ保護法の目標は、データ保護法を特徴づける諸原理（保護の領域原理、目的拘束の原則、データ最小化の原則、責任あるデータ取扱いの原則）によっても明確

[27] So etwa bei der automatischen Kennzeichenerfassung BVerfGE 150, 244 Rn. 37.
[28] BVerfGE 65, 1 (45).
[29] BVerfGE 152, 152 Rn. 91.
[30] *Hornung/Spiecker gen. Döhmann*, in: Simitis/Hornung/Spiecker, gen. Döhmann (Hrsg.), Datenschutzrecht, 1. Aufl. 2019, Art. 1 Rn. 36.
[31] Hinsichtlich weiterer relevanter Grundrechte *Buchner*, in: Kühling/Buchner, 3. Aufl. 2020, Art. 1 Rn. 13 f.

化される[32]。これらの諸原則は、基本権的地位への介入を必要不可欠なものに限定し、データ取得の場合でも、諸利益にかなった方法でのデータの取扱いを保障しようとするものである。つまりこの点で、データ保護に関する諸原則によって、データ対象者の基本権保護は最大化される。

GDPR の開放条項および詳細化条項の場合や刑事司法指令の国内法化において引き続き重要である憲法の観点からすると、連邦データ保護法は、特にデータ処理の法的根拠の十分な特定性に関して、また同時に基本法 10 条および 13 条の保護のためにも、情報自己決定権が単純法律上で具現化されたものである。このとき、同意（GDPR6 条 1 項 a、7 条）は、情報的自己決定が特に表出したものであるが（同意については後述）、まさに公的機関によるデータ処理の場合、自発性が欠如している可能性があるため、議論の的となっている。通知義務は、とりわけ間接的な取得の場合に重要な役割を果たす。通知義務によって、データ対象者に「誰が自分について何を知っているか」[33]ということの情報が提供されることで（より早い段階での）自己決定を実現し、データ対象者にはじめて自己の権利を保護する機会を与える（通知義務については後述する）。

[32] Siehe dazu etwa *Wolff*, in: BeckOK Datenschutzrecht, Stand 01.11.2021, Einl. Rn. 6 ff.
[33] BVerfGE 65, 1 (42).

III. スイス

Florent Thouvenin（チューリッヒ大学法学部教授）
Samuel Mätzler（(チューリッヒ大学大学院博士課程、スイス弁護士）

質問項目

1. 憲法と個人情報保護制度との関係性

①プライバシー権ないし情報自己決定権の憲法上の位置づけ

プライバシー権ないし情報自己決定権が、憲法上（条文または判例上）保障されているかどうか。またその際、プライバシー権と情報自己決定権との異同が意識されているかどうか。

***

回答：

プライバシー権はスイス連邦憲法 13 条（1）（以下「Cst.」）により保護されている。同号では、「すべての人は、私生活、家庭生活、郵便および電気通信に関するプライバシーの権利を有する」と明記している。

情報自己決定権は、Cst.13 条（2）により保護されている。直接的に明記されてはいないものの、スイス連邦最高裁判所（以下「FSC」）によりそのように認識されている。Cst.13 条（2）は、「すべての人は、個人データの悪用から保護される権利を有する」と明記している。そのため、情報自己決定権は Cst.13 条（1）で明記されているプライバシー権全般のサブセットなのである。特筆すべき点として、Cst.13 条（2）は FSC と法理の一部により、同規定は個人データの*悪用*に対して保護するだけでなく、情報自己決定権も提供していると広範に解釈されている。FSC は、憲法による情報自己決定権は「原則として、問題となっている情報の実際の機密性の高さにかかわらず、連邦政府機関や民間人による個人情報の処理に関して、すべての人が、そのデータがどのような目的で処理されるかを判断できなければならない」ことを保障するものであると一貫して判示している（FSC 判決 147 I 280、約因 7.1 を参照、英文は筆者が翻訳）。

したがって、FSC は Cst.13 条（2）には情報自己決定権が含まれていると明記していると同時に、情報自己決定権を非常に広義に解釈している。ただし、この見解は法理の一部により否定されており、スイスの連邦機関は適法性の原則に拘束されているため、個人データの処理を行う法的根拠が存在する場合のみしかそのような処理を行えない。連邦機関による個人データの処理は常に法的根拠に基づいているため、これらの機関がそのような処理についてデータ主体の同意を要求する必要はない。その結果、データ主体には、連邦機関による彼らの個人データの処理について決定する権利がない。結局のところ、連邦機関に関連して言えば、情報自己決定権は存在しない。

民間団体による個人データの処理については状況が異なる。これらは全体的に、透明性、利用目的制限、比例性などといったデータ保護の原則に準拠している限り、個人データを処理することが許可されている。GDPR とは対照的に、DPA は、禁止対象となる個人データの処理に関する一般的許可に基づいている。データ保護の原則に対する違反が生じた場合、民間団体は同意を求めること、処理に優先的な利益があることを請求、またはそのような処理を許容する法的根拠を参照することで処理を正当化しなければならない（詳しくは下記を参照）。その結果、ほとんどの場合、民間団体がデータ主体の同意を取得する必要はない。それ故に、情報自己決定権については中身がほとんど残されていない。

***

② 個人情報保護制度の憲法上の意義

プライバシー権ないし情報自己決定権が憲法上の権利として保障されている場合、かかる権利が、個人情報保護法の目的規定のなかに読み込まれているかどうか。別言すると、個人情報保護法が、プライバシー権などの憲法的価値を実現する法令として位置付けられているかどうか。

↓

参照：日本の個人情報の保護に関する法律では、目的規定で見られるようにプライバシー権または情報自己決定権の文言に明示的に参照していないものの、GDPR では個人データを保護する権利という憲法に定められている根拠に基づいて制定されていると宣言しており、欧州連合基本権憲章でも基本権として保障されている。

***

回答：

スイス連邦データ保護法（以下「DPA」）はスイスの連邦機関と私人（主に私法人）の両方に適用される。DPA の目的は、「個人データが処理されている自然人の人格と基本権を保護すること」である（DPA1 条）。

しかし、連邦機関と私人の間ではデータ処理に関する具体的な要件が違う。連邦機関とは異なり、私人は一般的に基本権により拘束されていない。しかし、基本権は私人に第三者としての効果も及ぼすことがある。特にデータ保護法では、立法者らには民間団体間の情報自己決定権を考慮した法律を制定する義務がある。このことは、連邦機関と民間団体による個人データの処理を規制する DPA とその規定において行われている。

***

2. 個人情報保護法制の現状と課題

①他国における法制度の影響

個人情報保護法を制定するにあたってモデルとした国はあるか。

***

回答：

1992 年に制定された当初のスイス連邦データ保護法とその起源には、スイスの DPA のモデルとなった特定国への明示的な参照は含まれていない。しかし、その準備はドイツ、フランス、およびオーストリアにおけるデータ保護法の制定後間もなく始まっており、スイスの DPA はこれらの国々の法律による影響を受けていると考えて差し支えない。ただし、FSC はドイツ連邦憲法裁判所（以下「FCC」）によるいわゆる「Volkszählungsurteil」判決を明示的に参照しており、前述の判決においてドイツの FCC が推論した情報自己決定権を認めている。

最近改訂され、2023 年 9 月 1 日に発効した 2020 年 DPA は、欧州連合の一般データ保護規則（以下「GDPR」）と、欧州評議会の個人データの自動処理に係る個人の保護に関する条約（ETS 第 108 号）を改正する議定書（以下「改正議定書」）による多大な影響を受けている。改訂は、スイスが GDPR45 条の意味の範疇における十分な保護レベルを保証する国家として認められ続けられるよう GDPR との調和を目指すものであった。また、改訂はスイス法と改正議定書の互換性を保証し、後者の署名と批准も目指していた。

***

②<u>「個人データ」の定義と範囲</u>

クッキー情報は個人情報保護法制における「個人データ（個人情報）」のなかに含まれているか。個人情報保護法上保護の対象となる「個人データ（個人情報）」の定義。

↓

GDPR では、「『個人データ』とは、特定された、または識別可能な自然人（「データ主体」）に関するあらゆる情報を意味し、識別可能な自然人とは、特に氏名、識別番号、位置情報、オンライン識別子などの識別子、または当該自然人の身体的、生理的、遺伝的、精神的、経済的、文化的もしくは社会的アイデンティティに固有の 1 つもしくは複数の要素を参照することによって、直接的または間接的に識別することができる者をいう」としている。対照的に、日本の個人情報の保護に関する法律は、個人情報の範囲を GDPR よりも狭く定義し、同法における個人情報は「特定の個人を識別できる」情報であるとしている。そのため、原則として、ある情報が個人情報のカテゴリに分類されるためには*特定*の人の*識別可能性*が厳密に必要であるため、クッキー情報そのものは個人情報を構成するものではない。この規制体制は、効果的なプロファイリング規制を妨げる要因として批判されている。

***

<u>回答：</u>

スイスの DPA では個人データを GDPR と同様に定義し、「特定された、または識別可能な自然人に関連するすべての情報」としている（DPA5 条（5））。GDPR の下では、人は管理者が手に入れることが可能な（その他の）データの組み合わせが不合理な努力なしに人の特定に繋がる場合に識別可能であると見なされる。

そのため、スイス法では、クッキーやその他のオンライン上の識別子も個人データとして扱われる。スイス電気通信法（以下「TCA」）ではさらに、電気通信的な方法を用いた送信手段による外部機器上でのデータ処理は、利用者が処理やその目的、ならびにそのような処理を拒否する権利について知らされる場合のみに許可されるものであると規定している（TCA45c 条（b））。この規定は、クッキーのユーザーにも当てはまる。

***

③ データ主体の権利と事業者の義務

a）利用停止請求権の範囲（例えば GDPR 第 17 条）

***

回答：

DPA32 条（2）は、人格権の保護に関連する行為がスイス民法典（以下「CC」）により統治されていると明記している。特に、DPA32 条（2）（c）では、請求者が個人データの削除または破棄を要求できると明記している。GDPR とは対照的に、削除権は人格権の侵害に対する救済措置として設計されており、そのためデータ主体がいつでも主張できる権利として解釈されしていない。その結果、スイスにおける個人データの削除権は一般的人格権に沿って存在しているものの、ケースバイケースで優先される利益を検討しなくてはならない。

***

民法に基づく人格権または削除権と DPA の規定の間には相関があるか？例えば、データ管理者が同意または目的拘束に関する DPA の規定に違反する場合、削除の要求は民法典の下で認められるか？消去または削除の要求が認められる条件について、ご教示いただきたい。

***

回答：

DPA はデータ主体の人格を保護することを目指していることから、民法における人格の保護とデータ保護法の間には密接な相関がある。さらに、DPA では、DPA に違反した場合にデータ主体が援用できる救済措置として CC の規定を参照している。

DPA は CC の規定を直接参照していることから、削除の要求は CC の下で与えられている。加えて、DPA32 条 2 項 c 号では、援用できる救済措置の一つとして削除の権利に明示的に言及している。DPA の規定に対する違反、特に DPA6 条で定められているデータ保護の原則への違反は、データ主体の人格の侵害を構成する。そのような違反は、正当化できる場合を除き違法である（詳しくは下記を参照）。データ主体の不法な人格侵害が生じた場合、CC による救済措置が利用可能である。特に、データ主体は法的措置を通じて人格侵害を停止するよう要求できる（CC28 条 *a*（1）（2））。さらに、データ主体は、削除権などの DPA で明示的に言及されている救済措置も援用できる。削除の要求が許可されるかどうかは、管轄民事裁判所による判決による。そのような要求は、不法な人格侵害が単に差し迫っているだけではなく現在発生しており、決定の時点で継続している場合のみに認められる。

***

b) 同意の位置付け（オプトイン方式かオプトアウト方式か）。本人の同意が要求される場面は。事業者が個人データを取得する場合に当該個人の同意を得ることが義務付けられているかどうか。また、個人データが第三者に提供される場合、当該個人の同意を得ることが義務付けられているかどうか。

***

回答：

GDPR の下におけるデータ処理は許可の留保を伴う一般的禁止の上に成立しているのに対し（GDPR6 条（1）を参照：「処理は以下の事項が一つ以上該当する場合のみ、その限りにおいて適法であること（…）」）、DPA の下における処理は禁止留保を伴う一般的許可の上に成立している。DPA30 条（1）では、「個人データを処理する者はデータ主体の人格を違法に侵害してはならない」と明記している。したがって、私人はデータ保護の原則に準拠している限り個人データを一般的に処理してもよい。例えば、処理は誠実に実施され、比例的であり、具体的な目的のみのために収集されなければならない（目的の制限）。これらの原則に違反する形でデータが処理される場合、そのような行為はデータ主体の人格を侵害するものと見なされる（DPA30 条（2）（a））。

そのような侵害は、（1）データ主体の同意、（2）データ主体の利益を上回る私的または公共の利益、または（3）制定法により正当化される場合を除き違法である（DPA31 条（1））。データ主体の利益を上回る管理者の利益の例は DPA31 条（2）に明記されている。その結果、事業は、例えば契約の履行の締結と直接関係して契約当事者の個人データを処理することについて契約当事者の利益を上回る私益があることを主張し（DPA31 条（2）（a））、したがってこれらのデータを処理するにあたり同意を取得することが求められない可能性がある。

個人データの処理が同意により正当化される場合、自由であり、具体的で、十分な情報に基づいており、明確である同意を根拠に実施されなければならない（『個人データ処理に係る個人保護の現代化した条』5 条（2）を参照）。しかし、明示的な同意が必要となる機微な個人データを処理する場合を除けば、一般的に暗黙の同意で十分である（DPA6 条（7）（a））。この点に関して、データ処理に対する意図の明示的な宣言も、人格侵害を構成するものであると付け加えることができ（DPA30 条（2）（b）を参照）、これは後で正当化されなければならない。そのため、一般的に、オプトアウトの可能性も存在している。

したがって、事業は、個人データを取得・処理する際はデータ主体から同意を定期的に取得する必要はない。むしろ、他の方法により個人データの処理を正当化できるのである（主にデータ主体の利益を上回る利益を根拠とする）。スイス企業データ保護協会が 2022 年～2023 年の冬に実施した（いささか非公式な）アンケートでは、参加企業 45 社によるデータ処理のうち同意に基づいていたのは約 15%程度でしかなかったことが明らかになっている。残りの 85%は、データ主体の利益を上回る利益または法的根拠などの他の正当な理由に基づいている、あるいは処理がデータ保護の原則に準拠していることから正当化が必要ないものであった。

個人データが第三者に提供される場合は同意は必要ではないが、情報開示義務（duty of information）の一環として、個人データの受領者または受領者カテゴリはデータを収集する時点で公開されなければならない。

***

c) ＜通知＝同意＞モデルの限界とその対策。プライバシー法の権威であるダニエル・J・ソロブは、データ保護法におけるプライバシー自己管理モデルの限界を次のように指摘している。「米国の個人情報保護法は、人々が自分のデータの管理方法について決定できるようにするための一連の権利を提供している。これらの権利は、主に個人データの収集、利用、開示に関する通知、アクセス、同意の権利により構成される。この一連の権利の目的は、人々が自分の個人データを管理できるようにすることである。

_...実証的・社会科学的研究が示すように、認知の問題は、個人データの収集、利用、開示への同意に伴うコストと利益について、十分な情報を得た上で合理的な選択をする個人の能力を損なう。」
そのため、個人の認知限界という観点から＜通知＝同意＞モデルの限界（同意疲れやプライバシーポリシーの流し読み）が予てから指摘されている。こうした課題に対して、各国の個人情報保護法制がどのように対応しているか（事業者に対して実効的な告知方法を義務付けるなど）。

***

回答：

DPA の執行は、主に調査を開始する権限を有する連邦データ保護情報コミッショナー（以下「FDPIC」または「コミッショナー」）が主に実行している（下記を参照）。このような形で、スイスの DPA では、専任の第三者に委ねることでプライバシーの自己管理モデルの限界に起因する課題に部分的に対処できていいる。ただし、DPA は、データ主体が合理的な選択をするという前提に基づいている。したがって、DPA はこれらの課題に説得力を持って対処できていない。DPA は、同意が一つ以上の具体的な処理活動に対して十分な情報を得た後に自由に与えられている場合のみに妥当であることを単に規定しているに過ぎない。機微な個人データが私人により処理またはプロファイリングされることが高リスクである場合、または連邦機関がプロファイリングを実施している場合、同意は明示的に与えられていなければならない（DPA6 条（7））。

***

d) 情報銀行や PDS（Personal Data Store）のように、パーソナル・データに対する本人の controllability を補助するための仕組みや制度はどのように社会実装されているか。

***

回答：

スイスにおける人による個人データの controllability を支援するプロジェクトは立ち上げられているものの、いずれも現時点では確立されておらず、（幅広く）活用されるには至っていない。

***

e) AI の利活用やプロファイリングの場面に特化したデータ保護の仕組みが存在するかどうか（GDPR 第 21 条）。

***

回答：

DPA のプロファイリングについては、いくつかの具体的な規制が設けられている。上述のとおり、プロファイリングが「高リスク」であると見なされる場合、明示的に同意が与えられる必要がある（DPA6 条（7）（b））。

(b) しかし、これは、同意が正当化スキームに関して求められる場合のみに適用される（上記を参照）。高リスク・プロファイリングとは、データ主体の人格または基本権に対し高いいリスクを伴うプロファイリングであり、自然人の人格の根本的な側面の評価を可能にするデータのペアリングを生み出してしまう（DPA5 条（g））。そのような場合、データ主体の人格または基本権に対するリスクが高いことから、データ保護影響評価が必須となる（DPA22 条（1））。

また、明示的な同意は連邦機関が実施するプロファイリングにおいても求められる（DPA6 条（7）（c））。

連邦機関によるそのようなプロファイリングについては、法的根拠となる正式な法律が存在しなければならない（DPA34 条（2）（b））。

***

f) データ・ポータビリティ権は保障されているか（例えば GDPR 第 20 条）。

***

回答：

データ・ポータビリティ権は 2020 年の改訂に伴い追加された。DPA28 条は GDPR に基づいており、GDPR20 条と密接に整合している。DPA28 条（1）によると、データが自動的に処理されており、データ主体の同意の下、または管理者とデータ主体の契約の締結または履行と直接関係して管理者に標準的な電子形式で開示した個人データを開示するよう、誰もが当該管理者に無償で要求できる。GDPR20 条（2）と同様に、DPA でも、一般要件が満たされており、データ移転に不相応な努力が伴わない限り、データ主体が管理者に別の管理者に直接個人データを移転するよう要求できる（DPA28 条（2））。

DPA29 条ではさらに、関連する条件が満たされた場合にデータ・ポータビリティ権に課せられる潜在的な制約を見越している。

***

またこの権利は具体的にどのような場面で社会実装されているか。

***

回答：

改訂版 DPA が 2023 年 9 月 1 日に発効したばかりなので、まだ何も言えない。***

④個人情報保護法を執行する監督機関の組織と権限（制裁や告訴の仕組み）。

***

回答：

FDPIC は DPA に基づいて監督機関となっている（DPA43 条 et seqq）。機関長はスイス国会により任命され、4 年間の任期の間に他の当局とは独立した職務を遂行する（DPA43 条（4）および 44 条（1））。

コミッショナーは、データ処理がデータ保護規則に違反していることが十分に示されている場合に、連邦機関または私人に対して調査を開始することがある（DPA49 条（1））。連邦機関または私人は DPIC にすべての情報を提供し、調査に必要なすべての文書を用意することが求められる（DPA49 条（3））。応じしない場合は、FDPIC が調査、構内や施設への立ち入り、証言者の尋問、専門家による評価の命令に必要なすべての情報や文書にアクセスすることがある（DPA50 条（1））。

行政措置により、FDPIC は、データ保護規則の違反が認められた場合、データの処理を完全または部分的に調整、延期、または停止し、個人データを完全または部分的に削除または破棄するようさらに命令できる（DPA51 条（1））。コミッショナーはさらに、外国へのデータ移転に関する規定が侵害された場合、外国への移転を延期または禁止することもある（DPA51 条（2））。

また、FDPIC は連邦機関と私人の両方に通知、訓練、および助言を行い、国民の意識を高め、人々に権利を行使する方法に関する情報を提供し、連邦法の草案について意見を提供する（DPA58 条（1））。

DPA の下では制裁は行政犯罪ではなく刑事犯罪として設計されている。GDPR の場合とは異なり、制裁は個人を対象としている

（例えば、事業そのものではなく事業の従業員）。罰金は GDPR のそれよりも少ないものの、罰金は（大）企業が織り込むことができず、従業員には罰金や刑事手続きに直面し、その結果犯罪歴に至るという可能性を避けるという強力なインセンティブが働くことから、その影響は GDPR の罰金よりも強力であると考えられる。訴訟法に関しては、DPA に基づいた犯罪行為の訴追や判決については、スイスの一般的な刑事法沿ってカントンが責任を負う。

DPA60 条（1）は、私人が情報開示義務やアクセス権に関する義務に違反した場合、最大 25 万スイスフラン（約 4200 万円）までの罰金について刑事責任を負うと規定している。私人は、データ主体に個人データの収集または自動化された個人の意思決定について適切に知らせなかった場合、データ主体が DPA19 条（2）に定められている権利を主張するために必要なすべての情報を故意に提供しなかった場合にはさらに責任が問われる。これらの責任は、苦情が提出された場合のみ適用される。

また、私人は調査の過程で FDPIC に故意に虚偽の情報を提供した場合、または協力することを拒否した場合、最大 25 万スイスフランの罰金を科せられる。

加えて、DPA61 条では善管注意義務に違反した場合の罰金を最大 25 万スイスフランとすると規定している。私人は DPA の他の規定に違反して国外で個人データを故意に公開した場合、DPA の関連する規定に準拠していることを保証せずにデータ処理を処理者に委託した場合、または最低のデータセキュリティ要件を遵守することを怠った場合にも責任を負う。

さらに、DPA62 条によると、私人は職業上の守秘義務に故意に違反した場合にも、告訴により最大 25 万スイスフランの罰金が科せられる。最後に、DPA63 条では、FDPIC または上訴機関が下した（DPA63 条の刑事罰への参照を含む）決定について私人が故意に従わなかった場合に同じ罰金が科せられると明記している。これらの法律の法的制限は 5 年間である（DPA66 条）。

***

⑤<u>司法的救済の仕組み（訴訟要件、集団訴訟の可能性）</u>

***

<u>回答：</u>

個人データが私人により処理される場合、データ主体は一般的に、誤ったデータの修正を要求できる（DPA32 条（1））。データ主体の人格の保護に関連する他の行為については、DPA は関連する条項が盛り込まれている CC を参照する。

特に、請求者は特定のデータ処理を禁止すること、第三者に対する特定の個人データの公開を禁止すること、個人データを削除または破棄することなどの要求を行う可能性がある（DPA32 条（2））。司法手続きは、管理者、処理者、または補助者など、人格権の侵害を引き起こす当事者に対して行うことができる。

民間団体間での司法手続きの場合はスイス民事訴訟法が適用される。データ主体は管理者に対する訴訟権を有し、いずれかの当事者の住所地または登録事務所の裁判所において訴訟を提起することができる。実質的および機能的管轄権は各カントンの法律に準拠する。

個人データが連邦機関により処理される場合、その手続きは行政手続きに関する連邦法の一般規定に準拠する（DPA41 条（6）参照）。担当の連邦機関に（1）違法な個人情報の処理を行わないこと、（2）違法な処理の結果を排除すること、または（3）処理の違法性を確認することを要求する者は、連邦機関から裁定を受ける権利を有する（DPA41 条（1）参照）。裁定はその後に連邦行政裁判所（以下「FAC」）、そして最終的には FSC に上訴して争うことができる。

FDPIC による調査も FDPIC の裁定に至る。彼らも FAC への上訴して争うことが可能である。データ主体は調査の当事者ではないものの、調査結果について FDPIC により知らされなければならない（DPA49 条（4））。***

⑥GDPR9 条（2）（g）では、「自然人及び健康に関するデータを一意に識別する目的での遺伝子データ、生体認証データの処理」が、追求される目的に釣り合うものでなければならず、データ保護の権利の本質を尊重し、データ主体の基本権および利益を保護するための適切かつ具体的な措置を提供しなければならない連邦法または加盟国の法律に基づき、実質的な公共の利益のために必要」であれば許容されることを規定している。
この条項と、研究目的での診療データの活用の関係性について、質問がある。
診療記録等を医薬品開発などの研究目的で利用する場合に、データ主体である患者の同意は要請されるのか。診療データを二次利用するにあたって、匿名加工などの一定の義務が課せられるか？ 欧州保健データスペース（EHDP）における最近の動向についてもご教示いただきたい。

***

回答：

スイスの法律では、研究目的や医薬品開発のために患者の医療記録や生体認証データを利用することは、ヒト研究法（以下「HRA」）の範囲に含まれることが多い。HRA は、ヒトの疾病および／またはヒトの身体の構造および機能に関するすべての研究に適用され、*特に*そのような目的のために健康関連の個人データを利用することが含まれる（HRA2 条(1) (e)）。HRA の範囲に含まれる研究の場合、健康関連個人情報の（第一次）収集にはインフォームド・コンセントが必要である（HRA16 条等）。従って、書面によりインフォームド・コンセントを与えた場合のみ研究プロジェクトに参加できる。正当なインフォームド・コンセントを受けるためには、（i）研究プロジェクトの性質、目的、期間、手続き、（ii）予測されるリスクと負担、（iii）特に自分自身や他の人々にとって研究プロジェクトから期待される利益、(iv) 収集された個人データを保護するための措置、および (v) 自分の権利について、理解しやすい口頭および書面による情報を受けなければならない（HRA16 条（2））。関係者は、同意するかどうかを決定する前に、適切な熟慮期間を与えられなければならない（HRA16 条（3））。さらに、いかなる研究プロジェクトも、担当の倫理委員会の認可を受けなければならない（HRA45 条（1）（a））。

遺伝子データ（及び生物試料）の更なる（二次）利用には特別な規則が適用される。これらの資料やデータは、関係者のインフォームド・コンセントがあれば、特定の研究プロジェクトのためにコード化されていない形で利用できる（HRA32 条（1））。さらに、関係者のインフォームド・コンセントがあれば、コード化された（すなわち仮名化された）形で研究目的全般に利用できる（HRA32 条（2））。さらに、生物試料および遺伝学的データは、関係者が事前に知らされ、匿名化に反対していなければ、研究目的のために匿名化できる。匿名化されている場合、生物試料と遺伝子データは HRA または DPA の適用範囲から外れる。

同様のカスケードは遺伝子以外の健康関連の個人データについても存在する。これらのデータは、関係者によりインフォームドコンセントが与えられていれば、一般的に研究目的でコード化されていない形でさらに利用できる（HRA33 条（1））。

コード化（すなわち仮名化）された形の場合、関係者が反対していないのであればデータをさらに利用できる（HRA33 条（2））。匿名で収集されたデータ、または匿名化されたデータは HRA の適用範囲外（HRA2 条（2）（c）を参照）であることから、そのようなデータのさらなる利用は制限なく許可されるものである。

加えて、HRA34 条には、次の三つの条件を満たしているのであれば、データ主体の同意なく生物試料や健康関連の個人データを研究目的で処理することを許容する例外条項が含まれている。第一に、同意を取得すること又は反対する権利について情報を提供することが不可能又は不相応に困難でなければならない。これは、関係者に過度な負担を課しうる場合にも適用される。第二に、文書化された拒否が入手可能であってはならない。第三に、研究の実施に関する利害は、データ主体の生物試料または健康関連の個人データのさらなる利用の決定に際する関係者の利害を上回るものでなくてはならない。HRA34 条は例外的な場合のみを想定して設計されているものの、実際には規則になっている。

スイスでは、今のところ欧州保健データスペースに参加する予定はない。しかし、スイス議会は、スイス連邦参事会がヘルスケアなどの戦略的に関連する領域におけるデータの二次利用について枠組み法を制定することを義務付けている。そのような法律の案が 2024 年または 2025 年までに提出されることは想定されていない。

***

免責条項：英語はスイスの公用語ではないため、DPA の文言は https://datenrecht.ch/gesetzestexte/ndsg-en/の非公式の翻訳から引用している。

***

※本研究は、JST【ムーンショット型研究開発事業】グラント番号【JPMJMS2293】の支援を受けたものです。

IV. フランス

小川有希子（帝京大学）

1. 個人情報保護法制と憲法的価値の実現

（1） 情報プライバシー権

フランスは、1978 年に制定した「情報処理、ファイル及び自由に関する 1978 年 1 月 6 日の法律第 78-17 号（Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés）」（以下、「情報と自由法」という）によって、国のデータ保護機関 CNIL（Commission Nationale de l'Informatique et des Libertés、情報処理と自由に関する国家委員会）を創設し、中央集権型の個人情報保護を図ってきた。本法律の起草時点において、既に、フランス国内だけではなく、先進諸国において多くの大規模データベースが実際に運用されていた。かかる状況に鑑み、市民の私生活の秘密（le secret de la vie privée）を保護するために、諸情報へのアクセス条件を厳格に規制する目的で、本法律が制定された[1]。

フランスでは、いわゆるプライバシー権は、私生活の尊重を受ける権利（droit au respect de la vie privée）として保障される。もともとは、ヨーロッパ人権条約 8 条を具体化するために、「すべての人は私生活を尊重される権利を有する」と規定する民法 9 条（loi n° 70-643 du 17 juillet 1970）として法制化され、以来、法律上の権利として司法裁判所によって保護されていた。1999 年の 2 つの憲法院判決[2]が、私生活の尊重を 1789 年人権宣言 2 条に根拠づけたことで、憲法上の権利としての位置づけが明確になったとされている。なお、1958 年のフランス第五共和国憲法は、私生活の尊重を受ける権利に関する直接的な規定を置いていない。

私生活の尊重を受ける権利の内容は、未だ発展途上にあるが、一般に、私生活の尊重は、私生活の秘密（住居、自動車、通信、個人情報等）と、私生活の自由（自己決定権や社会生活上のつながり）とに分けられ、憲法院判決にみられるのは主として前者の側面に限定されている[3]。

個人データの保護と私生活の尊重との関係については、2012 年の憲法院判決[4]は、「個人

---

[1] Texte n° 1004 (1973-1974) de M. Pierre-Bernard COUSTE, déposé à l'Assemblée Nationale le 4 avril 1974, Proposition de loi tendant à créer une Commission de contrôle des moyens d'informatique afin d'assurer la protection de la vie privée et des libertés individuelles des citoyens.

[2] Décision n° 99-419 DC du 9 novembre 1999（齊藤笑美子「婚姻外カップル立法化の合憲性―パックス（PaCS）判決」フランス憲法判例研究会編『フランスの憲法判例 II』91-94 頁）, Décision n° 99-422 DC du 21 décembre 1999.

[3] 馬場里美「私生活の尊重」同書 87-90 頁

[4] パスポート作成時の個人情報処理に際する指紋や目の色等の生体認証データの取得について規定するアイデンティティの保護に関する法律について、法律審署前に憲法適合性が争われた事案。Décision n° 2012-652 DC du 22 mars 2012.

データの収集、記録、保存、閲覧および通信」が私生活の尊重への権利に対する制約にあたることを前提に、当該処理が、「一般利益（intérêt général）によって正当化され、その目的に適切かつ比例した方法で実施されなければならない」と判示した。

（２）　情報自己決定権

情報自己決定権（le droit à « l'autodétermination informationnelle »）は、フランス憲法（憲法ブロック）に明文の規定はなく、憲法院も未だ憲法上の権利として真正面から承認しているものではないが、今日、実定法上の概念としては、「すべての人は、この法律に定める条件の下で、自分に関する個人データの使用を決定し及び管理する権利を有する」と規定する2016年10月7日のいわゆる「デジタル共和国法」(loi n° 2016-1321 du 7 octobre 2016 pour une République numérique）54条にあらわれている。この規定は、1983年12月15日のドイツ連邦憲法裁判所判決（国勢調査法判決（1983年12月15日：BVerfGE 65, 1 ））の影響を受け、政府提出法律案の最初の段階から提案されていた[5]。法律案に付された影響評価書によれば、自分のデータを自由に処分する権利（le droit à la libre disposition de ses données）ないしは〔自分の〕個人データ自由処分の原則（principe de libre disposition de ses données）の実現は、個人データ保護の新たな局面として認識されている。すなわち、単なる私生活の保護から、オンライン上の生活をコントロールしようとする個々人の保護へと、新しいパラダイムが提示された。アクセス権やデータポータビリティ権は、後者の権利として位置づけられる。他方で、データ処理が、デジタル共和国法や、後に言及する2018年の「個人データの保護に関する法律」等、法令の規定に従ってなされる場合、個人の自己決定よりも、悪用を避けるためにデータ管理者に課される条件が重視されており、情報自己決定権の主観的権利としての保障は十分には達成されていない、との指摘もある[6]。

2.　個人情報保護法制の現状と課題

（１）　1978年「情報と自由法」制定

フランスが、1978年に、情報と自由法（Loi Informatique et Libertés :LIL）[7]を制定し、データ保護機関CNILを創設するに至った大きなきっかけは、Safari事件であった。フランスでは、出生時に、フランス国立統計経済研究所（Institut National de la Statistique et des Études Économiques : INSEE）によって割り当てられる個人台帳登録番号（Numéro d'Inscription au Répertoire :NIR）が、全国個人識別台帳（Répertoire National d'Identification

---

[5] 政府提出法律案に付された影響評価書（Étude d'impact）96-97頁および立法理由（ecposé des motifs）参照

[6] Audrey BACHERT-PERETTI, « France », *Annuaire international de justice constitutionnelle (2021),* ECONOMICA/PUAM, 2022, pp. 324.

[7] 正式名称は、情報処理、ファイル及び自由に関する1978年1月6日の法律第78-17号（Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés）

des Personnes Physiques : RNIPP）に登録される。ジョルジュ・ポンピドゥ政権下のフランス政府は、警察署や行政機関など 400 以上の組織で分散して保有している 1 億近くの全ファイル（état-civil、租税、地籍台帳、健康データなど）を、国民に付与された単一の強制識別子（NIR）を用いて相互接続し、内務省（内務大臣ジャック・シラク）において一元管理する計画――Safari（Systeme Automatise pour les Fichiers Administratifs et le Repertoire des Individus、行政ファイルと個人台帳の自動システム）計画――を予定していたところ、1974 年 3 月 21 日のル・モンド紙が、「« Safari » あるいはフランス人狩り」という挑発的な見出しをつけて、この計画を暴露した[8]。これを受けて、ピエール・メスメル首相の同年 3 月 29 日付け通達により、予防措置として、異なる省庁に属する情報システム間の新たな相互接続が禁止され、1974 年 11 月 8 日のデクレにより、国務院副院長のベルナール・シュノと破毀院初代院長のモーリス・アイダロを委員長とする情報と自由委員会が設立された。この委員会は、政府当局による IT ツールの使用に関する規制についての検討を目的とするもので、総報告者の名前にちなんで命名されたトリコ報告書が、1975 年 6 月 27 日、首相に提出され、1977 年 11 月に、のちに情報と自由法となる法案に関する議会審議が開始された[9]。

情報と自由法制定に際しては、スウェーデンのデータ保護法（1973 年）、アメリカのプライバシー法（1974 年）、ドイツのヘッセン州データ保護法（1970 年 10 月 7 日）など、既に個人データ保護に関する法制を有する諸国の例のほか、イギリスの政府データベース創設に関する法律や私人の秘密の自由の保護に関する法律など、成立には至らなかった法案や政策も広く参照されている[10]。IT 技術の進展に伴って、こと先進国の公的機関が大規模なデータベースを保有し始めるなか、データ保護法の整備が急務として認識されるようになり、フランスもその潮流のなかで本法制定に至ったものである。

1978 年法によって設置された CNIL が、フランスで初めて「独立行政機関」としての法的性格を付与されたという事実は、SAFARI 事件を契機に露呈した公的機関による IT 利用の危険性と、公的機関から独立した組織設立の必要性の証左ともいえよう。行政機関による大規模な集中情報システムの実装に対応して、国民に新たな権利を認めることは、情報と自由法制定の最大の目的であった[11]。1978 年法のその先駆的な性格は、第 108 号条約として

---

[8] « Safari » ou la chasse aux Français, Le monde, 21 mars 1974, https://www.cnil.fr/sites/default/files/atoms/files/le_monde_0.pdf （最終閲覧日：2023 年 9 月 24 日）

[9] Audrey BACHERT-PERETTI, « France », *Annuaire international de justice constitutionnelle (2021),* ECONOMICA/PUAM, 2022, pp. 314.

[10] Texte n° 1004 (1973-1974) de M. Pierre-Bernard COUSTE, déposé à l'Assemblée Nationale le 4 avril 1974.

[11] もっとも、情報と自由委員会は、「公共、半公共及び民間の各部門における IT の発展が、私生活、個人の自由及び公的自由を尊重して行われることを保証する措置を政府に提案する」（1974 年のデクレ第 1 条）ことをその任務としており、当初から、公共部門と民間部門に同一の法律を適用することを想定していた点は、諸外国との比較において際立った特徴といえる。

知られる、個人データの自動処理に関する個人の保護に関する条約に大きな影響を与えたと評されている[12]。

なお、NIR は、社会保障の分野で利用されてきた経緯があり、社会保障番号とも呼ばれているが、今日、NIR を税、教育、警察など、他の行政サービスに関するファイルと統合して管理することは認められておらず、セクターごとに ID が割り当てられている[13]。ファイルの相互接続や個人情報の利用が、それが正当化される目的以外の目的でなされることを回避するために、CNIL は統一番号の使用には一貫して否定的な立場を示しており、SAFARI 計画への反動として CNIL が設置されたことを踏まえると、フランスは、「日本のような“統一番号制”は絶対に採用しない」ことが確実とも評されている[14]。2019 年には、「加盟国は、国民識別番号又はそれ以外の一般に利用されている識別子の取扱いのための特別の条件を別に定めることができる」と規定する EU 一般データ保護規則（以下、「GDPR」という）87 条を受けて、NIR の利用目的を制限するデクレ（Décret n° 2019-341 du 19 avril 2019、通称 « cadre NIR »）が制定された。« cadre NIR »では、社会保護、健康、雇用、租税、裁判、統計・国政調査、教育の分野ごとに NIR の利用が可能な目的を限定列挙し、これに該当しない目的での NIR 利用は禁止している。

（２） 2018 年「個人データの保護に関する法律」による「情報と自由法」改正

2016 年、GDPR（GDPR の立法過程については、第 8 章 II 参照）が採択されたことを受け、フランスは、GDPR に準拠する国内法の整備を迫られた。GDPR は「規則」である以上、加盟国の国内法に優先して、加盟国の政府や企業、個人等に直接適用される性質を有する。他方、規則には、その実施にあたり加盟国に判断・裁量の「余地」を認める部分が多かれ少なかれ存在するのが通例である。GDPR 上の「自然人」（4 条 1 号）に死者が含まれるか、「監督機関」（4 条 21 号、51 条）を新たに創設するのか、既存の機関を当てるのか、

---

[12] Audrey BACHERT-PERETTI, op.cit., p. 314.

[13] 個人 ID 管理のモデルをセパレートモデル（行政サービス分野ごとに異なる ID を管理し、それぞれの情報は相互に利用できない方式）、フラットモデル（一つの共通 ID を全ての分野で利用し、効率的に情報連携できる方式）、セクトラルモデル（行政サービス分野ごとに ID を管理する一方で、業務別の個別 ID が分野共通 ID と紐付けられ、分野間での情報連携の際には分野共通 ID を他の分野共通 ID に変換して情報を連携する方式）に分類する見解によれば、フランスは、セパレートモデルに分類される。株式会社国際社会経済研究所「国家情報システム（国民 ID）に関する調査研究報告書―英国、フランス、イタリア等における番号制度の現状―」（2011）20 頁 https://www.i-ise.com/jp/report/pdf/rep_it_201010.pdf（最終閲覧日：2023 年 9 月 24 日）、鈴木尊巳「日本がモデルにしたオーストリア電子政府と今後の ID 連携」Fujitsu 68（4）（2017） 80-87 頁 https://www.fujitsu.com/jp/documents/about/resources/publications/magazine/backnumber/vol68-4/paper02.pdf （最終閲覧日：2023 年 9 月 24 日）参照。

[14] 自治体国際化協会「平成 17 年度海外比較調査　各国の電子自治体の推進状況」（2006）77 頁［坂尻昇太担当執筆］

同意年齢を何歳にするか（8 条 1 項)、「削除権（忘れられる権利)」(17 条）や「データポータビリティ権」(20 条）などこれまでの情報と自由法には規定のなかった新しい権利をどう実効的に保障するか、プロファイリング等の自動処理に基づく決定をされない権利に関して加盟国に独自の措置を定めるか（22 条 2 項 (b))、規則違反に対して損害賠償を請求する集団訴訟の可能性（21 世紀に向けた司法の近代化に関する 2016 年 11 月 18 日の法律によって導入した集団訴訟の対象に含むか、その訴訟要件等)、データ処理事業者が従うべきルールの標準化・簡素化（特に、CNIL による許可等の事前手続きの軽減とリスクベースの事後手続きの導入）など、適用条件につき加盟国に選択の「余地」が与えられている 50 以上の部分については国内での議論が強いられた。とりわけ、加盟国に判断の余地が与えられた部分については、加盟国間での調整・調和が求められる。なぜなら、加盟国間で適用するルールやその条件が異なる場合、どのルールが適用されるかは、データ管理者やその下請け業者の所在地によって異なりうるからである。たとえば、同意年齢を 13 歳と定めるスウェーデンの法律は、スウェーデンを所在地とするデータ管理者等に適用されるため、当該データ管理者等がフランス国内において情報提供サービスを行う場合には、たとえフランスが同意年齢を 16 歳に設定していたとしても、フランス居住者はスウェーデンの法律の適用を間接的に受けることになる。なお、法改正に際しては、アイルランドに主要拠点を置く Google と Facebook を念頭に議論が進められた[15]。

（3）　「個人データ」の定義

情報と自由法は、「個人データ」を次のように定義している（第 2 条第 2 項第 1 文)。

個人データとは、識別された自然人又は識別番号若しくはその者に固有の一若しくは複数の要素を参照することによって、直接的または間接的に識別しうる自然人に関するあらゆる情報から構成される。

Cookie は、それ単体では、自然人を識別できないが、他の情報と組み合わせることにより自然人を識別しうるときは「個人データ」にあたる。自然人を識別しうるか否かの判断は、「自然人の識別を可能にするすべての手段又はデータ管理者若しくはその他の者がアクセスしうるすべての手段を考慮に入れなければならない」(同第 2 条第 2 項第 1 文）とされている。Cookie に関しては、情報と自由法 82 条によって、e プライバシー指令を国内法化しており、「個人データ」に該当するか否かに関わらず、同条の適用を受ける。

なお、GDPR の発効を受けて、CNIL が 2019 年に、Web サイト発行者によってユーザーのコンピューターに配置される「Cookie」およびその他のトラッカー接続ファイルに関する新しいガイドラインを策定したところ、さまざまな専門家団体から、ガイドラインの廃止を求める要望書が提出されたことを受け、国務院は、Cookie ウォールを法的に禁止する部分について無効と判断する一方で、Cookie の使用目的の明示、Cookie への同意の拒否ま

[15] Etude d'impact, Projet de loi relatif à la protection des données personnelles, 12 décembre 2017, p.75.

たは撤回の容易さ、Cookie の推奨保持期間など、他の推奨事項の合法性を確認した[16]。

（４）　個人データの処理が合法であるための要件

フランスにおいては、GDPR が直接適用されるため、データ主体の権利と事業者の義務について、基本的には、GDPR と同様のルールが適用される。

個人データの処理（traitements）は、以下に掲げる条件のうち少なくとも一つを満たしている場合に合法とされる（法 5 条）

①処理が、GDPR に規定する個人データ保護制度の対象となる処理にあたる場合は、GDPR4 条 11 号及び 7 条に規定する条件の下で、データ主体の同意を得ている場合

②処理が、データ主体が当事者である契約の履行又はデータ主体の要求に応じてとられる契約前の措置を実行するために必要な場合

③処理が、データ管理者が従うべき法的義務を遵守するために必要な場合

④処理が、データ主体又は他の自然人の重大な利益を保護するために必要な場合

⑤処理が、公共の利益のための役務遂行のために必要又はデータ管理者に与えられた公権力の行使の下で必要な場合

⑥公的機関がその役務を遂行するために行うものを除き、処理が、データ管理者又は第三者が追求する正当な利益の目的に照らして必要な場合。ただし、特にデータ主体が子どもである場合など、個人データの保護を必要とするデータ主体の利益、自由及び基本的権利が優先される場合はこの限りでない。

なお、GDPR8 条 1 項を受けて、フランスは、単独で有効に同意できる年齢を、15 歳としている（法 7-1 条、45 条）[17]。15 歳未満の者は、その親権者（le ou les titulaires）が共同で同意したときにのみ、個人データの処理が有効となる。

（５）　データ主体の権利と事業者の義務

①情報提供を受ける権利（droit à l'information）

GDPR12 条から 14 条に規定する条件の下で行使される（法 48 条 1 項）

---

[16] Conseil d'État n° 434684, lecture du 19 juin 2020.

[17] 同意年齢について、フランス政府案は GDPR に規定する 16 歳を維持していたが、国民議会（下院）では、13 歳を同意年齢とするスペインやチェコ共和国、14 歳とするエストニアなど、独自の選択をしている加盟国の法案がフランス社会に与える影響が考慮され、青少年のインターネット利用の実情、親権者からの同意取得可能性等を検討した上で、最終的には 15 歳を同意年齢とすることになった。なお、実際には、オンライン上で親権者の同意を得るのは簡単ではない。CNIL デジタルイノベーションラボラトリー（Laboratoire d'Innovation Numérique de la CNIL: LINC）では、ゼロ知識証明による「プライバシーを尊重した年齢認証システム」を開発中である。Jérôme Gorin, Martin Biéri et Côme Brocas, Démonstrateur du mécanisme de vérification de l'âge respectueux de la vie privée, 21 juin 2022, https://linc.cnil.fr/demonstrateur-du-mecanisme-de-verification-de-lage-respectueux-de-la-vie-privee（最終閲覧日：2023 年 9 月 24 日）

15 歳未満の者への情報提供は、明確かつわかりやすい言語で提供する（同条第 2 項）

必要な範囲で、情報と自由法 48 条〜56 条に規定する権利を死後に行使することができる（法 85 条）。したがって、死後の個人データの処理についての指示を定める権利についても情報提供を受ける（同条第 3 項）

②アクセス権（droit d'accès）

GDPR15 条に規定する条件の下で行使される（法 49 条 1 項）

個人データの隠匿又は消失のおそれがある場合、裁判官は、略式手続含め、隠匿又は消失を回避しうるあらゆる措置を命ずることができる（同条第 2 項）

ただし、統計の確立又は科学的若しくは歴史的研究の実施のみを目的として必要な期間を超えない期間、関係者のプライバシー及びデータ保護の侵害のリスクを明確に排除する形式で保管される場合並びに国内安全保障法 L. 863-2 条に基づいて専門諜報機関に送信された情報には適用されない（同条第 3 項）

③訂正権（droit de rectification）

GDPR16 条に規定する条件の下で行使される（50 条）

④削除権（droit à l'effacement）

GDPR 1 7 条に規定する条件の下で行使される（法 51 条第 1 項）

データ主体の請求に応じて、特に、当該データ主体が未成年だったときに、データ管理者がサービス提供に関連して収集した個人データは、できる限り早く消去しなければならない。当該データを第三者に送信した場合は、データ管理者は合理的な措置をとるとともに、データ主体から削除請求がなされている旨等を当該第三者に伝えなければならない（同条第 2 項）。

個人データが消去されない場合、又は請求から 1 ヶ月以内にデータ管理者から応答がない場合は、データ主体は、CNIL に苦情（réclamation）を申し立てることができる。CNIL は、苦情の申立てを受けた日から 3 週間以内に判断する。

⑤利用制限権（droit à la limitation du traitement）

GDPR 18 条に規定する条件の下で行使される（法 53 条）

利用制限権については、フランス法に固有の規定は置かれていない。

⑥個人データの訂正若しくは削除又は利用の制限に関する義務の通知

GDPR19 条に規定する条件の下で行使される（法 54 条）

⑦データポータビリティ権（droit à la portabilité des données）

GDPR20 条に規定する条件の下で行使される（法 55 条）

データポータビリティ権については、デジタル共和国法 48 条で規定され、消費法典に編纂されていたが（消費法典第 2 編第 2 章第 4 節第 3 款第 4 目「データの回収とポータビリティ（Récupération et portabilité des données）」）、GDPR 準拠法制定に伴い削除された[18]。

アルザス及びモーゼルの商工会議所議員選挙における電子投票システム開設にあたり、データポータビリティ権（削除権、利用制限権及び意義申立て権も）を放棄するアレテ[19]がある。

CNIL は、データポータビリティ権の行使を促進するための方策として、①データ主体が認証されたアカウント/スペースから標準的な機械可読形式（CSV、XML、JSON など）でデータを直接ダウンロードできる機能を提供すること、②許可された第三者（組織またはその他）がデータを自動的に取得する機能を提供すること、③そのための安全な API を提供すること、を提案している[20]。

⑧異議申立て権（droit d'opposition）

GDPR21 条に規定する条件の下で行使される（法 56 条）

ただし、個人データの処理が法的義務を満たしている場合又は GDPR23 条に規定する条件の下で、これらの権利と義務に関する規定の適用が、法律の明示的な条項によって除外される場合には、本条は適用されない。

⑨プロファイリングを含む自動処理に基づく決定をされない権利

個人の行動に関する評価を含む裁判所の決定は、その人の人格の特定の側面を評価することを目的とした個人データの自動処理に基づいてはならない（法 47 条第 1 項）。

個人に関して法的効果を生ずる、又は個人に重大な影響を与えるその他の決定は、その個人に関する特定の個人的側面を予測または評価することを目的としたデータの自動処理のみに基づいて行うことはできない（同法第 2 項）。

ただし、GDPR22 条 2 項 (a) 及び (c) に規定する場合並びに公共行政関係法典 L. L. 311-

---

[18] デジタル共和国法のもとにおいて、すでに、データを送信する権利だけではなく、データを取得する権利についても規定しており、取得データの形式や取得可能性についての情報提供など、サービスプロバイダ等のデータ管理者に課される義務については、2016 年法制定に際してとられたオンライン協議プロセスにおいて、事業者等も関与しながら活発に議論された。

[19] Arrêté du 25 septembre 2021 portant création d'un système de vote électronique en vue des élections des membres des chambres de métiers d'Alsace et de la Moselle devant se dérouler du 1er octobre au 14 octobre 2021

[20] CNIL, « Professionnels : comment répondre à une demande de droit à la portabilité ? », 7 avril 2021, https://www.cnil.fr/fr/professionnels-comment-repondre-une-demande-de-droit-la-portabilite

3-1 条及び第 4 編第 1 章第 1 節に基づいて行われた個別の行政上の決定で、その処理が情報と自由法第 6 条 I に記載するデータ（いわゆるセンシティヴデータ）に関わらない場合は、適用しない。これらの決定に関して、データ管理者は、処理がどのように実装されたかをデータ主体に詳細かつわかりやすい形式で説明できるように、アルゴリズム処理とその展開を確実に制御する。

情報と自由法第 6 条 I に規定する特別なカテゴリーの個人データに基づく自然人に対する差別をもたらすプロファイリングは禁止される（法 95 条第 3 項）。なお、情報と自由法第 6 条 I は、GDPR9 条 1 項に対応している。

⑩集団訴訟

フランスでは、2014 年に、消費に関連する 2014 年 3 月 17 日の法律第 2014-344 号によって初めて集団訴訟が法的救済手段の一つとして導入された。そして、2018 年法では、GDPR 違反の損害賠償請求（GDPR82 条）につき、集団訴訟の道を開いた。同様の状況に置かれた複数の自然人が、個人データ管理者またはその下請け業者の GDPR 違反または GDPR と性質を同じくする法律の規定違反を共通の原因として損害を被った場合、違反状態の解消または損害賠償（精神的損害の賠償を含む）を求めて、管轄権を有する民事裁判所または行政裁判所に集団訴訟を提起することができる。原告適格は、私生活の保護または個人データの保護を目的とすることを少なくとも 5 年間定期的に宣言している団体、個人データの処理が消費者に影響を与える場合には、消費法典に基づき承認された全国を代表する消費者保護団体、および、個人データの処理が国民の利益や公務員の権利義務に関する場合には、労働法典に規定する従業員または公務員の労働組合に認められる。

（6） 情報銀行、PDS

CNIL が 2013 年 8 月に取りまとめた IP（innovation and foresight）レポートは、イギリスの MiData、フランスの MesInfos[21]に言及し、顧客と企業との間でデータを相互に共有することに、新たなイノベーションの道を見出している。また、PDS の具体例としては、MyDex, Privowny, personal.com を挙げている。個人が消費者データを「再利用」する方法としては、自分の移動や二酸化炭素排出量から、消費に対して環境に配慮した対応について考える、といった例が示されている（Daniel Kaplan）。他方で、一回の簡単な同意で、あらゆる企業が保有する取引データにアクセスできるようになると、個人のアクセス権を一種の一般化されたオープンデータに変換することになりかねない、といった懸念も示されている（Meryem Marzouki）[22]。

医療データに関しては、これを公益のために利用するという観点から、2016 年 1 月に

[21] 野村敦子「個人起点のデータ流通システムの形成に向けて ―イギリスの midata の取り組みから得られる示唆―」JRI レビュー9 巻 70 号（2019）199-201 頁

[22] CNIL, PRIVACY TOWARDS 2020 EXPERT VIEWS, aug 2013, pp.16-17.

医療システムを近代化するための法律により National Health Data System（SNDS）が設立された。SNDS は、公的機関によって収集された匿名化された健康情報を収集し、公益目的の調査、研究および評価のための利用を促進するためのシステムで、健康保険データ(SNIIRAM データベース)、病院データ(PMSI データベース)、医学的死因(Inserm の CépiDC データ)、障害関連データ（MDPH-CNSA データ)および補完的な健康保険組織からのデータのサンプルで構成される。公的・私的、営利・非営利を問わず、あらゆる個人・法人は、保健政策の実施、健康および医療社会的ケアの分野における革新等、公益に関する調査、研究、評価を実施する目的で、CNIL の許可を得て、2017 年 4 月から SNDS データにアクセスできる。

さらに、健康データについては、医療システムの組織化と変革に関する 2019 年 7 月 24 日の法律によって、健康データを共有するためのプラットフォームである Health Data Hub が設立された。主な目的は、国民の医療データを一元化して管理したうえで、研究者や企業によるそのデータへのアクセスを容易にし、データの利活用を促進することにある。フランスには、SAFARI 事件以降、データの集中管理／一元管理に対する拒否反応が強かったことから、健康データに特化しているとはいえ、一元管理を可能にしたのは、大きな転機といえる。

（7） 個人情報保護法を執行する監督機関の組織と権限

情報と自由法制定の目的の一つは、個人情報保護のための独立行政機関を創設することであった。今日では、GDPR 上の独立監督機関としても機能しており、データ保護基準・行動規範等の規則制定権、議会による諮問への答申（法 8 条Ⅰ)、データ処理者・下請け業者に対する立入調査、勧告、警告、許可等の取消し、命令（データ処理の適正化・停止等)、急速審理の申立て、制裁金の賦課等（法 19 条－23 条)、苦情処理の権限を有する。

以下では、GDPR 違反に対する制裁の概略について説明する。

CNIL の委員長は、想定されるデータ処理が GDPR に違反するおそれがあるという事実について、データ管理者又はその下請け業者に警告する（avertir）ことができる（法 20 条Ⅰ)。データ管理者又は下請け業者が、GDPR 又はこの法律に基づく義務を遵守していない場合、委員長は、期限を定めて、命令する（mettre en demeure）ことができる（同Ⅱ)。それでも是正されない場合は、罰金、許可・認証等の取消、就業規則を承認する決定の停止等の制裁を課す（同Ⅲ)。

情報と自由法 1 条に規定する権利や自由が重大かつ即時に侵害された場合は、権利と自由を保護するために必要なあらゆる措置を求めて、急速審理手続を裁判所に申立てることができる。必要に応じて罰則を求めることもできる（法 21 条Ⅳ)。

CNIL は、違反行為を検察官に告訴する権限も有しており（法 8 条Ⅰ)、刑事罰を科す場合は、そこから行政刑罰として科された金額を差し引くことができる。

3. 研究・医薬品開発を目的とした診療データの二次利用

健康データとは、「医療サービスの提供を含め、本人の健康状態に関する情報を明らかにする、自然人の身体的又は精神的な健康に関連する個人データ」と定義されている（GDPR4条15号）。診療データは、これに含まれる。「健康データ」はセンシティヴデータにあたるため、原則として、データ処理は禁止されるが（GDPR9条1項）、データの利用について本人の同意がある場合のほか、予防医学、健康・社会ケア治療の提供等に必要な場合、公衆衛生分野における公益のために必要な場合など、本人の同意なくしてデータ処理が例外的に認められる場合もある[23]。

情報自由法は、健康データの処理は、公益目的を考慮する場合にのみ実施できるとしており（66条第1項）、公益目的かどうかの認可権限はCNILにある。さらに、個人の自由や権利にとって「ハイリスク」な処理の場合、データ管理者はデータ保護影響分析を実施しなければならない（法90条）。医薬品開発などの研究目的で利用する場合には、公益目的と評価されるとしても、情報自由法の枠内で利用することになるため、データ主体の同意は原則として要請される。

より厳密には、診療データの利用に必要な手続き上の要請は、二段階で検討されなければならない。第一に、データウェアハウスの構築に関するルール、第二に、同一のデータ管理者又は他の組織によってウェアハウスに保存されたデータを使用して実施される調査、研究、または評価プロジェクトの実施に関するルールである[24]。

また、データ主体である患者以外の者から間接的に収集する場合の情報提供については、特に、科学研究目的で処理する場合にまで患者本人の同意を要するとすると、不相応な労力を強いることになるため、データ管理者において、情報を一般に公開する（例: Web サイトで公開される一般情報）など、データ主体の権利、自由、正当な利益を保護するための適切な措置を講ずればよいとされる。

以上

※本研究は、JST【ムーンショット型研究開発事業】グラント番号【JPMJMS2293】の支援を受けたものです。

[23] 宮下紘『EU一般データ保護規則』（勁草書房、2018年）74頁参照。

[24] CNIL, Traitements de données de santé : comment faire la distinction entre un entrepôt et une recherche et quelles conséquences ?, 2 mars 2023. CNIL, Quelles formalités pour les traitements de données de santé à caractère personnel ?, 8 janvier 2018.

Ⅴ．タイ

タイ法における情報自己決定権に関する報告

Thitirat Thipsamritkul[1]

1. 憲法と個人情報保護制度との関係性

1.1 プライバシー権ないし情報自己決定権の憲法上の位置づけ

「プライバシー（privacy）」という用語は、第 15 版にあたる仏暦 2534 年（西暦 1991 年）タイ王国憲法 44 条が制定されるまでタイ憲法の本文に現れなかった[2]（*「人の家族の権利、尊厳、名誉およびプライバシーの権利は保護されなければならない」*）。それまでは、仏暦 2492 年（西暦 1949 年）憲法に通信における秘密の保護と、家族の権利（right to family）について記載されているだけに過ぎなかった。

同様の規定は仏暦 2534 年（西暦 1991 年）憲法の第 44 条に再び現れ、プライバシーを侵害する画像または発言の流通を禁止する条項がその後のいわゆる「人民の憲法」と呼ばれる仏暦 2540 年（西暦 1997 年）憲法に盛り込まれた。[3]

---

[1] タマサート大学法学部専任講師。2019 年個人情報保護法案の起草委員会にコンサルタントとして貢献し、個人情報保護委員会のメンバーに選出された（後に辞退）。本報告書に含まれる情報の一部は、著者自身の経験から得られたものである。

[2] 仏暦 2475 年（西暦 1932 年）の民主革命以来のタイでは、暫定的なものを含め 20 本もの憲法が制定されてきた。これらの変化の主な理由は、13 回にもわたる軍事クーデターである。基本権の章は同様の構造を維持し、時間の経過とともに進化している。仏暦 2540 年（西暦 1997 年）憲法は、広範な市民参加を伴い文民政権が起草したことから、これらの憲法の中で唯一の「人民の憲法」と呼ばれた点において一線を画している。

詳しくは Andrew James Harding , Rawin Leelapatana, “Constitution-Making in 21st-Century Thailand:The Continuing Search for a Perfect Constitutional Fit”, The Chinese Journal of Comparative Law, Volume 7, Issue 2, September 2019, Pages 266–284 を参照, https://doi.org/10.1093/cjcl/cxz009.

[3] 仏暦 2540 年（西暦 1997 年）タイ王国憲法 34 条：

人の家族の権利、尊厳、名誉およびプライバシーの権利は保護されなければならない。

いかなる方法であれ、人の家族の権利、尊厳、名誉またはプライバシーの権利を侵害し、またはこれに影響を及ぼすような発言または写真を、公衆に対して主張または流布することは、公衆にとって有益な場合を除き、行ってはならない。

また、仏暦 2550 年（西暦 2007 年）憲法には、個人情報の不法な利用に対する保護が追加されている。[4]

現在の仏暦 2560 年（西暦 2017 年）憲法も同様の保護を維持しているが、そのような権利に対する制限には個人情報全般が含まれるように拡大されている。

> *「**第 32 条。** 人は、プライバシー、尊厳、名誉および家族に関する権利を享有する。*
>
> *第 1 項の人の権利を侵害し、若しくはこれに影響を及ぼす行為又はいかなる方法によるかを問わず、個人情報の利用は、公共の利益のために必要な限度においてのみ制定された法律の規定による場合を除き許されないものとする。」*

この変更は、画像や発言の範疇を超える原題における個人データに対する幅広い理解を反映している。この憲法の起草が、サイバーセキュリティ法案と個人情報保護法案を含む一連の新たなデジタルエコノミー法を導入する取り組みと並行して行われていた点は特筆に値する。

仏暦 2534 年（西暦 1991 年）憲法	**仏暦 2540 年（西暦 1997 年）憲法**	**仏暦 2550 年（西暦 2007 年）憲法**	**仏暦 2560 年（西暦 1997 年）憲法**
住居の自由とは切り離したプライバシー権の簡単な認識	プライバシー権の認識 + プライバシーを侵害する可能性のある画像または発言の流通の禁止	プライバシー権の認識 + プライバシーを侵害する可能性のある画像または発言の流通の禁止 + データの不法な利用に対する保護	プライバシー権の認識 + 個人情報の不法な処理の全体的な禁止

全体的に、タイ法では、プライバシー権は情報自己決定権とは異なるものとして解釈されていない。また、住居の自由など、

---

[4] 仏暦 2550 年（西暦 2007 年）タイ王国憲法 35 条：

人の家族の権利、尊厳、名誉およびプライバシーの権利は保護されなければならない。

人の家族の権利、尊厳、名誉およびプライバシーの権利を侵害し、またはこれに影響を及ぼすような発言または写真を、いかなる方法であれ、公衆に対して主張または流布してはならない。

人は、法律の定めるところにより、自己に関する個人情報の不法な利用から保護されなければならない。

古典的な意味でプライバシー権に関連する他の条項もある。[5]

憲法による保護の他には、民法典[6]と刑事法典[7]は常に不法行為責任を規定してきた。これらの規定にはプライバシーの侵害が含まれることが一般的に理解されているが、民法典と刑事法典はどちらも立証責任をデータ主体に課している。[8] プライバシー権またはプライバシーに言及した裁判例は非常に少ない。最もよく知られた民事訴訟は最高裁判所の判決第 4893/2558 号[9]であり、マスメディアが侵害してはならない仏暦 2540 年（西暦 1997 年）憲法と仏暦 2550 年（西暦 2007 年）憲法の両方で定められているプライバシー権を参照している。

1.2 個人情報保護制度の憲法上の意義

個人情報保護法（PDPA）の主な目的は権利を保護することにある。同法には個人データの処理に関する根拠を提供する条項も含まれており、第 26 条が規定する憲法の下における基本権を制限するものとして説明されている。[10] したがって、以下の PDPA の前文は、プライバシー権を保障する仏暦 2560 年（西暦 2017 年）憲法 32 条を特に参照している。

> *「本法には人の権利および自由の制限に関する一定の規定が含まれており、タイ王国憲法 32 条、33 条および 37 条と併せて、26 条が法律により許可している。*

---

[5] 仏暦 2560 年（西暦 2017 年）タイ王国憲法

住居の占有者の同意なく住居に立ち入ること、または住居もしくは私的な場所を捜索することは、裁判所の発する命令もしくは令状による場合、または法律の定めるその他の理由がある場合を除き許可されないものとする。

[6] Civil Code, Section 420, 422, and 423.

[7] Criminal Code, Section 326-333.

[8] Janjira Iammaruya, 'Laws relating to Personal Information in Thailand' in the Research Report submitted to the Official of Information Act (2003), p 6 [in Thai].

[9] Supreme Court Judgment No.4893/2558, 11 May 2015.

[10] 仏暦 2560 年（西暦 2017 年）タイ王国憲法

*「**第 26 条。**人の権利または自由を制限する結果となる法律の制定は、憲法が規定する条件に従わなければならない。憲法がその条件を定めていない場合、当該法律は法の支配に反しないものでなければならず、人の権利または自由に不合理な負担を課し、またはこれを制限するものであってはならず、人の人間としての尊厳に影響を及ぼすものであってはならず、権利および自由の制限の正当性および必要性も明記されなければならない。*

第 1 項の法律は一般的に適用されるものであり、特定の事件又は人に適用されることを意図するものではない。」

本法に従って人の権利と自由を制限する根拠と必要性は、個人データを効率的に保護し、個人データ保護の権利を侵害されたデータ主体に対して効果的な救済措置を講じることにある。本法の制定は、タイ王国憲法 26 条に規定された基準に合致している。」

第 26 条への言及は、PDPA の前文が第 33 条で定められている住居の自由と第 37 条における財産権に言及していることを反映している。[11] また、財産権への言及は、データの所有権を経済的権利の一部として捉えるという考え方も反映している。

タイでは一般的に、立法者らが参考にした主な研究を簡潔に参照するための注釈を法律の末尾に記載している。PDPA には、以下の注釈が記載されている。

「本法は、個人情報保護に関するプライバシー権の侵害が非常に多く、データ主体に苦痛と損害を与えてきたことが理由となり制定されている。また、技術の進歩は、このような侵害に該当する可能性がある個人データの収集、利用、または開示を可能にするとともにそれらを加速させてきており、最終的には経済に損害を与えることになった。したがって、個人データの利用を規制する規則、仕組み、または措置を設定するために、個人データ全般を保護する法律を発行する必要がある。」

この注釈は、タイの議員らの念頭にあるプライバシー権と経済的なインセンティブの両方の重要性を反映している。学術研究では、PDPA がプライバシー権を保護していることを一様に述べている。

2. 個人情報保護法制の現状と課題
2.1 他国における法制度の影響

PDPA 制定前の法律に与えた影響

汚職防止、政府の透明性、およびメディアの自由の台頭といった世界的な傾向に続き、政府の情報にアクセスする人々の権利を強化するために仏暦 2540 年（西暦 1997 年）公的情報法が制定された。本法の第 3 章には、個人情報の保護に関する規定が含まれている。必要性の原則、目的の制限、直接的なデータ収集、透明性が示されている。

---

[11] 仏暦 2560 年（西暦 2017 年）タイ王国憲法

*「**第 37 条。** 人は、財産および相続に関する権利を享有する。そのような権利の範囲および制限は、法律の定めるところによる。 ….」*

その後の仏暦 2546 年（西暦 2003 年）信用情報事業法（Credit Information Business Act）では個人データ保護に関するより詳細な規定が盛り込まれており、（欧州連合指令 95/46/EC に従っている）1998 年の英国データ保護法と 1970 年の米国公正信用報告法の両方による影響を受けているが、これら二つのモデルは特にデータ主体の同意について原則や法律のスタイルが異なっている。[12]

個人情報保護法（PDPA）

個人情報保護法の起草と成立の試みは仏暦 2540 年（西暦 1997 年）に公的情報法を制定した直後から始まった。[13] PDPA 草案の初期バージョンは EU、英国、豪州、シンガポールを含む異なる国々の法律による影響を受けていた。起草作業は公式情報局（Office of Official Information） とタイ国立電子コンピューター技術研究センター（NECTEC）が開始した。

しかし、2014 年のクーデター後は、軍事政権がデジタル経済法の改革へと繋がった「タイ 4.0」政策を宣言した。[14] 著作権法、電子取引、コンピュータ犯罪、電気通信規制の改正を経て、電子取引開発機構（ETDA）とデジタル経済社会省（MDES）の協力の下でサイバーセキュリティ法案と個人データ保護法案が起草された。

2014 年の軍事クーデターから 3 年後の 2017 年、新たな仏暦 2560 年（西暦 2017 年）憲法の制定に至った論争の的となった国民投票を経て、軍事政権は学界コミュニティ、市民社会、および一般国民による抵抗が広がる中、仏暦 2550 年（西暦 2007 年）コンピュータ犯罪法を改正した。この改正は恣意的な執行を可能にするようなオンラインでの自由の抑圧への固執について国内外から批判され、民主的な選挙の約束が予定どおり果たされていない中で

---

[12] Chalaware Chusap, *Problems of the application of The Credit Information Business Act 2002: Study on the issue of data suject's consent* (Thammasat University Master of Law Thesis, 2009). [タイ語]

[13] Nakorn Serirak, *Privacy*, (Faham Publishing 2nd edn, 2020), p 265-289. [タイ語]

14 Rumana Bukht & Richard Heeks, 'Digital Economy Policy: The Case Example of Thailand', Paper No. 7 Development Implications of Digital Economies**,** 2018, p 12-13 <https://diode.network/publications/>.

自己検閲を誘発させた。[15] 当時、サイバーセキュリティ法案は他国における同様の法律と同じように政府が人々のプライバシーに侵入するためのさらなるツールとして見なされていた。[16]

> 「*本法案に対する国民の反発の高まりは、権力の濫用やデータプライバシー侵害への懸念から、オンラインとオフラインの両方で激震を引き起こしている。法案はあまりにも広範囲に及び、実行は不可能であり、個人や法人の権利を侵害する可能性があると非難されている。*[17]

これらの事情を背景に、サイバーセキュリティ法案を個人情報保護法案と併せて検討しなくてはならないことを要求する声が主流となった。したがって、ETDA と MDES の両方が両法の草案を見直すために市民社会による関与を深めることを試みた。GDPR が 2018 年に発効したことが ETDA、MDES、および法制委員会の起草者に巨大な影響を与え、個人情報保護法案をその構造や原則から変更させるに至った。[18] 軍事政権の第一内閣におけるデジタル経済社会省大臣のピチェート・ドゥロンカヴェロージ博士は GDPR の施行を、タイが世界的なデジタル経済に参加することを可能にするための個人情報保護法案の起草過程を加速化させるための重要な後押しとして言及している。[19]

---

15 'Thailand passes amendment to cyber law despite opposition' (Reuters, 16 December 2016) <https://www.reuters.com/article/us-thailand-cyber-idUSKBN14513I> ; Danny O'Brien and Gennie Gebhart, 'The Amended Computer Crime Act and the State of Internet Freedoms in Thailand' (Electronic Frontier Foundation, 21 December 2016) <https://www.eff.org/deeplinks/2016/12/amended-computer-crime-act-and-state-internet-freedoms-thailand> ; Article19, *Thailand Computer Crime Act 2017: Legal Analysis*, (Article19, 2017) <https://www.article19.org/data/files/medialibrary/38615/Analysis-Thailand-Computer-Crime-Act-31-Jan-17.pdf>.

16 'Thai proposal for all-powerful cyber agency alarms businesses, activists'(Reuters, 16 November 2018) <https://www.reuters.com/article/us-thailand-cyber-idUSKCN1NL0JP>. 'Deputy PM insists cyber security bill still subject to change' (National News Bureau of Thailand, 17 October 2018) も参照 <https://thainews.prd.go.th/en/news/detail/WNPOL6110170010018>.

17 'The Cybersecurity Balancing Act: A draft law is positioned to give the state unprecedented power over the digital arena' (Bangkok Post, 22 October 2018) <https://www.bangkokpost.com/thailand/politics/1562230>.

18 'Thailand: MDES publishes revised draft data protection bill' (Data Guidance, 26 February 2018) <https://www.dataguidance.com/news/thailand-mdes-publishes-revised-draft-data-protection>.

19 The Nation, "Government Fast Tracks Personal Data Protection Law", 18 May 2018, https://www.nationthailand.com/in-focus/30345749 .

学術的なガイドラインを通じた GDPR の影響

デジタルや銀行の分野の法律事務所や企業と協働で作成された学界主導のガイドラインである「タイ・データ保護ガイドライン（TDPG）1.0」[20] では、EU の原則やその他の国際的なデータ保護の慣行を取り入れている。一部の企業は GDPR がタイの企業にとって高すぎる基準を求めるのではないかという懸念を示したものの、TDPG 1.0 は欧州の企業と取引をするタイの企業が GDPR に準拠し、国内に集中する企業も新たな個人情報保護法案に向けて準備を整えるよう手伝う弁護士らにとって参考となった。

個人情報保護法案を（サイバーセキュリティ法案と併せて）検討したタイ国民議会の委員会[21] も TDPG 1.0 を参考文献として扱い、タイが EU の「ホワイトリスト」に含まれる可能性に複数回にわたり言及している。さらに、GDPR モデルはこれまでの草案よりもプライバシー権を保護し、官民両方の組織に適用されることで政府機関による個人データの乱用を防ぐ可能性も秘めているものとして見なした市民社会も GDPR モデルを支持した。

PDPA の最終版は GPDR の重要な原則に従っていた。研究や統計の目的は、追加の合法的根拠として加えられた。同様の一連のデータ主体の権利も、自動的な決定における介入の権利以外が含まれた。GDPR とは異なり、学界が強烈に異論を唱えたにもかかわらず、刑罰も導入された。これはのちに PDPA に関する不必要な誤解を招き、その執行を遅らせる一因となった。[22]

国際的な慣行に従おうとする動きと、適用除外を狙う国内の抵抗の狭間で

PDPA は GDPR や他の高所得国の慣行に従った経済的な意欲に動機付けられていたことは明らかである。GDPR が持つプライバシー権に優しいという評判も、MDES がコンピュータ犯罪法の改正による反発に反応し、サイバーセキュリティ法に対する批判を回避することを可能にした。

しかし、PDPA4 条は、これらの利点を薄めうる様々な政府機関に対して広範な適用除外を定めている。新法の起草には、PDPA の適用除外が含まれる傾向が見られる。

---

[20] Piyabutr Boonaramruang et al, Thailand Data Protection Guideline 1.0 (Chulalongkorn University Press, 2018) [タイ語]. 本報告書の著者も、この学術グループの一員である。

[21] タイ国民議会は 2014 年のクーデター後に軍事政権により指名された機関であり、立法府として機能している。

[22] 様々な組織がこの誤解を解こうと試みている。例えば [タイ語] 大学 <https://www.chula.ac.th/news/75005/>、ファクトチェック機関「CoFact」 <https://blog.cofact.org/digital-thinkers22/>、コンサルティング提供機関 <https://pdpathailand.com/knowledge-pdpa/7things-misleading-about-pdpa/ >。

仏暦 2566 年（西暦 2023 年）のテクノロジー犯罪に対する保護対策とその抑圧に関する王令（The Royal Decree on Measures for Protection and Suppression of Technology Crimes）には、データ処理の目的に関する個人情報保護法（PDPA）に基づく義務を免除する第 12 条[23] が盛り込まれている。このことは、PDPA が法律により規定された公的任務のための個人情報保護を処理するための明確な合法的根拠を当局に提供しているにもかかわらずタイの役人が PDPA や、公的情報法を含む他の個人情報保護法をサイバー犯罪や詐欺の防止などの公益を追求する上での障害物として見なした場合に明らかに発生している。多くの学者や市民社会は、当局によるデータ処理を監督する手段を伴わずに国民の情報をさらに収集するためにこの一般的な適用除外が乱用されることを懸念している。これには銀行と電気通信という二つのデータ集約型の産業による個人データの処理が関わっていることから、透明性の原則はこの文脈においてかなり損なわれてしまっている。

2023 年 6 月には、暫定内閣が、個人データが汚職防止関連の要求などの政府の要求に応じるために提供される場合において、より多くの政府機関や民間セクターをデータ保護に関する複数の義務から免除する新たな法令を承認した。[24] この新たな法令は、国会による検討を伴わずに行政府による適用除外の拡大を許容する、PDPA4 条（2）の規定に記されている解釈の余地が大きい文言に基づいて発行されている。

> *「本法の規定の全部または一部を、第 1 項のデータ管理者と同様の方法、事業または団体に適用する例外、またはその他の公益目的のために適用する例外は、法令の形式で公布されるものとする。」*

このような適用除外の増加と拡大は民間企業のデータガバナンス制度に多大な混乱をもたらし、タイの PDPA を GDPR モデルからあからさまに脱線させてしまうことが予想されている。また、これは憲法によるプライバシー権の保護のレベルを下げてしまう恐れもある。しかし、そのような適用除外の合憲性について憲法裁判所において争うような戦略的訴訟が起こるとは考えにくい。仏暦 2560 年（西暦 2017 年）憲法 32 条の法文は、そのような適用除外が「公益」に該当するものとして説明される可能性が高いという解釈を許容するであろう。多くの市民社会は、そのような決定が下されれば、政府機関がさらなる適用拡大の拡大を行うという前例となってしまうことを恐れている。

2.2「個人データ」の定義と範囲

[23] *第 12 条。この王令に基づく個人データの開示、交換、アクセス、保管、収集、利用は、個人情報保護法の施行下にはない。ただし、データを受領または保有する者は、当該する個人データを関連義務のない者に開示してはならない。*

24 Royal Thai Government, Press Release 11 July 2023, at https://www.thaigov.go.th/news/contents/details/70221

「個人データ」の範囲は、次のとおり、PDPA6 条により定義されている。

「『個人データ』とは、人に関する情報であって、直接的または間接的に当該する人を識別することができるものを指すが、特に死者の情報は含まれない。」

公的情報法では、「個人情報」を次のとおり定義している。

「個人情報」とは、「教育、財政状態、健康記録、犯罪記録、雇用記録など、個人のすべての個人的特定事項に関連する情報であって、当該個人の氏名が含まれ、または指紋、音声が記録されたテープもしくはディスケット、または写真など、当該個人を特定する数値参照、コード、またはその他の表示が含まれるものであり、死者の個人的特定事項に関連する情報も含まれること」を意味する。

PDPA の定義は公的情報法と比較して広いが、死者のデータを除外している。間接的に識別可能なデータを包含することで、保護範囲を拡大している。広範な定義にはクッキーやその他のオンライン上の識別子も含まれている。クッキーやその他のオンライン上の識別子の処理には、PDPA の個人データ保護措置の下、何らかの評価や措置が必要であると一般的に考えられている。[25]

2.3 データ主体の権利と事業者の義務

PDPA におけるデータ主体の権利は、特に委員会が執行について持つ権力が非常に限られている公的情報法による仕組みと比較すると、格段に包括的な形で保護されている。データ主体の権利は情報提供を受ける権利、[26] アクセス権、[27] 訂正権、[28] 削除権、[29] 利用制限権、[30] およびデータ・ポータビリティ権である。[31]

---

[25] Piyabutr Boonaramruang et al, *Thailand Data Protection Guideline 3.0* (Chulalongkorn University Press, 2020), p 85 [タイ語].

[26] PDPA Section 25 and 27.

[27] PDPA Section 30.

[28] PDPA Section 35.

[29] PDPA Section 33.

[30] PDPA Section 34.

[31] PDPA Section 31.

この権利の一覧は GDPR と似ているが、データ主体には PDPA に基づくプロファイリングを含む自動化した個人の意思決定の対象となる権利がない点は例外である。

a) 個人データの削除権または利用停止請求権

個人データの削除、破棄、および匿名化する権利は PDPA33 条に含まれている。この権利は（1）必要な目的が存在しなくなった場合、（2）同意が撤回された場合、（3）データ処理に公的任務または正当な利益という合法的根拠がなかったとするデータ主体の異議申し立てが認められた場合、または（4）データが不法に処理された場合に援用できる。PDPA は、データが一般公開された場合に行動し、他の関連するデータ管理者にも通知するようデータ管理者に義務付けている。

個人データの利用を制限する権利は PDPA34 条にも含まれている。[32] この権利は、データ主体またはデータ管理者が他の措置を追求する前の一時的な措置として行使されることを想定している。

b) 同意の位置付け

---

[32] ***34 条。****データ主体は、データ管理者に対し、以下に該当する場合、個人データの使用を制限するよう要求する権利を有する。*

(1) データ管理者が第 36 条に基づくデータ主体の要求に従って審査手続中である場合

(2) 第 33 条（4）に従って削除または破棄されるべき個人データであるが、データ主体が当該個人データの利用制限を要求している場合

(3) 当該収集の目的のために当該個人データを保持する必要がなくなったが、データ主体が法的請求の確立、遵守、行使、または法的請求の防御の目的のために保持を要求する必要がある場合

(4) データ管理者が第 32 条（1）に関して検証中である場合、または第 32 条（3）に関して、データ主体が第 32 条第 3 項に従って行った異議申し立てを拒否するために審査中である場合

データ管理者が第 1 項に従って措置を講じない場合、データ主体はデータ管理者にそのような措置を講じるよう命令するために専門家委員会に苦情を申し立てる権利を有する。

委員会は、第 1 項に従って利用停止に関する規則を制定し、公表できる。

タイの PDPA24 条は必要性の原則を統合し、正当な目的のための適法かつ公平な処理について七つの根拠を規定している[33]（これらは同意、過去のアーカイブおよび研究／統計、[34] 重大な利益、契約上の義務（または契約の締結）、公的任務または職務権限、正当な利益、[35] およびデータ管理者の法的義務である）。

後に発表されたデータ保護委員会による規則に従って実施されなくてはならない「過去のアーカイブおよび研究／統計」の根拠を除くと、他の六つの根拠は GDPR とほぼ同一である。同意は現在のデジタル環境に関する唯一の主たる根拠とすることはできず、またそうあるべきでもないと起草委員会が認めているにもかかわらず、同意の根拠は一般原則として、他の根拠は例外として定められている。これは、法制委員会により主張された法案の起草の既定の方法である。この規定が実務において同意を過剰に優先させる結果となったことは驚くべきことではない。

起草の経緯と併せ、同意を処理のための主な根拠として明らかに定められていない他の関連する規定を考慮に入れると、[36] 同意は主な根拠に頼ることができない場合においてのみ必要となる。主な根拠は通常の事業運営における「契約」、通常の政府運営における「公的任務／職務権限」、および両方の文脈における「法的義務」である。GDPR と同様に、第 19 条ではデータ主体の自律性と彼らのデータを管理する権利を優先する複数の厳しい条件を必要としていることから、データ管理者にとって同意は最良の根拠ではない。オプトインへの同意が必要でありデータ主体がほとんどの状況において同意を撤回できることから、「正当な利益」の方がより実用的な根拠である。

結論として、「同意」はマーケティング目的や追加のサービスなどに適している。通常の業務では依拠してはならない。しかし、多くのデータ管理者はほとんどの状況において「同意」が求められていると未だに混同している。

---

[33] 第 24 条で用いている用語は「収集（collection）」である。しかし、第 24 条で指定している根拠と関係している他の規定の文脈を考慮し、この規定は、利用、公開、保管、および削除を含むすべてのデータ処理活動を対象としているものとして読み取ること。

[34] しかしながら、仏暦 2550 年（西暦 2007 年）国民健康法（National Health Act）9 条では、実験の対象としての医療サービス受給者の使用について同意を得ることを義務付けている。PDPA3 条（1）と併せて読むと、同意は医療実験の合法的根拠であり続けている。PDPA に加え、他のセクター規制者も同様の条件を設定している可能性がある。

[35] タイで用いられている用語は「合法的な利益（lawful interest）」であるものの、PDPC やその他の専門家による準備作業やその後の説明では、当該用語が GDPR における「正当な利益（legitimate interest）」と同等であることが示されている。

[36] Piyabutr Boonaramruang et al, *Thailand Data Protection Guideline 3.0* (Chulalongkorn University Press, 2020) p 65-94 [タイ語].

この迷信は、データ保護に関係する過去の法律[37]と直接関係しない過去の法律[38]の両方における同意への言及、2022年6月のPDPAを発効した際における関係者による誤った伝達などの様々な理由によってもたらされている。

個人データの第三者への開示では、かかる開示が処理目的という当初の範囲に必要である場合、同意が求められない。第23条と第25条では適切な通知を義務付けているが、第27条と第39条ではそのような開示の記録が要求されている。

c) ＜通知＝同意＞モデルの限界とその対策。

第19条における妥当な同意の要件は、人間の認知能力が限られていることによる自己管理モデルの限界に部分的に対処している。同条はGDPRに従い、以下の事柄を要求している。

> *「このような同意の要求は、他の事項とは明確に区別できる方法で、分かりやすく明確な言葉を使用し、容易にアクセスできる分かりやすい形式および記述で提示し、このような目的に関してデータ主体を欺くことや誤解を招くことがないものとする。」*

また、第19条では、同意を取得する際にデータ管理者が使用すべき標準書式や文言を規定する裁量権をPDPCに与えている。ただし、PDPCは単独で標準書式を発行せず、第3条に従ってデータ管理者に追加の義務を規定している他の法律による強制的な標準書式を参照している。[39]

---

[37] 例えば、仏暦2550年（西暦2007年）信用情報法（Credit Information Act）。

[38] 例えば、仏暦2550年（西暦2007年）国民健康法における医療サービスや医療研究のための患者によるインフォームドコンセント、民法典における未成年者による民間取引のための親・保護者の同意。

[39] 第3条は、他の法律と重複する以下の内容を規定している。
「あらゆる方法、あらゆる事業、またはあらゆる事業体において、個人データの保護を規定する分野固有の法律が存在する場合は、当該法律の規定が適用される。

(1) 個人データの収集、使用、および開示に関する規定、およびデータ主体の権利に関する規定（関連する罰則を含む）については、上記の特定法との重複の有無にかかわらず、本法の規定が追加的に適用されるものとする。

(2) 苦情に関する規定、データ主体を保護する命令を出す権限を専門家委員会に付与する規定、および関連する罰則を含む管轄官吏の権限および義務に関する規定については、以下の場合に本法の規定が適用されるものとする：

また、データ管理者に、産業が自主的に定めた既存の標準書式を使用すること、さらに 2022 年 9 月 7 日に発表された PDPC ガイドラインを遵守することも勧告している。[40] このガイドラインは欧州データ保護会議のガイドラインや、TDPG 3.0 と呼ばれるタイの学者らによるガイドラインと同様の提案を行っている。2022 年 9 月 7 日に発行された通知に関する別の PDPC ガイドラインでも GDPR と ICO の勧告に従っている。[41] これらのガイドラインには法的な拘束力はないものの、専門委員会と裁判所にはこれらを考慮した上で法を解釈することが期待されている。

研究・医薬品開発を目的とした患者の診療記録または生体認証データの利用

PDPA24 条では、過去のアーカイブや研究／統計を一般個人データ（機微でないデータ）の処理のための別の法的根拠として規定している。[42] 解釈の方向性は知られていないため、この合法的な根拠に頼る者は少ない。PDPC からは、保護措置に関する具体的なガイドラインはまだ発表されていない。

診療記録または生体認証データを含む機微データを統治する第 26 条でも厳格な同意条件の例外を提供しており、そのほとんどが医療従事者や、ヘルスケアならびに福祉のための手配に関係している。GDPR9 条（2）（i）と同様に、第 26 条（5）b[43] も法律により定義された公衆衛生の利益のための診療データの正当な目的を提供している。

(a) 苦情に関する規定が当該法律において定められていない場合

(b) 当該法律が、当該法律に基づき苦情を検討する権限を有する主管官吏にデータ主体を保護する命令を発する権限を与える規定を有するが、当該権限が本法に基づく専門家委員会の権限と同等でない場合であって、当該法律に基づき権限を有する主管官吏が専門家委員会に要求する、データ主体が専門家委員会に苦情を申し立てるかのいずれかである場合。」

[40] 次の URL より閲覧可能 [タイ語] <https://www.mdes.go.th/uploads/tinymce/source/สคส/แนวทางการด เนินการในการขอความยินยอมฯ.pdf>.

[41] 次の URL より閲覧可能 [タイ語]<https://www.mdes.go.th/uploads/tinymce/source/สคส/แนวทางการด เนินการในการแข้งวัตถุประสงค์ฯ.pdf>.

[42] しかしながら、仏暦 2550 年（西暦 2007 年）国民健康法（National Health Act）9 条では、実験の対象としての医療サービス受給者の使用について同意を得ることを義務付けている。PDPA3 条（1）と併せて読むと、同意は医療実験の合法的根拠であり続けている。PDPA に加え、他のセクター規制者も同様の条件を設定している可能性がある。

[43] **第 26 条。**人種、民族的出身、政治的意見、カルト、宗教または哲学的信条、性的行動、犯罪歴、健康データ、障害、労働組合情報、遺伝子データ、バイオメトリクスデータ、またはデータ主体に同様の影響を与える可能性のあるデータに関する個人データの収集は、データ主体の明示的な同意がない限り、当委員会が定める場合を除き、禁止されている。

これは、特定の法律に基づいて実施される研究プロジェクトでは患者の同意が必要でないことを意味している。また、PDPC の委員は、民間の研究所が政府機関と協働していない場合に研究を実施するにあたり患者の同意しか頼れないことから、それらの研究所に不当な不利益をもたらしうることも認めている。いずれにせよ、データを匿名化または仮名化する義務は PDPA が直接要求しているわけではないものの、医療や研究に携わる職業に関係する他の職業倫理やその他の規制により要求されることが考えられる。

第 26 条第 5 項の e も、もう一つの同意の例外として法律で定義された公益を規定している：*「データ主体の基本権および利益を保護するための適切な措置を提供することによる実質的な公共の利益。」*

同項の各段における「適切な措置（suitable measure）」を提供する義務は、個人データの処理から得られる可能性のある公益と、それが個々のデータ主体の権利や自由に及ぼす影響のバランスを取る試みを反映している。

d) 情報銀行や PDS（Personal Data Store）のように、パーソナル・データに対する本人の controllability を補助するための仕組みや制度はどのように社会実装されているか

情報銀行や PDS（Personal Data Store）のような個人データに対する本人の control lability を補助するための具体的な仕組みや制度の社会実装は行われていない。そのような活用は禁止されていない。

これについてタイではこれまでに広い議論が行われていない。そのような活用は PDPA24 条に基づく合法的根拠として「契約」または「正当な利益」として行われることが考えられる。そのような PDS の運営者は、データ管理者として見なされなくてはならない。機微データの処理は、PDPA26 条に基づいてより厳格な条件の対象となる。

e) AI の利活用やプロファイリングの場面に特化したデータ保護の仕組みが存在するかどうか。

GDPR21 条で提供されているような、プロファイリングに異議を申し立てる権利を規定する具体的な条項はない。

---

(5) 以下の目的を達成するために法律を遵守する必要がある場合

(b) データ主体の権利および自由を保護するための適切かつ具体的な措置、特に義務または職業倫理に従って個人データの機密性を維持するための措置が講じられていることを根拠とした、国境を越えた危険な伝染病または伝染性もしくは疫病の流行に対する保護、または医薬品、医薬品または医療機器の基準もしくは品質の確保などの公衆衛生上の公益

ただし、これは過去にも PDPA 制定後にも議論されたことがあり、データ保護影響評価（DPIA）に関する議論や TDPG 3.0 のマーケティング部門のガイドラインなどで行われている。[44] プロファイリングがデータ主体のリスクを高めるのであれば、データ管理者はデータ主体のための保護措置を採用し、その誠意を証明するために影響評価を記録すること。また、データ主体はアクセス権や制限権をデータ管理者に対して援用し、プロファイリング過程の透明性を回復し、個人データの不公平な使用に反対することも可能である。

f) データ・ポータビリティ権は保障されているか（例えばGDPR 第20 条）。またこの権利は具体的にどのような場面で社会実装されているか。

第 31 条は、自分の個人データにアクセスし、データ管理者からかかるデータを受領する権利を規定している。データ・ポータビリティ権は、次のとおり PDPA31 条（2）に含まれている。

> *(2) 技術的な事情により不可能な場合を除き、データ管理者が他のデータ管理者に送信または転送する形式の個人データを直接取得する要求。*

タイ国民議会の委員会は、草案の検討過程において、この規定について詳細に議論している。公共セクターからの数々の代表者が、この権利を他国で見られるような市場の競争を促すものよりも、オープンな政府の取り組みを可能にするものとして見なしている。立法過程における起草者や論評者のそのような意図とは対照的に、PDPA はオープンデータ構想への主な障害として何度も言及されている。

この権利の実施は、まだ実務では見られてない。この権利はデータ管理者の存在を容易に存在できるという技術的な状況を条件としていることから、この規定に基づいた苦情の申し立てが認められる見込みは薄い。

2.4 個人情報保護法を執行する監督機関の組織と権限（制裁や告訴の仕組み）。

組織構造と政府との関係性

個人情報保護委員会（PDPC）は、PDPA を施行する主な監督機関である。この委員会の資格を有する委員は首相、国会議長、オンブズマン、および国家人権委員会により任命された独立した特別委員会により選出されなければならない。

---

[44] Piyabutr Boonaramruang et al, *Thailand Data Protection Guideline 3.0* (Chulalongkorn University Press, 2020), p 213-222, p 353-366 [タイ語].

PDPC の現メンバーは法律の他に医療業界、証券取引、法執行、軍事などの関連分野の専門家 10 名である。MDES の事務総長、首相府事務総長、法制委員会の事務局長、消費者保護委員会の事務局長、自由権利保護局長、PDPC 事務所の司法長官および事務局長が職権により委員の役割を担う。資格を有する PDPC の委員の任期は 4 年間であり、2 期まで任命されることが可能である。[45] 内閣は、PDPC の委員をそのその行為により解任できる。[46]

タイ公法の下、PDPC は「独立行政組織」の地位を持っている。PDPC は通常の政府機関による様々な規則により管理される可能性のある中立的な政府機関であり、政治的な介入を受けてはならない。[47] PDPA46 条は、政府がシードファンドと年間予算を適切に提供しなくてはならないことを定めている。

権限

PDPC は個人情報保護に関連する法律を監督し、内閣に妥当な提案を行う責任を負っている。また、PDPC は個人データの促進と保護に関する計画立案、ガイドラインや措置の規定、様々規則、規範、下位規制の発行なども担当する。さらに、PDPC は国家経済社会デジタル開発委員会が策定した方針に従った個人情報保護の規制についても責任を負い、それに伴い委員会のために基本計画も立案する。[48] 加えて、PDPA は既存の法律とともに適用される新しい基準を追加することから、特に特定のセクターの個人情報保護を規制する権限を有する他の政府機関に助言するとともにそれらと協力する義務も負う。

制裁や告訴の仕組み

PDPC は、適切と判断した場合に苦情を検討するための専門委員会を任命し、コンプライアンス違反を調査し、紛争を解決することができる。[49]

---

[45] PDPA, Section 12.

[46] PDPA, Section 13.

[47] 政府機関の「独立行政組織」としての分類は、公共部門開発委員会室（Office of the Public Sector Development Commission）の原則と慣行に従っている。

これらの原則と実践は次の URL より閲覧できる [タイ語] :

<https://webdev.excise.go.th/act2560/images/files/กฎหมายอนๆ/_แก้ไข_เพิ่มเติม.pdf>. 最新版の各カテゴリのリストは

<https://po.opdc.go.th/>より閲覧できる [タイ語]。

[48] PDPA, Section 16(1).

[49] PDPA, Section 72.

現在、PDPC は 2 つの専門委員会を任命しており、一つは財務・経済関連の苦情、もう一つはデジタル医術関連の苦情に特化している。PDPA71 条～76 条では、データ主体を対象とした苦情を申し立てるための仕組みを規定している。苦情は PDPC に直接、または電子メールを経由して提出できる。苦情のテンプレートでは、苦情を申し立てる対象が①データ管理者、または②その他の政府機関（PDPC 下の専門委員会、行政裁判所またはその他の裁判所、その他の政府機関）かどうかをデータ主体が明確にすることが義務付けられている。[50] これは、他の政府機関の監督下にある他の苦情を申し立てる仕組みも検討することを専門委員会に義務付けている第 73 条第 2 項と一貫している。

> *「苦情の申出、受理拒否、却下、審議、および審議期間は、他の法令により審議権限があった場合の苦情の受理拒否又は却下を考慮した上で、委員会の定めるところによるものとする。」*

この第 73 条の解釈は、異なる法律の下で重複している課題を規定する第 3 条と併せて、PDPC と、銀行、保険、電気通信などの特定のセクターに関わるプライバシー関連の問題を規制する他の政府機関の間で管轄の問題を引き起こしてしまう恐れがある。

苦情を解決できない場合、専門委員会はデータ管理者またはデータ処理者に①履行または訂正、②行為を禁止または損害を停止する行為を実施するよう命令する権限を持つ。[51] 不履行の場合、専門委員会は行政処分 [52] と行政刑罰を行える。[53] 行政処分には通知、召喚、調査、押収、没収が含まれる。行政刑罰は最大 THB 5,000,000 までを課すことが可能である。[54] 行政処分や行政刑罰への異議は行政裁判所に申し立てることが可能である。[55]

加えて、PDPA79 条～81 条では最高刑期 1 年の刑事罰を規定しており、さらに第 78 条では実際の損害の 2 倍までの懲罰的損害賠償を認めている。これらの規定は、司法裁判所（民事裁判所と刑事裁判所の両方）が PDPA 関連の紛争を判断する可能性を残している。

---

50 詳しくは https://www.mdes.go.th/mission/detail/6408-ประกาศและคำสั่งของสำนักงาน を参照。

51 PDPA, Section 74, paragraph 3.

52 PDPA, Section 74, paragraph 4.

53 PDPA, Section 90.

54 PDPA, Section 85 and 87.

55 タイの行政裁判所制度の詳しい情報については次も参照：
https://www.admincourt.go.th/admincourt/en/structure.php

2.5 司法的救済の仕組み

PDPC の権限の下における主な強制措置である行政制裁の他に、PDPA では民事責任[56]と刑事責任[57]も規定している。データ主体は、民事裁判所や刑事裁判所に苦情を提出することもできる。民事責任の具体的な規定は、データ主体が立証責任を果たす場合に役立つ。

PDPA は、立件または集団訴訟に関する具体的な規定を提供していない。タイの訴訟法の一般原則が適用される。[58] データ侵害に対する集団訴訟は、タイ民事訴訟法 222/8 条で認められている訴訟累計に該当する可能性がある。[59] ただし、司法裁判所の裁判官の知識が PDPA 関連の紛争における専門的な問題に取り組む上で十分かどうかについては、全体的にまだ疑問が残っている。

※本研究は、JST【ムーンショット型研究開発事業】グラント番号【JPMJMS2293】の支援を受けたものです。

---

[56] PDPA, Section 77-78.

[57] PDPA, Section 79-81.

[58] タイにおける集団訴訟手続きの詳しい情報については Tanaporn Farungsang, 'Summary of Class Action under the Civil Procedure Code' (SEC, 2019)も参照。

<https://www.sec.or.th/EN/Documents/LawsandRegulations/ClassAction-appendix-EN.pdf.

[59] タイ民事訴訟法 222/8 条。

集団の構成員が多数存在する以下の事件については、集団の構成員である原告は集団訴訟を請求することができる：

(1) 不法行為事件

(2) 契約違反事件

(3) 環境法、消費者保護法、労働法、株式・株式市場法、貿易競争法などの様々な法的権利を主張する事件

VI. 台湾

研究プロジェクト：分散型データ管理を通じた心の自由と価値の協創 ― 台湾に関するレポート

Chien-Liang Lee
台湾　中央研究院法律学研究所

1. 憲法と個人情報保護制度との関係性

① プライバシー権ないし情報自己決定権の憲法上の位置づけ

(1) プライバシー権または情報自己決定権は、台湾憲法で保障されている権利である。

プライバシー権または情報自己決定権は台湾憲法において明示的に規定されておらず、司法院大法官（台湾憲法裁判所、以下「TCC」）による憲法解釈を通じて認められ、実践されている。

TCC は、司法院（J.Y.）解釈第 293 号（1992 年）において初めてプライバシー権に言及している。司法院解釈第 585 号（2004 年）の判決理由は、プライバシー権が、干渉に対する個人の生活や私的な生活空間の保護と個人データの自律性について定めている憲法 22 条[1] により保証されている基本権であることを明示的に示している。司法院解釈第 603 号（2005 年）の判示によると、個人データを公開するかどうか、する場合はどの程度、いつ、どのような形で誰に公開するのかを決定する権利、個人データの利用について知りそれを管理する権利、ならびに個人データに含まれる誤りを訂正する権利を保証する「*情報プライバシー権（the right to informational privacy）*」または「*個人情報プライバシー権（the right to personal informational privacy）*」という用語が作り出されている。司法院による解釈の発展を踏まえると、個人情報の自律性の定義は調整や修正が施され続けている。

技術の発展を鑑みて、前述の情報プライバシー権の保護の意味は後に継承されただけでなく、2022 年に設立された憲法裁判所によりさらに拡張されている。2022 年 8 月 12 日に TCC が下した判決 111-Hsien-Pan-13 は事後的な管理権を強調しており、例えば情報プライバシー権はデータを活用する前に影響を受ける者にデータが活用されるかどうかを決定する事前的な管理権があること、

[1] 憲法 22 条：「社会秩序または公共の福祉を害しない国民の他のすべての自由および権利は、憲法の下で保障されなければならない。」

データの活用中およびその後に事後的な管理権があることを保証している。特定の前提条件の下では、影響を受ける者には同意の有無にかかわらず個人データの収集、処理、および活用について事後の権利がある。加えて、事後的な管理権には個人データを削除する権利や、個人データの活用を停止または制限する権利が含まれる。

(2)　情報自己決定権またはプライバシー権

米国憲法には情報自己決定を表す用語がない。プライバシー権の概念を利用しており、それに情報自己決定権の保護も含まれている。ドイツ連邦憲法裁判所が 1983 年の国勢調査判決において *the right to informational self-determination*（すなわち情報自己決定権）という用語を考案しており、一般的人格権や人間の尊厳に由来している。

台湾では、TCC がプライバシー権の劣位型として「情報プライバシー権（the right to informational privacy）」という用語を用いており、その側面を情報自己決定権と名付けている。特に指摘すべき点として、TCC は自由な立憲民主主義の中核的な価値が人の尊厳を守り、人格の自由な発展を尊重することであるという考え方からプライバシー権を導出しているため、私生活の私的領域を侵入から守るとともに、個人情報の自己決定を保護している（司法院解釈第 603 号の判示）。

台湾の一部の学者は、情報自己決定権と情報プライバシー権の内容、性格、および保護範囲は異なっていると主張している。彼らによると、前者は個人的な行動の外的自由を保護しており、個人情報を処分する権利が外部から抑圧、制限、または妨げられていない限りそれを保障している。後者は内的な人格形成という柔軟な空間を保護しており、細かい個人情報とその人格や主観性との密接な結びつきにより多くの重要性を持たせている。しかし、筆者の意見では、情報プライバシー権と情報自己決定権の間には本質的な違いはない。大事なのは、我々による内容の解釈の仕方と適用範囲である。台湾憲法裁判所の解釈から判断すると、プライバシーという用語には自己決定の意味が含まれている。情報プライバシーと情報自己決定を区別することは、プライバシーと自己決定の意味を制限することである。この文脈の下、本稿では、情報プライバシー権の範囲に情報自己決定権を含めるものとする。

② 個人情報保護制度の憲法上の意義

コンピュータ処理個人情報保護法（Computer Processed Personal Data Protection Act）は改正され、同法の題名も個人情報保護法へと変更された。

台湾の現行の個人情報保護法（以下「PDPA」）は 2010 年に制定され、1995 年のコンピュータ処理個人情報保護法（以下「CPDPA」）に取って代わった。改正した条項は 2012 年 10 月 1 日に施行された。CPDPA も PDPA もプライバシー権や情報自己決定権には言及していない。議会による改正した条項の説明では、頻繁に「プライバシー」に言及している。これは、個人データのプライバシーが PDPA の主な検討事項であることを表している。

人格権の保護は、PDPA で明記されている目標の一つである。また、PDPA に情報プライバシーや情報自己決定が含まれていることで、人格権の解釈が強化される。PDPA の前身である CPDPA によると、本人の同意は政府機関や非政府機関による個人データの収集の法的根拠の一つであり、個人データの利用は元の収集目的に原則的に制限されていた。これは、当時個人データの自律性が形成されたことを示している。現行 PDPA ではインフォームドコンセントに重点を置いており、個人データの主体による管理を保証している。このことは、情報自己決定権が PDPA の原則であるという立法的な考え方も反映している。

2. 個人情報保護法制の現状と課題

①他国における法制度の影響

PDPA の前身である CPDPA の制定は、1980 年に OECD が採択した「プライバシー保護と個人データの国際流通に関するガイドライン（Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data）」の八つの原則を参照している（すなわち収集制限の原則、データ内容の原則、目的明確化の原則、利用制限の原則、安全保護の原則、公開の原則、個人参加の原則、責任の原則）。

PDPA の一部の条項の改正では、個人データの処理に関する個人の保護とかかるデータの自由な移動を扱った指令 95/46/EC（GDPR の前身）の要件に言及している（すなわち、データの品質、データ処理の合法性、機微データの処理、関係者への通知、関係者の権利、関係者の異議、自動化された個人の意思決定、データの機密性とセキュリティ、登録、処理業務の公表、国際的なデータ移転）。

②「個人データ」の定義と範囲

全体的に、台湾の PDPA における個人データの定義は GDPR のそれと類似している。基準は、自然人を直接的または間接的に識別できるかどうかである。

死者の個人データは除外される。暗号化[2] 又は非識別化した[3] データが PDPA の適用範囲内であるかどうかは、人がデータを比較、結合、または接続した後に識別できるかどうかによる。クッキーが個人データであるかどうかは、特定のケースにおいて収集されたデータにより人を直接的または間接的に識別できるかどうかによる。「個人データ」の定義と範囲に関する PDPA と GDPR の比較をまとめている。

GDPR	個人情報保護法
GDPR4 条（1）： 「個人データ」とは、特定された、または識別可能な自然人（「データ主体」）に関するあらゆる情報を意味し、識別可能な自然人とは、特に氏名、識別番号、位置情報、オンライン識別子などの識別子、またはその自然人の身体的、生理的、遺伝的、精神的、経済的、文化的、社会的アイデンティティに固有の 1 つ以上の要素を参照して、直接的または間接的に識別できる自然人を指す。 ▪ GDPR は死者の個人データには適用されない。（前文 27）	PDPA2 条 1 項： 「データ」とは、自然人の氏名、生年月日、ID カード番号、パスポート番号、特徴、指紋、配偶者の有無、家族情報、学歴、職業、医療記録、ヘルスケアデータ、遺伝子データ、性生活に関するデータ、身体検査記録、犯罪記録、連絡先情報、財務状況、社会活動に関するデータ、その他自然人を直接的または間接的に特定するために使用される可能性のある情報を指す。 ▪ 第 3 条　PDPA の施行規則： PDPA2 条 1 項 1 号の「間接的に識別される」状況とは、当該データを保有する政府機関または非政府機関が、当該データを他のデータと比較、結合、 または連結しない限り、データ主体を直接識別できない状況を意味する。

[2] 国家発展委員会 fa-fa-zi No. 1090004500 の行政規定も参照も参照：「暗号化されたデータは、特定の個人を直接識別することはできないが、比較、結合、接続の結果、個人を識別できる場合は、個人情報保護法にいう個人情報に該当する。」

[3] 国家発展委員会 fa-fa-zi No. 1080081030 の行政規定も参照：「電子試験センターによる個人データ非識別化認定に合格したデータについて、個人情報保護法が適用されるかどうかは、非識別化されたデータが直接的または間接的に特定の個人を識別するために利用できるかどうかにより決まる。争点は司法判断により決定される。」

	・個人データとは、生きた自然人のデータのことを意味する。死者のデータは、PDPA による保護の範疇の外である。（国家発展委員会 fa-fa-zi No. 1090021610）

③データ主体の権利と事業者の義務

A. データ主体の権利

PDPA 第 3 条によると、データ主体はその個人データに関して、1. 自分の個人データについて照会し、その内容を確認する権利、2. 自分の個人データの複製を要求する権利、3. 自分の個人データを補足または訂正する権利、4. 自分の個人データの収集、処理、または利用の停止を要求する権利、5.　自分の個人データを消去する権利を行使できなくてはならず、これらの権利は前もって契約上放棄または制限されてはならない。これに基づき、本法の下、データ主体にはその個人データに関して少なくとも以下の権利があると理解できる。

1. 照会またはアクセスを要求する権利
2. 複製を要求する権利
3. 訂正または補足を要求する権利
4. 収集、処理、または活用の停止を要求する権利
5. 削除を要求する権利

PDPA の規定に基づいた各権利の具体的な内容は以下のとおりである。

1. 照会またはアクセスを要求する権利：データ主体は政府機関または非政府機関に照会に応じ、データ主体が収集された個人データを確認することを許可してもらうよう要求できる（10 条 1 項）。
2. 複製を要求する権利：データ主体は、政府機関または非政府機関に、自分について収集された個人データの複製を提供してもらうよう要求できる（10 条 1 項）。
3. 訂正または補足を要求する権利：データ主体は、政府機関または非政府機関に、機関が所有する彼らの個人データの正確性を確保し、かかるデータの訂正または補足を行うよう要求できる（11 条 1 項）。
4. 収集、処理、または活用の停止を要求する権利：

(1) 個人データの正確性に関する紛争が生じた場合、データ主体は、政府機関または非政府機関に個人データの処理または利用を停止するよう要求できる（11条2項）。
(2) データ収集を行うための具体的な目的が存在しなくなった場合、または該当する期間が満了した場合、データ主体は、政府機関または非政府機関に個人データの削除またはその処理または利用を停止するよう要求できる（11条3項）。
(3) 個人データの収集、処理、または利用がPDPAに違反する場合、データ主体は、政府機関または非政府機関に、収集された個人データを削除するか、個人データの収集、処理、または利用を停止するよう要求できる（11条4項）。

5. 削除を要求する権利：
(1) データ収集を行うための具体的な目的が存在しなくなった場合、または該当する期間が満了した場合、データ主体は、政府機関または非政府機関に個人データの削除またはその処理または利用を停止するよう要求できる（11条3項）。
(2) 個人データの収集、処理、または利用がPDPAに違反する場合、データ主体は、政府機関または非政府機関に、収集された個人データを削除するか、個人データの収集、処理、または利用を停止するよう要求できる（11条4項）。

GDPRとは対照的に、台湾のPDPAにはデータ・ポータビリティ権、自動処理のみに基づいた決定に同意する権利、または（GDPR17条の忘れられる権利と同様の）個人データが収集または処理された目的に関係して必要でなくなった個人データを削除する権利の規範がない。

B. 政府機関の義務：

PDPA6条1項に規定されている個人データを除き（自然人の診療記録、ヘルスケア、遺伝子、性生活、身体検査、および犯罪歴に関するデータ）、政府機関による個人データの収集または処理は具体的な目的の下で、以下の根拠のいずれかに基づいて行われること：

1. その法廷義務を履行するために必要な範囲内にあること
2. データ主体による同意[4] が与えられていること、または

[4] 第15条1項の2で言及している「同意」とは、データ主体がPDPAに基づいて必要とされる情報についてデータ収集者により知らされた後に当該データ主体が与えた合意の宣言のことを意味する（第7条1項）。(Art. 7 para. データ主体の同意は、第15条1項の2に従い、データ主体が異議を申し立てず、政府機関または非政府機関がデータ主体にPDPA8条1項で規定されている関連情報について知らせた後に

3. データ主体の権利と利益が侵害されていないこと（PDPA15 条）。

政府機関は、PDPA の第 15 条または第 19 条に従って個人データを収集する場合、データ主体に以下の情報を明確に知らせること：

1. 政府機関または非政府機関の名称
2. 収集の目的
3. 収集する個人データのカテゴリ
4. 個人データを利用する期間、地域、受領者および方法
5. 第 3 条に基づいたデータ主体の権利とかかる権利を行使する方法
6. データ主体がその個人データを提供しないことを選択する場合に影響を受ける当該データ主体の権利と利益（PDPA8 条 1 項）

政府機関または非政府機関は、第 15 条または第 19 条に従ってデータ主体が提供していない収集された個人データを処理または利用する前に、データ主体にデータソースと、第 8 条 1 項の 1～5 で規定されているその他の情報を知らせること（PDPA9 条 1 項）。

政府機関は、以下の情報をオンラインで公開するか、一般社会が他の適切な手段を通じて照会できるようにすること。また、以下の情報に如何なる変更が施された場合も適用されるものとする。

1. 個人データファイルの名称
2. 個人データファイルを所有する機関の名称と連絡先
3. 個人データファイルを保管するための法的根拠と目的
4. 個人データのカテゴリ（PDPA17 条）

個人データファイルを所有する政府機関は、個人データの盗難、改竄、損害、破壊、または公開を防ぐために

セキュリティ対策や維持管理を実施するための専門の人員を割り当てること。（PDPA18 条）

C. 非政府機関の義務

PDPA6 条 1 項に規定されている個人データを除き（自然人の診療記録、ヘルスケア、遺伝子、性生活、身体検査、および犯罪歴に関するデータ）、政府機関による個人データの収集または処理は具体的な目的の下で、以下の根拠のいずれかに基づいて行われること：

データ主体が積極的に個人データを提供する場合に同意するものと見なせる（7 条 3 項）。

1. 法律により明確に必要であること
2. 非政府機関とデータ主体の間に契約関係または準契約関係があり、個人データのセキュリティを保証するために適切なセキュリティ対策が講じられていること
3. 個人データがデータ主体により一般公開されている、又は合法的に一般公開されている場合
4. データ提供者により処理された、またはデータ管理者により公開されたかかるデータが特定のデータ主体の識別に繋がらないことを前提に、公益を追求するための学術機関による統計収集または学術研究に必要であること
5. データ主体により同意が与えられていること[5]
6. 公益を促進させるために必要であること
7. データ主体がかかる個人データの処理または利用を禁止することについて個人の利益を上回る利益がある場合を除く、個人データが一般公開されているソースから取得されていること
8. データ主体の権利と利益が侵害されていないこと（PDPA19 条 1 項）。

非政府機関は、PDPA の第 15 条または第 19 条に従って個人データを収集する場合、データ主体に以下の情報を明確に知らせること：

1. 政府機関または非政府機関の名称
2. 収集の目的
3. 収集する個人データのカテゴリ
4. 個人データを利用する期間、地域、受領者および方法
5. 第 3 条に基づいたデータ主体の権利とかかる権利を行使する方法
6. データ主体がその個人データを提供しないことを選択する場合に影響を受ける当該データ主体の権利と利益（第 8 条 1 項）

非政府機関は、第 15 条または第 19 条に従って

データ主体が提供していない収集された個人データを処理または利用する前に、データ主体にデータソースと、第 8 条 1 項の 1～5 で規定されているその他の情報を知らせること（PDPA9 条 1 項）。

---

[5] 第 19 条 1 項の 5 で言及している「同意」とは、データ主体が PDPA に基づいて必要とされる情報についてデータ収集者により知らされた後に当該データ主体が与えた合意の宣言のことを意味する（第 7 条 1 項）。データ主体の同意については、第 19 条 1 項の 5 に従い、データ主体が異議を申し立てず、政府機関または非政府機関がデータ主体に PDPA8 条 1 項で規定されている関連情報について知らせた後にデータ主体が積極的に個人データを提供する場合に同意するものと見なせる（第 7 条 3 項）。

個人データを所有する非政府機関は、個人データの盗難、改竄、損害、破壊、または公開を防ぐために適切なセキュリティ対策を実施すること。（27 条 1 項）

④ 個人情報保護法を執行する監督機関の組織と権限

台湾では、個人情報保護に関する単一の所轄官庁がまだない。このことは、個人情報保護が分散型であることを意味している。行政機関は、それぞれの実務についてデータ保護の責任を負う。行政院は、個人データ保護の観点から非政府機関の監督を行う中央管理東京の一覧を定めている。[6]

台湾憲法裁判所は、判決 111-Hsien-Pan-13（2022）において、PDPA には個人データ保護のための独立した監督機構が欠けていると判示している。情報プライバシーの保護は不十分である。これは憲法に違反している可能性がある。関連する仕組みは、三年以内に創設させるべきである。

行政院は、2023 年 4 月 13 日に、PDPA の所轄官庁として個人情報保護委員会を設置する新たな 1-1 条を PDPA の改正案として導入している。PDPA の新たな 1-1 条は 2023 年 5 月 31 日に立法院により可決したが、まだ発効には至っていない。第 1-1 条が発効する日付を指定する権限は行政院に委ねられている。

⑤ 司法的救済の仕組み（訴訟要件、集団訴訟の可能性）

個人情報保護の救済という問題は前述のデータ主体の権利と密接に関係しており、相互依存的な関係を形成している。台湾の救済制度では、債務者が政府機関である場合は行政訴訟手続きを通じて救済を図り、非政府機関である場合は民事訴訟手続きを通じて図られる。これらの救済は、個人情報保護法（PDPA）では直接規定されていない。しかし、これらは違反の性質に基づいており、行政不服審査法、行政事件訴訟法、および民事訴訟法の規定に従って進められている。加えて、PDPA には、以下にまとめているとおり、損害賠償について具体的な規定を定めている。

A. 請求の根拠と責任の原則

1. 政府機関：

(1)

6 https://www.moj.gov.tw/media/16809/542114375377.pdf?mediaDL=true

政府機関は、天災、非常事態またはその他の不可抗力による場合を除き、当該政府機関の個人情報保護法違反に起因する個人情報の不法な収集、処理、利用、またはデータ主体の権利侵害によって生じた損害に責任を負うものとする。（28 条 1 項）

→政府機関は、ほぼ無過失な責任を負う。

(2) 被害者が被った損害が非金銭的損害である場合、被害者は適切な額の金銭賠償を請求することができ、被害者が被った損害が名誉の毀損である場合、被害者は名誉回復のための適切な是正措置を請求することができる。（28 条 2 項）

2. 非政府機関：

(1) 非政府機関は、その故意または過失によって生じたものではないことを証明できない限り、個人情報の違法な収集、処理、利用、またはその他のデータ主体の権利侵害によって生じた損害について責任を負うものとする。（29 条 1 項） → 立証責任は非政府機関に移される。

(2) 被害者が被った損害が非金銭的損害である場合、被害者は適切な額の金銭賠償を請求することができ、被害者が被った損害が名誉の毀損である場合、被害者は名誉回復のための適切な是正措置を請求することができる（29 条 2 項を 28 条 2 項を準用）

B. 補償の制限

1. 政府機関：

(1) 前 2 項の状況において、被害者が実際の損害の金銭的価値を証明することが困難または不可能である場合、被害者は裁判所に対し、損害の重大性に基づき、1 人 1 事件につき 500 元以上 2 万元以下の賠償額を請求することができる。（28 条 3 項）

(2) 複数のデータ主体の権利が同一の事件により侵害された場合、かかるデータ主体に対する損害賠償の総額は NT$2 億を超えないものとする。ただし、当該事件に関与する利益が NT$2 億を超える場合、損害賠償は当該利益の価額を上限とする。（28 条 4 項）

2. 非政府組織についても上記のとおりである（PDPA29 条 2 項）。

3. PDPA の規定の他に、損害賠償の法的根拠として（31 条）：

(1) 国家賠償法が政府機関を適用できる

(2) 民法典を非政府機関に適用できる

4. 集団訴訟（第 32 条～第 40 条）

(1) 同一の事件により複数のデータ主体の権利が侵害された場合、財団法人または公益法人は、少なくとも 20 人のデータ主体の訴訟権の委任状を取得した後、自己の名で裁判所に訴訟を提起することができる。（34 条 1 項）

(2) 台湾では、国家賠償請求訴訟は民事裁判所が審理し、民事訴訟法の規定が適用される（国家補償法 12 条）。したがって、前述の集団訴訟に関する規定は政府機関に対する国家賠償請求訴訟にも適用される。救済に関する PDPA と GDPR の比較を以下に列挙する。

GDPR	個人情報保護法
GDPR77 条（1）： 他の行政上または司法上の救済手段を損なうことなく、データ主体は、自己に関する個人情報の処理が本規則に違反していると考える場合、特に、自己の居住地、勤務地または違反が疑われる場所の加盟国において、監督当局に苦情を申し立てる権利を有する。 GDPR79 条（1）： 第 77 条に基づき監督機関に苦情を申し立てる権利を含む、利用可能な行政的または非司法的救済手段を損なうことなく、各データ主体は、本規則に準拠していない個人情報の処理の結果、本規則に基づく自己の権利が侵害されたと考える場合、効果的な司法的救済を受ける権利を有する。	救済[7] 28 条 1 項（政府機関）： 政府機関は、天災、非常事態またはその他の不可抗力による場合を除き、当該政府機関の個人情報保護法違反に起因する個人情報の不法な収集、処理、利用、またはデータ主体の権利侵害によって生じた損害に責任を負うものとする。 →政府機関は、損害が自然災害、緊急事態、またはその他の不可抗力により生じた場合に限り、責任を免除される。

[7] 複数のデータ主体の権利が同一の事件により侵害された場合、かかるデータ主体に対する損害賠償の総額は NT$2 億を超えないものとする。ただし、当該事件に関与する利益が NT$2 億を超える場合、損害賠償は当該利益の価額を上限とする。（28 条 4 項、29 条 2 項）。28 para. 4, Art. 2)

GDPR82 条（1）： 本規則の侵害により物質的または非物質的損害を被った者は、被った損害について管理者または処理者から補償を受ける権利を有する。 GDPR82 条（2）： 処理に関与する管理者は、本規則に違反する処理によって生じた損害について責任を負うものとする。処理者は、特に処理者に向けられた本規則の義務を遵守しなかった場合、または管理者の合法的な指示の範囲外もしくは指示に反して行動した場合に限り、処理によって生じた損害について責任を負うものとする。 GDPR82 条（3）： 管理者または処理者は、損害の原因となった事象についていかなる責任も負わないことを証明する場合、第 2 項に基づく責任を免除されるものとする。GDPR80 条（1）：	これは GDPR よりも厳格である。 29 条 1 項（非政府機関）： 非政府機関は、その故意または過失によって生じたものではないことを証明できない限り、個人情報の違法な収集、処理、利用、またはその他のデータ主体の権利侵害によって生じた損害について責任を負う。 → 非政府機関は、損害がその故意または過失により生じたものではないことを証明できる場合に責任を免除できる。これは GDPR と同様である。 第 34 条第 1 項前段（集団訴訟）： 同一の事件により複数のデータ主体の権利が侵害された場合、財団法人または公益法人は、少なくとも 20 人のデータ主体の訴訟権の委任状を取得した後、自己の名で裁判所に訴訟を提起できる。
データ主体は、加盟国の法律に従って適切に構成され、公益を目的とする法的目的を有し、個人情報の保護に関してデータ主体の権利および自由を保護する分野で活動している非営利団体、組織または協会に対し、自己に代わって苦情を申し立て、自己に代わって第 77 条、第 78 条および第 79 条に規定される権利を行使し、加盟国の法律に規定されている場合には、自己に代わって第 82 条に規定される補償を受ける権利を行使するよう委任する権利を有する。	

追加の質問：研究・医薬品開発を目的とした診療データの二次利用

診療記録等を医薬品開発などの研究目的で利用する場合に、データ主体である患者の同意は要請されるのか。診療データを二次利用するにあたって、匿名加工などの一定の義務が課せられるか？

PDPA6 条 1 項の 4 但し書によると、自然人の診療記録、ヘルスケア、遺伝子、および身体検査に関するデータは、データ提供者が処理したとおり、またはデータ管理者が開示したとおりのかかるデータが特定のデータ主体の識別に至らない限り、ヘルスケア、公衆衛生、または防犯を目的とした政府機関または学術機関による統計収集または学術研究のために必要な場合に収集、処理、および利用できる。言い換えると、データ主体を識別できなければ、患者の同意なしに診療データを収集、処理、または利用できるのである。

憲法裁判所は、判決 111-Hsien-Pan-13（2022 年）[8] において、PDPA と他の関連規制にはデータ保護のための独立した監督手段が欠けていると判示している。

[8] 本判例の背景：全民健康保険被保険者は契約医療機関による医療サービスを受けるが、これは全民健康保険法（NHIA）80 条によると、

所轄官庁は、判決の発表から 3 年以内に、関連する法的仕組みを制定することを保証しなければならない。

全民健康保険法 79 条によると、衛生福利部全民健康保険局は、保険事業を運営するために必要な情報を提供するよう関連する機関に要求できる。全民健康保険法 80 条によると、所轄官庁は被保険者、団体保険申請者、保険料徴収者、および契約下にある医療機関に、会計記録、領収書、病歴、診断記録、または医療支出額などの関連する文書や、その他の文書または関連情報を提供するよう求めることができる。

憲法裁判所は同判決において、全民健康保険法の 79 条と 80 条には、データベースとして全民健康保険データの保存、処理、外部送信、および全民健康保険局（National Heatlh Insurance Administration）により外部から提供されるための対象、目標、法的要素、範囲、および措置に関する明示的な規制が欠けていると判示している。また、記載されている規定は、組織的および手続き上のデータ保護事項に関する監督手段などの重要な事項について明示的な規制も提供できていない。これらは、憲法 22 条により保証されている情報プライバシー権に違反している。所轄官庁は、三年以内に、当該規定を改正するか、特別法を制定すること。

加えて、憲法裁判所は同判決において、全民健康保険局から他の政府機関または学術研究機関へ送信された、元の収集目的の範疇を超える個人的な健康保険データの利用に関して、現行の法体系にはデータ主体がオプトアウトすることを可能にする規制が欠けており、そのため憲法 22 条により保証される情報プライバシー権に違反していると判示している。

医療費を請求するために関連する診療記録と処方データを全民健康保険局に提供している。

長年にわたり、全民健康保険局は膨大な量の健康保険データを収集しており、その中には個人的な健康保険データも含まれる。全民健康保険局は、一般公開されている「全民健康保険研究データベース」を構築するためにデータを国家衛生研究院に提供している。また、一般公開されている健康保険データを衛生福利部（MHW）衛生福利データ科学センターにも送信している。

申立人の意見は、憲法上のプライバシー権により守られている彼らの個人健康保険データが全民健康保険による事業の範疇を超える目的で利用されていることから、当該行為が違法行為であるというものであった。彼らは、全民健康保険局が、全民健康保険による事業の範疇を超える目的で他者に彼らの個人健康保険データを提供してはならないと主張したのである。

全民健康保険局は、この主張を棄却している。これに対し、申立人は行政訴訟を開始した。最終判決で判例に敗訴した後、申立人は個人情報保護法 6 条 1 項の 4 但し書及び全民健康保険法の 79 条 1 項及び 80 条 1 項が違憲であると主張し、違憲審査を請求している。

所轄官庁は、三年以内にオプトアウトの対象、根拠、手続き、および効果を規定する、またはオプトアウトを拒否する法律を改正または制定すること。
当該法律の改正または制定の期限が過ぎている場合、データ主体は元の目的以外でのデータ利用を停止するよう要求すること。

批判すべき点：

1. 本判決は、個人情報保護法 6 条 1 項の 4 但し書が全民健康保険局による国家衛生研究院に対する全民健康保険研究データベースを設立するための健康保険データを提供するための法的根拠となりえるかどうかという問いを明確にしていない。

2. 本判決が影響を受ける人が持つ活用停止を求める権利の規制する規定を立法府に求めているものの、影響を受ける人の同意を伴わない強制的な収集、処理、または活用（個人情報プライバシー権から生じる事前同意を伴う個人データを影響を受ける者が管理する権利の制限）を可能にする個人情報保護法 6 条 1 項の 4 但し書の合憲性を認めていることは矛盾しているように思える。活用を停止する権利、またはオプトアウトする権利は、影響を受ける者の事前同意を前提としている。オプトインする権利とは対照的である。法的な前提条件の下で公的機関が影響を受ける者の同意なしに個人データを強制的に収集、処理、または活用できるのであれば、影響を受ける者はどのようにして活用を停止する権利を行使できるのだろうか？対照的に、影響を受ける者がその個人データの活用を停止する権利を享受している場合、公的機関はどのようにして個人データを強制的に収集、処理、または活用できるのだろうか？

※本研究は、JST【ムーンショット型研究開発事業】グラント番号【JPMJMS2293】の支援を受けたものです。

Ⅶ. 韓国

韓国法における個人情報自己決定権の保護

慶應義塾大学 訪問研究員 尚知永（サン·ジヨン）

I. はじめに

韓国法上の個人情報の主体は、自己の個人情報に関して憲法上の基本権として「個人情報自己決定権」を有する。本稿では、韓国憲法上の個人情報自己決定権の意味について述べ、さらに、その個人情報自己決定権が具体的な法律（「個人情報保護法」）を通じて如何に保護されているかについて取り上げる。

II. 情報主体の憲法上の基本権としての個人情報自己決定権

1. 個人情報自己決定権の意義

韓国の憲法には、明文の条項として個人情報自己決定権が示されていない。しかしながら、２００５年、個人の指紋情報を収集・保管・電算化してそれを犯罪捜査のために利用されるようにした旧住民登録法の関連条項などが違憲かどうかが問題になった事件において、憲法裁判所が個人情報自己決定権を憲法上の独自の基本権として認めた以来（憲法裁判所２００５年5月２６日宣告９９憲マ５１３、２００４憲マ１９０（併合）決定[1]、以下「指紋情報事件」）、かかる権利は憲法上の基本権として認められている。

上記の指紋情報事件の判示で定義された個人情報自己決定権とは、「自己に関する情報が、いつ、誰に、どの範囲まで知られ、また利用されるようにするかをその情報主体が自ら決める権利、すなわち情報主体が個人情報の開示・利用に関して自ら決める権利」をいう。このような個人情報自己決定権の概念は、ドイツ連邦憲法裁判所が１９８３年「人口調査事件（BVerfGE 65,1）」で最初に判示した情報自己決定権（die Recht auf informationelle Selbstbestimmung）、すなわち「自己の個人的情報のどれを第三者に開示して利用させるかを自ら決める権利」の影響を受けたものと評価されている[2]。

---

[1] 憲法裁判所は、審判対象条項は、個人情報である指紋を収集してそれを犯罪捜査などに利用することで個人情報自己決定権を制限するものであるが、これは法律留保原則及び過剰禁止原則に反しないため、個人情報自己決定権を侵害したとはいえないと判断した。

[2] クォン・ヨンジュン、「個人情報自己決定権と同意制度に対する考察」、法学論叢第３６巻第１号、２０１６、６７７頁；チェ・ソンヒ、「個人情報自己決定権と忘れられた憲法裁判所決定などのための弁明」、情報法学第２０巻第3号、２０１７、３０６頁

憲法裁判所は、上記の指紋情報事件で「新しい独自的基本権としての個人情報自己決定権を憲法的に承認する必要性」が台頭した背景について、現代の情報通信技術の発達によって国の個人情報の収集・処理力量が強化されたことに注目した。また、このような社会的状況のもとで個人情報自己決定権を憲法上の基本権として承認することは、「現代の情報通信技術の発達に内在する危険性から個人情報を保護することで、窮極的には個人の決定の自由を保護し、さらに自由民主体制の根幹が総体的に損ねられる可能性を遮断するうえで必要な最小限の憲法的保障装置」であると判示した。

個人情報自己決定権が初めて認められた２００５年の指紋情報事件以降にも情報通信技術の発達は一層加速化しており、かかる技術を基に、国に限らず、私人（各種企業や団体など）が個人情報を収集・処理しようとする需要や力量も共に急速に高まっている。また、情報主体にとっても、発達された情報通信技術によってその力量が強化された個人情報処理者が情報主体の権利を侵害しないように防ぐなど、個人情報自己決定権を防御的に行使するだけでなく、一方では発達した技術を基に様々な方面に分散している自己の個人情報を能動的に活用して管理するなど、個人情報自己決定権を積極的に行使しようとする需要もますます増えていくことが見込まれる。

結局、「自己に関する情報がいつ、誰に、どの範囲まで知られ、また利用されるようにするか」を自ら決める個人情報自己決定権は、今後の現代社会でより重要な意味を持つようになると考えられる。

2. 憲法に示されていない独自的基本権としての個人情報自己決定権

ア. 個人情報自己決定権の憲法上の根拠

前述のとおり、韓国の憲法には明文の条項として個人情報自己決定権が基本権として示されていない。そうであれば、個人情報自己決定権の憲法上の根拠は何か？

憲法第１０条第１文
すべての国民は、人間としての尊厳と価値を持ち、幸福を追求する権利を有する。

憲法第１７条
すべての国民は、私生活の秘密と自由を侵害されない。

憲法裁判所は、２００５年の指紋情報事件で、個人情報自己決定権の理念的基礎として、憲法第１０条第１文（人間の尊厳と価値及び幸福追求権に基づく一般的人格権）、憲法第１７条（私生活の秘密と自由）、憲法の自由民主的な基本秩序ルールや国民主権原理と民主主義の原理などを考慮することができるとしながらも、個人情報自己決定権により保護しようとする内容をこのような各基本権など及び憲法原理などの一部に完全に取り込ませることは不可能なので、個人情報自己決定権の憲法的根拠を敢えて一部に限定することは望ましくないとし、結局、個人情報自己決定権とはこれらを理念的基礎とする「独自的基本権であって、憲法に示されていない基本権」と認めた。

ちなみに、指紋情報事件以降の憲法裁判所による決定例などによれば、個人情報自己決定権の憲法的根拠として「自由民主的な基本秩序や国民主権原理など」に触れずに、憲法第１０条第１文と第１７条のみに触れている傾向がある（憲法裁判所２０１５年6月２５日宣告２０１４憲マ４６３決定など）。この点に関して、憲法裁判所がその後の判示などで自由民主的な基本秩序や国民主権原理などに触れなくても、指紋情報事件決定に同じ説示を繰り返したり、そのまま引用していることなどに照らし、憲法裁判所の個人情報自己決定権の捉え方について従来の指紋情報事件決定の説示から逸脱したりその見解を変えたとは言い難いという意見がある[3]。

イ．プライバシー権との関係

個人情報自己決定権の憲法的根拠ないし理念的基礎になる憲法第１７条における私生活の秘密と自由は、プライバシー権（Right to privacy）にも密接な関わりがある。プライバシー権の意義や脈絡は、様々な観点によって理解されることができ、各観点によって韓国憲法上のプライバシー権の意味もそれぞれ別に理解されると考えられる。

まずプライバシー権を狭く理解する場合（狭義説）、これは私生活の平穏が侵害されず私生活の秘密がむやみに開示されない権利であるといえる。これは初期に米国で認められた概念であり、私生活の領域から派生される各種の事実が他人に露出しない消極的権利（right to be alone）にあたると考えられる。一方、このような消極的な性格の権利に加え、積極的な性格の権利として自己に係る私的な生活や情報を管理・統制する権利もプライバシー権に含まれるという見解があり、これは近来学界の多数説（広義説）と捉えられている[4]。

憲法裁判所は、多くの決定例で、憲法第１７条の私生活の秘密や自由について、私生活の秘密とは「私生活に関わりのある、自分だけの私的な領域が本人の意思に反して他人に知られないようにする権利」であり、私生活の自由とは「社会共同体の一般的な生活ルールの範囲内で私生活を自由に形成していき、その設計や内容について外部から干渉されない権利」であるとしている[5]。案ずるに、この憲法裁判所の判示は、憲法第１７条を基本的に消極的な性格の権利と捉えながらも、その中で積極的に「私生活を自由に形成できる権利」があることを認めたものであり、このような流れから憲法第１７条は前述の広義のプライバシー権の概念に相応しいものと考えられる。

ところで、このようなプライバシー権の概念を前提とすれば、プライバシー権の保護法益は、自己の私生活の秘密に係る事項を自由に形成・維持し、それをむやみに他人に開示されない法的利益であるといえる。このような私生活に係る情報は、個人の社会的評価を低下させ得る情報や隠密な私生活

---

[3] チェ・ソンヒ、「個人情報自己決定権と忘れられた憲法裁判所決定などのための弁明」、情報法学第２０巻第３号、２０１７、２９４～２９６頁。

[4] プライバシー権に関する韓国の諸学説を分類した内容は、パク・ソンヨン、「プライバシー権の比較憲法的研究」、西江大学校一般大学院、２０１６、３１～３３頁参照。

[5] 憲法裁判所２００２年3月２８日宣告２０００憲マ５３決定、憲法裁判所２００１年8月３０日宣告９９憲バ９２決定など。

情報であり、かかる情報の外部開示による名誉などの人格権を保護するためのものであるといえる[6]。一方、個人情報自己決定権については、情報主体が自己の個人情報が如何に利用されるかについて同意し、個人情報が如何に利用されているかを閲覧して確認するなど、個人情報に対する統制権限をその内容とするものと捉えるべきであり、個人に関する情報開示などによって私生活（プライバシー）が侵害されるかどうかは、その権利の一部に該当すると考えられる[7]。

そうであれば、個人情報自己決定権は自己に関する情報を自ら統制することができる権利であることから、上記のプライバシー権の概念範囲の一部と重なるといえるが、個人情報自己決定権とプライバシー権は基本的に権利保護の対象や目的が異なるといえる。憲法裁判所もこれらの点を考慮し、指紋情報事件で、個人情報自己決定権により保護しようとする内容を第１７条の私生活の秘密や自由など一部の基本権や憲法原理の一部に完全に取り込ませることができないとし、個人情報自己決定権を憲法に示されていない独自的基本権と認めたのではないかと考えられる。

III. 韓国の個人情報保護法上の個人情報自己決定権の保護

憲法上の基本権である個人情報自己決定権を具体的に実現する個別法としては、「個人情報保護法」がある[8]。個人情報保護法は２０１１年制定当時、「情報主体の権利を明確に定めることにより、情報主体がより容易に個人情報に対する自己統制権を実現」できるようにするために制定された（２０１１年３月２９日法律第１０４６５号に制定された個人情報保護法の制定理由を参照）。さらに、個人情報保護法第１条の目的規定には、このような制定目的に限らず、個人情報自己決定権の憲法的根拠になる憲法第１０条第１文（人間の尊厳と価値及び幸福追救権に基づく一般的人格権）の内容も入っていることがわかる。

個人情報保護法第１条（目的）
この法は、個人情報の処理及び保護に関する事項を定めることにより、個人の自由と権利を保護し、さらに個人の尊厳と価値を具現することを目的とする。

このような個人情報保護法は、個人情報の処理及び保護に関する事項を定める一般法の地位を有する（個人情報保護法第６条[9]）。個人情報の中でも、一部の個人情報（個人信用情報、個人位置情報など）においては優先して適用される特別法など（「信用情報の利用及び保護に関する法律」、「位

[6] イ・インホ、「第２世代プライバシー保護法としての個人情報保護法に対する理解」、司法第８号、２００９年６月、５６～６４頁。
[7] カン・ダルチョン、「個人情報自己決定権保護の限界の観点から見た「個人情報保護法」改正の問題点」、中央法学第２２集第３号、２０２０年９月、１５頁。
[8] クォン・ヨンジュン、「個人情報自己決定権と同意制度に対する考察」、法学論叢第３６巻第１号、２０１６年、６７８頁；カン・ダルチョン、「個人情報自己決定権保護の限界の観点から見た「個人情報保護法」改正の問題点」、中央法学第２２集第３号、２０２０年９月、２０～２１頁；キム・ヘウォン、「個人情報に対する憲法的検討」、公法学研究第２０巻第４号、２０１９年、８２頁。
[9] 個人情報保護に関しては、他の法律に特段の規定がある場合を除き、この法の定めによる。

置情報の保護及び利用などに関する法律」など）が存在するが、本稿では一般法である個人情報保護法を基準に情報主体の個人情報自己決定権が韓国の法制を通じて具体的に保護される態様について述べる。

1. 情報主体による権利行使

韓国の個人情報保護法は、次のように第４条に情報主体の権利を概括的に明示し、その権利などは「個人情報の開示と利用に関して自ら決める権利」である個人情報自己決定権の内容を要諦としている。

個人情報保護法[10]第４条（情報主体の権利）
情報主体は、自己の個人情報処理に関して次の各号の権利を有する。
1. 個人情報の処理に関する情報の提供を受ける権利
2. 個人情報の処理に関する同意の有無、同意の範囲などを選択して決める権利
3. 個人情報の処理有無を確認し、個人情報に対して閲覧（写し発給を含む）を要求する権利[11]
4. 個人情報の処理停止、訂正・削除及び破棄を求める権利
5. 個人情報の処理によって発生した被害が迅速且つ公正な手続によって救済される権利

本１.項（情報主体による権利行使）では、個人情報処理が通常的に行われる過程で情報主体が行使できる権利として個人情報保護法第４条第１号ないし第４号の各権利が如何に保障されるかについてまず取り上げる。また、異常な個人情報処理による被害に関し、情報主体が行使できる権利を項目を分けて２.項（司法的救済システムによる情報主体の被害救済）で取り上げる。

ア. 個人情報処理者への義務付与による間接的な権利保障

1) 個人情報処理に関する情報の提供を受ける権利

個人情報保護法は、個人情報処理者をして個人情報を収集・利用するなど個人情報を処理することに関する情報を情報主体に知らせることを義務づけている。詳しくは、個人情報処理者は個人情報の収集・利用・（第三者への）提供のために、その目的・範囲などを情報主体にあらかじめ告知して同意を得なければならない（個人情報保護法第１５条第２項、第１７条第２項、第３９条の３第１項

[10] 以下に引用する個人情報保護法の条文は、基本的に２０２３年７月施行されている現行法（２０２０年８月５日施行法律第１６９３０号）を基準とする。２０２３年３月１４日公布され、２０２３年９月１５日又は２０２４年３月１５日施行される改正個人情報保護法（法律第１９２３４号）条文の関連内容は、別途の注釈などに説明を加える。

[11] ２０２３年９月１５日施行される改正個人情報保護法のもとでは、第３号の「閲覧を求める権利」が「閲覧及び転送を求める権利」に改正され、「完全に自動化した個人情報処理による決定を拒否したり、それに対する説明などを求める権利」が第６号に新設された。この点、本１.項の「ウ.最近の改正により一層能動的な自己情報統制権を実現」の項目で詳述する。

[12]）。さらに、個人情報処理者が情報主体以外から収集した個人情報を処理するときは、その収集・出処・処理目的などをテキストメッセージ、電子メールなど情報主体がわかりやすい方法で情報主体に知らせなければならない（個人情報保護法第２０条第１項及び第２項[13]）。

一方、個人情報処理者は、個人情報の処理目的、保有・利用期間などを盛り込んだ個人情報処理方針（Privacy Policy）を策定して開示し（個人情報保護法第３０条第１項）、一定規模以上の情報通信サービスプロバイダーは、利用者に個人情報利用内訳を周期的に通知しなければならない（個人情報保護法第３９条の８第１項[14]）。

2) 個人情報処理に関する同意の有無、範囲などを選択して決める権利

個人情報自己決定権で重要なのは、情報主体が、個人情報処理者の個人情報処理に対して実質的な統制権を有することである。したがって、情報主体に個人情報処理の有無及び同意範囲などを選択できる権利を与えるとしても、個人情報処理者が事実上同意を強要すれば、情報主体の権利が形式化されてしまう恐れがある。個人情報保護法は、このような問題を解決するために、情報主体の個人情報自己決定権を保障すべく、その同意方法を法律で具体化して包括的な同意を禁止している（個人情報保護第２２条）[15]。

例えば、個人情報処理に関する重要事項は、字の大きさなどを別々にして明確に表示し、契約の締結などのために情報主体の同意なく処理できる（必須の）個人情報と、情報主体の同意を要する（選択的な）個人情報とを区分するなど、個人情報保護法第２２条は同意を得る方法をかなり詳しく規律している。大法院もまた、個人情報処理者が情報主体から適法な同意を得るためには、「利用者（情報主体）が個人情報の提供に関する決定権を十分自由に行使できるよう、情報通信サービスプロバイ

---

[12] 情報通信サービスプロバイダー（オンライン上、利用者の個人情報を収集及び利用する個人情報処理者など）に対する特例規定である第３９条の３は、２０２３年９月１５日施行される改正個人情報保護法のもとでは削除され、情報通信サービスプロバイダーも一般個人情報処理者と同様、個人情報収集・利用に関する規定が適用される。
ちなみに、過去の情報通信サービスプロバイダーに対する個人情報保護関連規定は「情報通信網の利用促進及び情報保護等に関する法律」で定められたが、当該内容が現行個人情報保護法（２０２０年２月４日法律第１６９３０号に改正されたもの）において特例規定である第３９条の３ないし第３９条の１５に移された。

[13] 個人情報処理者が規模などにおいて一定の基準に満たなければ、情報主体の要求があるときに限って関連情報を告知することができる（第２０条第１項）。

[14] 情報通信サービスプロバイダーに対する特例規定である第３９条の８は、２０２３年９月１５日施行される改正個人情報保護法のもとでは削除される。当該内容は、同日施行される改正法に新設される第２０条の２に移され、当該通知義務は情報通信サービスプロバイダーにとどまらず、個人情報処理者一般に拡大して適用される。このとき、一定基準以上の個人情報処理者（５万人以上の情報主体の敏感情報又は固有識別情報を処理する者、又は１００万人以上の情報主体の個人情報を処理する者）は、収集した個人情報の利用・提供の内訳や利用・提供の内訳がわかる情報システムに接続する方法を周期的に情報主体に通知しなければならない。

[15] 個人情報保護委員会、「個人情報保護法令及び指針・告示解説」、２０２０年１２月、３４頁及び１４７頁。

ダーがあらかじめ当該インターネットサイトに通常の利用者に法定告知事項[16]の詳細がわかりやすいよう法定告知事項の全部を明確に掲載しなければならない」と判示しました（大法院２０１６年6月２９日宣告２０１４ドゥ２６３８判決[17]）。

もっとも、２０２３年9月１５日施行される改正個人情報保護法のもとでは、上記第２２条の内容の多くが緩和され、これは従来の個人情報保護法における「同意万能主義」の問題[18]を解消しようという改正の趣旨が反映されたものとみられる[19]。これを補足すれば、韓国の個人情報保護法は、欧州連合のGeneral Data Protection Regulation（ 以下「ＧＤＰＲ」）に類似して個人情報の収集・利用の正当な根拠として、同意、法令上の根拠、公的業務の遂行、契約の締結・履行、重大な利益、正当な利益を並列的に並べているが（個人情報保護法第１５条第１項など）、多くの個人情報処理者は、同意なく個人情報処理が可能であるという点に対する立証責任を負わないために（同意がなくても個人情報を収集・利用することができる場合までも）一概に同意を通じて個人情報を収集・利用している。

これに対して、前述のとおり、規制機関や司法機関が「明確な告知による適法な同意を得なければならない」という立場を取るほど、個人情報処理者としては、却って法令上の基準に相応しい同意さえあれば個人情報の収集・利用は適法であるという認識が蔓延することになる一方、情報主体としては、同意書式の語句をきちんと確認せずに習慣的に同意したり、同意しなくては関連サービスを利用できないため仕方なく同意することが頻繁になる。

これらの点を踏まえ、２０２３年9月１５日施行される改正個人情報保護法は、個人情報の収集・利用の正当な根拠のうち「契約の締結・履行」要件を緩和[20]して不必要な同意徴求の慣行の解消を図

---

16 個人情報の収集・利用・提供をするために情報主体から同意を得る前に情報主体に必ず告知しなければならない事項である。例えば、個人情報の収集にあたり、個人情報の収集・利用目的、収集しようとする個人情報の項目、個人情報の保有及び利用期間、同意を拒否する権利があるという事実及び、同意拒否による不利益がある場合には、その不利益の内容が法定告知事項に該当する（個人情報保護法第１５条第２項）。

17 Webサイトのバナーやイベント広告のポップアップ画面を通じて個人情報の収集項目及び目的、保有期間に対する案内なく「確認」をクリックすれば同意したものとみなす方法であり、明示的な同意を得ずに利用者の個人情報を収集して保険会社などに提供した行為について、適法な同意のない個人情報提供行為であると判断したケース。

18 チョ・スヨン、「個人情報保護法における情報主体の同意と基本権保障に関する研究」、法学研究第１８巻第1号、２０１８年、３３１頁；個人情報保護委員会も、現行の同意制度に関して「複雑で硬直的な同意制度の運用により企業・機関などの個人情報処理者は合理的な個人情報の処理及び活用に制約を受け、情報主体も複雑な告知事項と手続などにより「同意の形式化」が蔓延」しているとした（個人情報保護委員会２０２３年3月7日付けプレスリリース１１頁）。

19 個人情報保護委員会の２０２３年3月7日付けプレスリリースによれば、２０２３年9月１５日施行される改正個人情報保護法は、「これまで情報主体の「同意」に過度に依存していた個人情報処理慣行から脱し、相互契約など合理的に予想できる範囲内では同意がなくても個人情報の収集・利用が可能になるよう整備」されたものである（個人情報保護委員会２０２３年3月7日付けプレスリリース３頁）。

20 現行の個人情報保護法上の関連要件は、「情報主体との契約の締結及び履行のためにやむを得ず必要な場合」となっているが（個人情報保護法第１５条第１項第４号）、２０２３年9月１５日施行される改正個人情報

り、前述の個人情報保護法第２２条もまた情報主体の同意なく処理できる個人情報に対しては、同意ではない関連する個人情報処理根拠に従ってこれを個人情報処理方針に開示しなければならないことを明確にする方向に改正された。

イ．情報主体が自ら行使できる権利の明示

1)　個人情報の処理有無の確認及び閲覧を求める権利

個人情報保護法第３５条（個人情報の閲覧）

① 情報主体は、個人情報処理者が処理する自己の個人情報の閲覧を当該個人情報処理者に求めることができる。

② 第１項にも拘わらず、情報主体が自己の個人情報の閲覧を公共機関に求めようとするときは、公共機関に自ら閲覧を求め、又は大統領令の定めによって保護委員会を通じて閲覧を求めることができる。

③ 個人情報処理者は、第１項及び第２項による閲覧を求められたときは、大統領令に定める期間内に情報主体が当該個人情報を閲覧できるようにしなければならない。この場合、当該期間内に閲覧することができない正当な事由があるときは、情報主体にその事由を知らせて閲覧を延期することができ、その事由が消滅すれば遅滞なく閲覧させなければならない。

④ 個人情報処理者は、次の各号の一にあたる場合には、情報主体にその事由を知らせて閲覧を制限・拒絶することができる。

1. 法律に基づいて閲覧が禁止・制限される場合
2. 他人の生命・身体を害する恐れがあり、又は他人の財産その他の利益を不当に侵害する恐れがある場合
3. 公共機関が次の各目の一にあたる業務を行うにあたり、重大な支障をもたらす場合
   - ア．租税の賦課・徴収又は還付に関する業務
   - イ．「小・中等教育法」及び「高等教育法」による各級学校、「生涯教育法」による生涯教育施設その他の法律に基づいて設置された高等教育機関での成績評価又は入学者の選抜に関する業務
   - ウ．学歴・技能及び採用に関する試験、資格審査に関する業務
   - エ．補償金・給付金の算定などについて行われている評価又は判断に関する業務
   - オ．その他の法律に基づいて行われている監査・調査に係る業務

⑤ 第１項から第４項までの規定による閲覧要求、閲覧制限、通知などの方法並びに手続に関して必要な事項は大統領令に定める。

情報主体は、個人情報処理者が処理する自己の個人情報に対する閲覧を当該個人情報処理者に求めることができる。かかる閲覧要求権は、個人情報処理者による無分別な個人情報の収集・利用の提供

保護法は、当該規定を「情報主体と締結した契約を履行したり契約を締結する過程で情報主体の要請による措置を履行するために必要な場合」に改正し、「やむを得ない」という要件を削除した。

を防ぐ機能を果たすことができる。

個人情報処理者が情報主体の閲覧を拒絶できる事由は、法律に基づいて閲覧が禁止・制限される場合、他人の生命・身体を害する恐れがあったり他人の財産その他の利益を不当に侵害する恐れがある場合、又は公共機関による特定業務の遂行に重大な支障をきたす場合に限られるため、個人情報処理者は情報主体の閲覧を任意に拒絶する余地がほとんどない。さらに、個人情報処理者は、情報主体から閲覧を求められたときは、１０日以内に情報主体が当該個人情報を閲覧できるようにしなければならない。

一方、情報主体は自己の個人情報の閲覧を求めるためには、個人情報処理者が設けた方法や手続に従って求めなければならない（個人情報保護法第３５条第５項、同法施行令第４１条第１項）。これは、一方的で非効率的な閲覧要求の濫用により、個人情報処理者の利益が不当に侵害されないようバランスをとったものと思われる。このとき、個人情報処理者は閲覧要求の方法や手続を設けるにおいて、個人情報を収集する方法や手続に比べて難しくしてはならない。

2) 個人情報の訂正・削除、処理停止及び破棄を求める権利

個人情報保護法第３６条（個人情報の訂正・削除）

① 第３５条に基づき、自己の個人情報を閲覧した情報主体は個人情報処理者に対してその個人情報の訂正又は削除を求めることができる。ただし、他の法令にその個人情報が収集対象に掲げられている場合には、その削除を求めることができない。

② 個人情報処理者は、第１項による情報主体の要求を受けたときは、個人情報の訂正又は削除に関して他の法令に特段の手続が規定されている場合を除き、遅滞なくその個人情報を調べて情報主体の要求に応じて訂正・削除など必要な措置を講じた上で、その結果を情報主体に知らせなければならない。

③ 個人情報処理者が第２項に基づいて個人情報を削除するときは、復旧又は再生されないよう措置を取らなければならない。

④ 個人情報処理者は、情報主体の要求が第１項但書きにあたるときは、遅滞なくその内容を情報主体に知らせなければならない。

⑤ 個人情報処理者は、第２項による調査を行うにあたり、必要に応じて当該情報主体に訂正・削除を求める事項の確認に必要な証拠資料を提出させることができる。

⑥ 第１項・第２項及び第４項による訂正又は削除の要求、通知方法及び手続など必要な事項は大統領令に定める。

情報主体は、個人情報保護法第３５条に基づいて自己の個人情報を閲覧した後、個人情報処理者にその個人情報の訂正・削除を求めることができる。この場合、個人情報処理者はその個人情報が他の法令に収集対象に掲げられていない限り、その訂正・削除を求められた日から１０日以内に当該個人情報の訂正・削除などの措置をとった事実（削除の要求に応じない法的根拠があれば、その事実及び理由と異議申立方法）を情報主体に知らせなければならない。一方、情報主体は、前述の閲覧要求と

同様、個人情報処理者が設けた方法や手続に従って訂正・削除を求めなければならない。

個人情報保護法第３７条（個人情報の処理停止など）

① 情報主体は、個人情報処理者に対して自己の個人情報処理の停止を求めることができる。この場合、公共機関に対しては、第３２条に基づいて登録対象になる個人情報ファイルのうち自己の個人情報に対する処理の停止を求めることができる。

② 個人情報処理者は、第１項による要求を受けたときは、遅滞なく情報主体の要求に応じて個人情報処理の全部を停止し、又は一部を停止しなければならない。ただし、次の各号の一にあたる場合には、情報主体の処理停止要求を拒絶することができる。

1. 法律に特段の規定があり、又は法令上の義務を守るために避けられない場合
2. 他人の生命・身体を害する恐れがあり、又は他人の財産その他の利益を不当に侵害する恐れがある場合
3. 公共機関が個人情報を処理しなければ他の法律に定める所管業務を行うことができない場合
4. 個人情報を処理しなければ情報主体との間で取り決めたサービスを提供することができないなど、契約の履行が困難な場合であって、情報主体がその契約の解約意思をはっきり明らかにしていない場合

③ 個人情報処理者は、第２項但書きによって処理停止の要求を拒絶したときは、情報主体に遅滞なくその事由を知らせなければならない。

④ 個人情報処理者は、情報主体の要求に応じて処理が停止された個人情報に対し、遅滞なく当該個人情報の破棄など必要な措置を講じなければならない。

⑤ 第１項から第３項までによる処理停止の要求、処理停止の拒絶、通知などの方法及び手続に必要な事項は、大統領令に定める。

次に、情報主体は個人情報処理者に対し、自己の個人情報処理を停止することを求めることができる。このときは、個人情報処理者は、法令上の規定などの制限的な事由に限らず、当該個人情報を処理しなければ契約履行が困難な場合であって情報主体がその契約の解約意思をはっきり明らかにしていない場合にも、個人情報処理の停止要求を拒絶することができる。かかる拒絶事由がなければ、個人情報処理者は処理停止を求められた日から１０日以内に当該個人情報の処理停止措置をとった事実（処理停止の要求に応じない法的根拠がある場合、その事実及び理由と異議申立方法）を情報主体に知らせなければならない。一方、情報主体は個人情報処理者が設けた方法や手続に従って処理停止を求めなければならない。

個人情報保護法第３９条の７（利用者の権利等に対する特例）

① 利用者は、情報通信サービスプロバイダーなどに対し、いつでも個人情報の収集・利用・提供などの同意を撤回することができる。

② 情報通信サービスプロバイダーなどは、第１項による同意の撤回、第３５条による個人情報の閲覧、第３６条による訂正を求める方法を個人情報の収集方法より容易にしなければならない。

③ 情報通信サービスプロバイダーなどは、第１項に基づき同意を撤回すれば、遅滞なく収集さ

れた個人情報を復旧・再生できないよう破棄するなど、必要な措置を講じなければならない。

なお、現行の個人情報保護法は、情報通信サービス（オンラインサービス）に関して利用者がいつでも個人情報の収集・利用・提供などの同意を撤回できるという規定を設けている（個人情報保護法第３９条の７）。かかる同意撤回権は、情報主体自らが同意したものに限って同意を撤回できるので、情報主体自らが処理に同意していなくても個人情報処理者が処理している情報主体に関するすべての個人情報の処理停止を求められる処理停止要求権とは相違する。しかしながら、２０２３年9月１５日施行される改正個人情報保護法のもとでは、情報通信サービスプロバイダーに対する特例規定である第３９条の７が削除され、当該内容は前述の従来の第３７条（個人情報の処理停止など）の規定でカバーされている[21]。

最後に、個人情報保護法は情報主体の破棄要求権に関する明示的な規定を設けていないが、情報主体は個人情報の漏洩などの被害を防止し、自分の個人情報が誤用・濫用にならないよう、個人情報の処理目的が達成されるなど個人情報を保管し続ける必要性がなくなったときは、個人情報処理者に自己の個人情報の破棄を求めることができる[22]。

ウ．最近の改正により一層能動的な自己情報統制権を実現

２０２３年3月１４日公布された改正個人情報保護法に基づき、情報主体の権利に関して次の規定が新設された。

1)　個人情報の転送要求

個人情報保護法第３５条の２（個人情報の転送要求）

① 情報主体は、個人情報処理能力などを考慮して大統領令の定める基準にあたる個人情報処理者に対し、次の各号の要件をいずれも満たすときは、個人情報処理者が処理する自己の個人情報を自己に転送することを求めることができる。

1. 情報主体が転送を求める個人情報が情報主体の本人に関する個人情報であって、次の各目の一にあたる情報であること
   ア．第１５条第１項第１号、第２３条第１項第１号又は第２４条第１項第１号による同意を得て処理される個人情報
   イ．第１５条第１項第４号に基づいて締結した契約を履行し、又は契約を締結する過程で情報主体の要請による措置を履行するために処理される個人情報

[21] 情報主体が同意を撤回した場合、前述の処理停止拒絶事由に該当しなければ、個人情報処理者は遅滞なく収集された個人情報を復旧・再生できないように破棄するなど必要な措置を講じなければならない（２０２３年9月１５日施行される改正個人情報保護法第３７条第3項）。

[22] 個人情報保護委員会、「個人情報保護法令及び指針・告示解説」、２０２０年１２月、３４頁。

ウ. 第１５条第１項第２号、同項第３号、第２３条第１項第２号又は第２４条第１項第２号に基づいて処理される個人情報のうち、情報主体の利益又は共益的目的のために関係中央行政機関の長からの要請に応じて保護委員会が審議・議決して転送要求の対象に指定した個人情報

2. 転送を求める個人情報が、個人情報処理者が収集した個人情報に基づいて分析・加工して別途生成した情報でないこと

3. 転送を求める個人情報がコンピューターなど情報処理装置で処理される個人情報であること

② 情報主体は、売上高、個人情報の規模、個人情報処理能力、産業別の特性などを考慮し、大統領令の定める基準にあたる個人情報処理者に対し、第１項による転送要求対象である個人情報を技術的に許容される合理的な範囲内で、次の各号の者に転送することを求めることができる。

1. 第３５条の３第１項による個人情報管理専門機関

2. 第２９条による安全措置義務を履行し、大統領令の定める施設及び技術基準を満たす者

③ 個人情報処理者は、第１項及び第２項による転送を求められた場合には、時間、費用、技術的に許容される合理的な範囲内で当該情報をコンピューターなど情報処理装置で処理可能な形態で転送しなければならない。

④ 第１項及び第２項による転送要求を受けた個人情報処理者は、次の各号の一にあたる法律の関連規定にも拘わらず、情報主体に関する個人情報を転送しなければならない。

1. 「国税基本法」第８１条の１３

2. 「地方税基本法」第８６条

3. その他第１号から第２号までの規定に類似する規定であって、大統領令に定める法律の規定

⑤ 個人情報処理者は、情報主体が本人であるかどうかが確認されない場合など大統領令に定める場合には、第１項及び第２項による転送要求を拒絶・中断することができる。

⑥ 情報主体は、第１項及び第２項による転送要求により、他人の権利又は正当な利益を侵害してはならない。

⑦ 第１項から第６項までの事項以外に、転送要求の対象になる情報の範囲、転送を求める方法、情報を転送・拒否する方法、転送要求の拒絶及び転送中断の方法など必要な事項は大統領令に定める。

従来の個人情報保護法は、ＧＤＰＲの個人情報移動権規定（第２０条 Right to data portability）に相応する権利に関する規定を導入していなかった。しかしながら、個人信用情報（個人情報の中でも個人の信用度や信用取引能力を把握するために必要な情報）に適用される特別法である「信用情報の利用及び保護に関する法律」は、個人信用情報に対する転送要求権の規定（第３３条の２）[23]を設けていた。この点、一般法である個人情報保護法にも一般的権利として個人情報の転送要求権規定を

[23] 「信用情報の利用及び保護に関する法律」上の転送要求権規定は２０２１年８月４日施行された。これは、信用情報主体である個人が、金融会社、公共機関などに提供した本人の個人信用情報を本人や本人の信用情報管理会社（マイデータ事業者）、個人信用格付け会社などに転送することを求める権利に関して規定している。

導入するために、２０２３年３月１４日公布された改正個人情報保護法のもとで個人情報の転送要求権規定が新設された[24]。

情報主体は、一定規模以上の個人情報処理者に対して自己の個人情報を本人、その他の個人情報処理者又は個人情報管理専門機関に転送することを求めることができ、個人情報処理者は時間、費用、技術的に許容される合理的な範囲内で当該情報を情報処理装置（コンピューターなど）で処理可能な形態で転送しなければならない。

この新設規定の詳細は、今後立法される個人情報保護法の施行令に盛り込まれるが、公布された法律規定の内容は概ねＧＤＰＲの転送要求権規定の内容に類似するものと思われる。しかしながら、情報主体が自己ではない第三者に個人情報の転送を求めるにおいて、技術的に可能な場合（where technically feasible）、他の個人情報処理者に個人情報を直接移転する権利がある旨が示されたＧＤＰＲ第２０条とは異なり、改正個人情報保護法第３５条の２によれば、情報主体は一定の基準（売上高、個人情報の規模、個人情報の処理能力、産業別特性など）にあたる個人情報処理者のみに対して転送を求めることができ、個人情報の転送を受ける者も個人情報管理専門機関又は一定の基準（法律による安全措置義務を履行し、一定の施設及び技術基準を満たさなければならない）にあたる者に限られる。これらの点で、改正個人情報保護法の転送要求権の規定は、ＧＤＰＲの転送要求権に比べて一部限られた範囲の権利を規定するものとみられる。

2)　自動化した決定に対する情報主体の権利

個人情報保護法第３７条の２（自動化した決定に対する情報主体の権利など）

① 情報主体は、完全に自動化したシステム（人工知能技術を適用したシステムを含む）で個人情報を処理して行われる決定が、自己の権利又は義務に重大な影響を及ぼすときは、その個人情報処理者に対して当該決定を拒否し、又はその決定に対する説明などを求めることができる。ただし、自動化した決定に対する拒否は、個人情報が第１５条第１項第３号又は第５号から第７号までの規定によって処理される場合に限って行うことができる。

② 個人情報処理者は、第１項に基づいて情報主体が自動化した決定を拒否し、又はこれに対する説明などを求めたときは、正当な事由がない限り、自動化した決定の適用を排除し、又は人的介入による再処理・説明など必要な措置を講じなければならない。

③ 個人情報処理者は、自動化した決定の基準と手続を情報主体が容易に確認できるよう開示するなど必要な措置を講じなければならない。

④ 第１項から第３項までの事項以外に自動化した決定の基準・手続の開示などに必要な事項は大統領令に定める。

[24] ただし、本規定の施行日は、公布（２０２３年３月１４日）から１年が経過した日から公布後２年が過ぎない範囲で大統領令に定める日とし｛個人情報保護法付則第１条第２号（２０２３年３月１４日法律第１９２３４号に改正されたもの）｝、２０２３年７月11日を基準に未だ指定されていない（２０２３年５月１８日付けで立法予告された個人情報保護法施行令改正案には当該内容なし）。

２０２４年3月１５日施行される改正個人情報保護法のもとでは、ＧＤＰＲの自動化した意思決定規定（第２２条 Automated individual decision-making, including profiling）に相応する権利として、自動化した決定に対する情報主体の権利規定が新設された。

情報主体は、完全に自動化したたシステム（人工知能技術を適用したシステムを含む）で個人情報を処理して行われる決定に対し、これを拒否したり当該決定に対する説明などを求めることができる。個人情報処理者は、かかる情報主体の要求に対し、正当な事由がない限り、自動化した決定の適用を排除したり、人的介入による再処理・説明など必要な措置を講じなければならない。さらに、個人情報処理者は、自動化した決定の基準や手続を情報主体にわかりやすく開示するなど、必要な措置を講じなければならない。

この新設規定の詳細も今後立法が行われる個人情報保護法施行令に盛り込まれることが見込まれ、公布された法律規定の内容は概ねＧＤＰＲの自動化した意思決定の規定に類似すると思われる。

2. 司法的救済システムによる情報主体の被害救済

個人情報保護法は、前述の第４条第５号における情報主体の権利、すなわち個人情報の処理による被害を迅速且つ公正な手続によって救済を受ける権利を保障するために、民法や民事訴訟法などの一般法の法理とは別に損害賠償を請求したり権利侵害の禁止・中止を請求できる権利に関する規定を整備している。

ア．個人情報保護法による損害賠償請求

1) 立証責任が転換された損害賠償請求

個人情報保護法第３９条（損害賠償責任）

① 情報主体は、個人情報処理者が同法に違反した行為によって損害を被った場合、個人情報処理者に損害賠償を請求することができる。この場合、その個人情報処理者は故意又は過失がないことを立証しなければ、責任を免れることができない。

個人情報処理者の責に帰すべき事由による個人情報の漏洩などの事故が発生し、それによって情報主体が損害を被った場合、情報主体は個人情報処理者に民法上の不法行為（民法第７５０条）に基づく損害賠償を請求することができる[25]。ただし、このとき、情報主体（原告）は個人情報処理者（被

[25] 情報主体は個人情報処理者に対して債務不履行（契約不履行）に基づく損害賠償を請求することも可能であり（不法行為とは請求権競合関係にあり、債務者である情報主体は2つの損害賠償請求権のいずれでも選択して行使することができる）、この場合には債務者（個人情報処理者）が自己の故意又は過失がないことを立証しなければならない（民法第３９０条）。しかし、この場合にも、債権者（情報主体）は、債務者（個人情報処理者）に個人情報の漏洩などの事故において責に帰すべき事由があるという事実及び債務者が債務の内容による履

告）の故意又は過失があったことを立証する責任があるが、その立証に必要な情報の所在の不均衡などにより、個人である情報主体が、主に企業や団体又は公共機関であることが多い個人情報処理者の故意又は過失を具体的に立証することは現実的に極めて難しい。よって、情報主体をして個人情報処理者の故意又は過失を証明させることは、事実上、情報主体の被害が救済されることを著しく困難にする結果を招く。

これらの点を踏まえ、個人情報保護法第３９条は、同法の規定に違反した行為によって情報主体が損害を被った場合、個人情報処理者に自ら故意又は過失がないことを証明する責任を負わせることで、情報主体の権利の一つとされる迅速且つ公正な被害救済を受ける権利を実質的に保障するとともに、個人情報処理者の遵法率を高めることを目指している[26]。

すなわち、個人情報保護法第３９条による損害賠償請求権は、（ⅰ）個人情報処理者の個人情報保護法の違反行為に（ⅱ）よって（違法行為と損害との因果関係）（ⅲ）損害を被ったという3つの要件を立証すれば行使することができる。このとき、損害は、財産的損害（例えば、クレジットカード番号、住民登録番号などの漏洩によるクレジットカードの不正使用、不法ローンなどにより財産的損失）と、精神的損害（例えば、メールアドレス、電話番号などの漏洩により情報主体の意思に反して迷惑メール、マーケティング広告などが受信されることによる非財産的被害）をいずれもいう[27]。

情報主体は、上記の損害賠償請求権の行使要件のうち、（ⅲ）損害が発生したこと並びにその損害額を立証しなければならないが、大法院はこれについて（特に精神的損害について）、諸事情を総合考慮してその裁量により損害額（慰謝料の額）を定めることができるという立場である。具体的に、「個人情報を処理する者が収集した個人情報が、情報主体の意思に反して漏洩された場合、それによって情報主体に慰謝料で賠償するに足りる精神的損害が発生したかどうかは、漏洩された個人情報の種類と性格は何か、個人情報の漏洩により情報主体を識別する可能性が発生したかどうか、第三者が漏洩された個人情報を閲覧したかどうか又は第三者の閲覧有無が明らかになっていなければ第三者による閲覧可能性があるかどうか、今後閲覧される可能性があるかどうか、漏洩された個人情報がどの範囲まで拡散したかどうか、個人情報の漏洩により更なる法益侵害の可能性が発生したかどうか、個人情報を処理する者が個人情報を管理してきた実態と個人情報が漏洩された具体的な経緯、個人情報の漏洩による被害の発生・拡散を防ぐために如何なる措置が講じられたのかなど、諸事情を総合考慮して具体的な事件に応じて個別に判断しなければならない」と判示し（大法院２０１２年１２月２６日宣告２０１１ダ５９８３４、５９８５８、５９８４１判決など参照）、不法行為による精神的苦痛

行をしないことによって債権者が損害を被ったという点を立証しなければならない。一方、個人情報保護法上、損害賠償請求権は個人情報処理者が「個人情報保護法に違反した行為」により情報主体が損害を被ったという点さえ立証すれば良いため、原告である情報主体にとっては民法上の債務不履行に基づく損害賠償請求権の行使に比べて個人情報保護法上の損害賠償請求権を行使したほうが有利であるといえる。

[26] 個人情報保護委員会、「個人情報保護法令及び指針・告示の解説」、２０２０年１２月、３９４～３９５頁。

[27] 個人情報保護委員会、「個人情報保護法令及び指針・告示の解説」、２０２０年１２月、３９２～３９３頁。

に対する慰謝料の額に関しては「事実審の法院が諸事情を斟酌してその職権に属する裁量によって定めることができる」と判断した（大法院２０１８年１０月２５日宣告、２０１８ダ２１９３５２、判決[28]）。

2) 懲罰的損害賠償

個人情報保護法第３９条（損害賠償責任）

③ 個人情報処理者の故意又は重大な過失により、個人情報が紛失・盗難・漏洩・偽造・変造又は毀損された場合であって、情報主体に損害が発生したときは、法院はその損害額の３倍[29]を超えない範囲内で損害賠償額を定めることができる。ただし、個人情報処理者が故意又は重大な過失がないことを証明したときは、その限りではない。

④ 法院は、第３項の賠償額を定めるときは、次の各号の事項を考慮しなければならない。

1. 故意又は損害発生の恐れを認識した程度
2. 違反行為によって被った被害の規模
3. 違反行為によって個人情報処理者が取得した経済的利益
4. 違反行為による罰金及び課徴金
5. 違反行為の期間・回数など
6. 個人情報処理者の財産状態
7. 個人情報処理者が情報主体の個人情報紛失・盗難・漏洩後、その個人情報を回収するために努力した程度
8. 個人情報処理者が情報主体の被害救済のために努力した程度

個人情報処理者が単に個人情報保護法に違反したことにとどまらず、個人情報処理者の故意又は重大な過失により個人情報が紛失・盗難・漏洩・偽造・変造又は毀損された場合のように、侵害行為の可罰性が高い場合、個人情報保護法は情報主体の被害救済強化のために法院をして実損害の３倍（２０２３年９月１５日施行される改正個人情報保護法においては５倍）を超えない範囲で懲罰的損害賠償を許容している。一方では、不合理に過度な賠償にならないよう、かかる懲罰的損害賠償額を算定するにあたり、法院は多様な要素を総合考慮して判断することを義務付けている。

---

[28] 当該ケースにおいて、被告（クレジットカード会社）は個人情報保護法など関連法令などに違反してセキュリティソフトのインストール及び管理・監督義務などセキュリティ措置を取る義務を果たしておらず、個人情報が漏洩された原告らに対して不法行為による損害賠償責任が認められた。法院は、そのクレジットカードの顧客情報漏洩事故によって漏洩された個人情報は原告ら個人を識別できるだけでなく、個人の私生活及び信用と密接な関わりのある情報であり、漏洩事故の全般的な経緯などを総合してみれば、その伝播及び拡散過程で既に第三者によって閲覧されたか、今後個人情報が閲覧される可能性が高いので、社会通念上、原告らに個人情報の漏洩による精神的損害が現実的に発生したとされるのが妥当であるとし、諸事情を考慮して被告が原告らに賠償すべき慰謝料をそれぞれ１０万ウォンとした。

[29] ２０２３年９月１５日施行される改正個人情報保護法によれば、この限度は５倍に引き上げられる。

3) 法定損害賠償

個人情報保護法第３９条の２（法定損害賠償の請求）

① 第３９条第１項にも拘わらず、情報主体は個人情報処理者の故意又は過失により、個人情報が紛失・盗難・漏洩・偽造・変造又は毀損された場合には、３００万ウォン以下の範囲で相当の金額を損害額にして賠償を請求することができる。この場合、当該個人情報処理者は故意又は過失がないことを立証しなければ、責任を免れることができない。

② 法院は、第１項による請求がある場合、弁論全体の趣旨と証拠調査の結果を考慮して第１項の範囲で相当の損害額を認めることができる。

③ 第３９条に基づき、損害賠償を請求した情報主体は、事実審の弁論が終結する前までその請求を第１項による請求に変えることができる。

情報主体は、前述の個人情報保護法第３９条に基づき、一般的な損害賠償の法理に比べてより容易に個人情報処理者に対して損害賠償を請求することができる。それにも拘らず、大量の個人情報の漏洩などの事故があった場合、被害者である情報主体としては自ら被った被害の規模さえも具体的に算定することが難しいことが多い。

すなわち、個人情報保護法第３９条の請求権の要件である「違反行為によって損害が発生したこと」に関し、損害が発生したという事実及びその損害額を立証することそのものが現実的に困難なことがある。例えば、財産的被害については、個人情報を違法に利用して不法ローンを受けたり不法な取引により情報主体の財産の損失が発生しない限り、個人情報の漏洩だけで財産上の損害を認めることは容易ではない。さらに、精神的損害についても、法院は、前述のとおり、漏洩された個人情報の種類と性格、個人情報の漏洩による情報主体の識別可能性の発生有無など諸事情を総合考慮して事件に応じて精神的損害の認定有無を個別に判断するため、被害者である情報主体が個人情報の漏洩などによって精神的損害が発生したという事実や具体的に被った損害規模を証明することは困難である[30]。

こうした背景のもと、大量の個人情報漏洩事故において個人に過ぎない被害者（情報主体）を損害から容易に救済されるようにする一方、個人情報処理者に個人情報保護責任を実質的に負わせるために、個人情報保護法は法定損害賠償制度を設けている。

これによれば、情報主体は、損害賠償請求権を行使するために具体的な損害額を証する必要がなく、個人情報処理者の故意又は過失により個人情報の紛失・盗難・漏洩・偽造・変造又は毀損によって損害が発生したことさえ主張すれば、法院が弁論全体の趣旨と証拠調査の結果を考慮して３００万ウォンの範囲で相当の損害額を認めることができる。

このときも、個人情報処理者の故意又は過失の不存在に対する立証責任は被告である個人情報処理者が負担することから、民法上の不法行為の法理による損害賠償請求（原告が被告の故意又は過失の

[30] 個人情報保護委員会、「個人情報保護法令及び指針・告示の解説」、２０２０年１２月、３９８頁。

存在を立証しなければならない）に比べて故意又は過失に対する証明責任が転換されている。

情報主体は、個人情報保護法第３９条による損害賠償を請求したにも拘らず、事実審の弁論が終結する前にはいつでもその請求を法定損害賠償請求に変えることができる（個人情報保護法第３９条の２第３項）[31]。従って、原告（情報主体）が第３９条による損害賠償請求訴訟で実損害の証明が困難になっても、事実審の弁論が終結する前であれば、第３９条の２による損害賠償請求に変えることにより最小限の権利救済が行われるようにすることができる。

イ．損害賠償の保障

個人情報保護法第３９条の９（損害賠償の保障）

① 情報通信サービスプロバイダーなどは、第３９条及び第３９条の２による損害賠償責任の履行のために保険又は共済に加入し、又は準備金を積み立てるなど必要な措置を講じなければならない。

② 第１項による加入対象になる個人情報処理者の範囲、基準などに必要な事項は大統領令に定める。

個人情報保護法は、情報通信サービスの利用者が個人情報保護法第３９条及び第３９条の２に基づいて個人情報処理者である情報通信サービスプロバイダーに損害賠償を請求する場合、その賠償責任の履行を保障するために、一定基準以上の売上高及び利用者数以上の情報通信サービスプロバイダーに保険や共済に加入するなど必要な措置を取らせている。

本規定は当初、情報通信技術の発達によって個人情報の漏洩による利用者の被害事例が増える中で、情報通信サービスプロバイダーに賠償能力がなく利用者に損害が賠償されない状況を防ぐために導入された特例規定である[32]。しかし、２０２３年３月１４日公布された改正個人情報保護法のもとで情報通信サービスプロバイダーに対する特例規定が一概に削除されたことにより、当該内容は２０２４年３月１５日施行される改正個人情報保護法の新設規定第３９条の７に移管され、その適用対象も情報通信サービスプロバイダーではない個人情報処理者一般に拡大した。

ウ．団体訴訟

個人情報保護法第５１条（団体訴訟の対象等）

[31] 明文の規定はないが、権利救済の実効性の強化を図る趣旨を踏まえ、法定損害賠償を請求した情報主体が事実審の弁論終結前までに実損害を証明することにより、個人情報保護法第３９条による損害賠償請求に変えることも可能とされる（個人情報保護委員会、「個人情報保護法令及び指針・告示の解説」、２０２０年１２月、４０１頁）。

[32] 個人情報保護委員会、「個人情報保護法令及び指針・告示の解説」、２０２０年１２月、４５６～４５７頁。

次の各号の一にあたる団体は、個人情報処理者が第４９条による集団紛争調停を拒否し、又は集団紛争調停の結果を受諾しないときは、法院に権利侵害行為の禁止・中止を求める訴訟（以下「団体訴訟」という）を申し立てることができる。

1. 「消費者基本法」第２９条に基づき、公正取引委員会に登録した消費者団体であって、次の各目の要件をいずれも備えた団体
   ア. 定款によって常時的に情報主体の権益増進を主な目的とする団体であること
   イ. 団体の正会員数が１千人以上であること
   ウ. 「消費者基本法」第２９条による登録から３年が経過していること
2. 「非営利民間団体支援法」第２条による非営利民間団体であって、次の各目の要件をいずれも備えた団体
   ア. 法律上又は事実上、同じ侵害を被った１００人以上の情報主体から団体訴訟の申立てを求められていること
   イ. 定款に個人情報の保護を団体の目的に掲げた後、直近３年以上、そのための活動実績があること
   ウ. 団体の常時構成員数が５千人以上であること
   エ. 中央行政機関に登録されていること

市場経済の持続的な発展、情報通信技術の急激な発達などにより、個人情報侵害被害の拡散速度は速くなっており、その被害規模もますます大型化している一方、個人情報侵害被害を被る不特定多数の個人は依然として非組織化・破片化の状況にとどまっている。このように、個人情報侵害誘発者と侵害被害者との非対称性により、個人情報の侵害に対する被害救済を情報主体である個人だけに任せる場合、実質的な被害救済が行われない問題が発生し得る[33]。

とりわけ、個人情報に係る侵害行為の中でも、個人情報の目的外利用・提供又は収集目的を達成した個人情報の未破棄など、情報主体の権利を侵害する行為については、個別の情報主体は被害事実がわかりにくく、かかる権利侵害行為が持続するだけでなく、今後情報主体が到底予期せぬ方向に２次、３次被害が起きる可能性が高い。例えば、個人情報の目的外利用・提供においては、情報主体が予期できないほどに当初の収集・利用目的を逸脱した目的で個人情報が利用されたり、情報主体に知られていない第三者に個人情報が提供される場合、情報主体は自己の個人情報の開示や利用に関して自ら決める権利、すなわち個人情報自己決定権が著しく侵害される。

さらに、このような権利侵害行為による被害は、個別の情報主体ではなく、当該侵害行為によって被害を被る全体被害者の利益のために一概に禁止・中止されることが求められ、これによってはじめて個人情報保護法第４条第５号における情報主体の権利、すなわち個人情報の処理によって発生した被害から迅速且つ公正な手続によって救済される権利が実質的に保障されることができる。

これらの点を総合考慮し、個人情報保護法は２０１１年制定当時、欧州型団体訴訟（Verbands-kla

[33] 個人情報保護委員会、「個人情報保護法令及び指針・告示の解説」、２０２０年１２月、５０９～５１０頁。

ge）[34]を導入した。これにより、一定の基準を備えた消費者団体や非営利民間団体は、個人情報の目的外利用・提供や個人情報の閲覧禁止など個人情報の処理に係る情報主体の権利侵害行為に対して禁止・中止を請求することができる。このとき、訴訟の対象は訴の申立て当時から続いている個人情報に係る権利侵害行為なので、訴の申立て当時、その行為が終了したり訴訟進行中に禁止・中止された場合、その訴訟は特段の事情がない限り、訴訟の利益を失って却下される。さらに、権利侵害行為の禁止・中止請求ではない金銭的被害救済請求は、団体訴訟によって申し立てることができないため、損害賠償などの請求は被害者である情報主体個人が前述の個人情報保護法第３９条などに基づいて行わなければならない。

個人情報保護法第５３条（訴訟代理人の選任）

団体訴訟の原告は、弁護士を訴訟代理人に選任しなければならない。

個人情報保護法第５４条（訴訟許可申請）

① 団体訴訟を申し立てる団体は、訴状とともに次の各号の事項を記載した訴訟許可申請書を法院に提出しなければならない。
   1. 原告及びその訴訟代理人
   2. 被告
   3. 情報主体の侵害された権利の内容

② 第１項による訴訟許可申請書には、次の各号の資料を添付しなければならない。
   1. 提訴団体が第５１条各号の一にあたる要件を備えていることを疎明する資料
   2. 個人情報処理者が調停を拒否し、又は調停結果を受諾しなかったことを証明する書類

個人情報保護法第５５条（訴訟許可要件など）

① 法院は、次の各号の要件をいずれも備えた場合に限って、決定により団体訴訟を許可する。
   1. 個人情報処理者が紛争調停委員会の調停を拒否し、又は調停結果を受諾しなかったこと
   2. 第５４条による訴訟許可申請書の記載事項に欠缺がないこと

② 団体訴訟を許可し、又は許可しない決定に対しては、即時抗告することができる。

個人情報保護法第５６条（確定判決の効力）

原告の請求を棄却する判決が確定した場合、これと同じ事案に関しては第５１条による他の団体は団体訴訟を申し立てることができない。ただし、次の各号の一にあたる場合には、その限りではない。

1. 判決が確定した後、その事案に関して国・地方自治体又は国・地方自治体が設立した機関によって新しい証拠が現われた場合

[34] 一定の資格を備えた団体が多数の被害者らの利益のための訴訟を申し立てる権限が与えられる制度であり、ドイツ式団体訴訟制度を受け入れたものと理解されている（チョ・マンヒョン、「個人情報保護法上の団体訴訟に関する小考」、土地工法研究第６０巻、２０１３、３７３頁）。これは、多数の被害者のうち個人（代表当事者）が被害者集団全体のために訴訟を申し立てる集団訴訟（Class Action）と相違する。

2. 棄却判決が原告の故意によるものであることが判明した場合

一方、不必要な訴訟の濫用を防ぐために、個人情報団体訴訟は必ず個人情報集団紛争調停手続を経る必要があり、管轄法院に訴訟許可申請書を提出して訴訟許可決定を得て申し立てることができる。

団体訴訟の確定判決の効力は他の団体へ及び、当該事案と同じ事案に関しては他の団体が改めて団体訴訟を申し立てることができない。しかしながら、当該効力は個別の情報主体へ及ぶものではないので、情報主体の個人は団体訴訟の結果に関係なく、自ら権利侵害行為の禁止・中止を請求する訴訟（例えば、民法上の不法行為の中止又は差止請求訴訟など）を申し立てることができる。

3. 制裁システムによる個人情報処理者の義務履行の強制

前述の１.と２.での内容は、情報主体が自ら行使することができる個人情報自己決定権の内容と範囲を定めることで、情報主体の個人情報自己決定権が実現されるようにするものだった。本項目では、個人情報保護に係る政府の主務機関である個人情報保護委員会[35]が行政的・刑事的な制裁手段を通じて個人情報処理者の義務履行を強制し、情報主体の個人情報自己決定権の行使が実際に個人情報自己決定権の実現につながるよう担保する内容について取り上げる。

ア. 行政制裁手段

1) 資料提出の要求及び検査

個人情報保護法第６３条（資料提出の要求及び検査）

① 保護委員会は、次の各号の一にあたる場合には、個人情報処理者に関係物品・書類など資料を提出させることができる。
   1. この法に違反する事項を見つけ、又は嫌疑があることを知った場合
   2. この法の違反に対する通報を受け、又は苦情が受理された場合
   3. その他情報主体の個人情報保護のために必要な場合であって大統領令に定める場合

② 保護委員会は、個人情報処理者が第１項による資料を提出せず、又はこの法に違反した事実があると認められれば、所属の公務員をして個人情報処理者及び当該法の違反事実に係る関係人の事務所又は事業場に出入りして業務状況、帳簿又は書類などを検査させることができる。この場合、検査を行う公務員は、その権限を表す証票を持参し、それを関係人に提示しなければならない。

[35] 個人情報保護に関する事務を独立して行うための国務総理所属の中央行政機関（個人情報保護法第７条第１項及び第２項）。

③　関係中央行政機関の長は、所管の法律に基づいて個人情報処理者に第１項による資料の提出を要求し、又は個人情報処理者及び当該法の違反事実に係る関係人に対して第２項による検査を行うことができる。

個人情報保護委員会は、個人情報保護法の違反行為などを調べて確認するために、個人情報処理者に資料の提出を求めたり、個人情報処理者の事務所や事業場に出入りして関連資料の検査を行うことができる。対象になる個人情報処理者には、公共機関に限らず民間企業や団体も含まれ、法執行の統一性や一貫性を維持するために、金融機関、医療機関、教育機関、通信キャリアなど他の部処所管の民間企業や団体に対しても、資料提出の要求や事務所などへの出入り・検査が可能とされる。

ただし、個人情報の保護に係る所管の法律である個別法（例えば「信用情報の利用及び保護に関する法律」など）において、関係中央行政機関の長に資料提出の要求又は事務所などの出入り・検査権限を与えている場合には、その分野ならではの特殊性や自律性を尊重するために、関係中央行政機関の長にも当該所管法律による資料提出の要求又は事務所などへの出入り・検査が可能であるという規定も併せて設けている（個人情報保護法第６３条第３項）[36]。

2)　是正措置、過料又は課徴金

個人情報保護法第６４条（是正措置など）

①　保護委員会は、個人情報が侵害されたと判断するに足りる相当の根拠があり、それを放置した場合には回復し難い被害を被る恐れがあると認められれば、この法に違反した者（中央行政機関、地方自治体、国会、法院、憲法裁判所、中央選挙管理委員会は除く）に対して次の各号にあたる措置を命ずることができる。

1.　個人情報侵害行為の中止
2.　個人情報処理の一時的な停止
3.　その他個人情報の保護及び侵害防止に必要な措置[37]

②　関係中央行政機関の長は、個人情報が侵害されたと判断する相当の根拠があり、これを放置する場合、回復し難い被害を被る恐れがあると認められれば、所管の法律に基づいて個人情報処理者に対して第１項各号にあたる措置を命ずることができる。

③　地方自治体、国会、法院、憲法裁判所、中央選挙管理委員会は、その所属機関及び所管の公共機関が同法に違反したときは、第１項各号にあたる措置を命ずることができる。

---

[36] ２０２３年９月１５日施行される改正個人情報保護法のもとでは、関係中央行政機関の長の権限に関する内容が削除され、個人情報保護に係る法規の違反行為によって重大な個人情報侵害事故が発生した場合、関係機関の長に協力を求めることができるという旨が新設される。一方、新設規定である第６３条の２を通じ、法違反の疑いや通報がなくても、個人情報の侵害事故が発生する危険性が高く、個人情報保護の脆弱点を事前に点検する必要性が認められる個人情報処理者に対する個人情報保護実態の事前点検に関する根拠規定を設ける。

[37] 個人情報漏洩サイトの遮断、技術的・管理的保護措置、個人情報処理方針又は約款の改正などが盛り込まれることができる（個人情報保護委員会、「個人情報保護法令及び指針・告示の解説」、２０２０年１２月、５５４頁）。

④　保護委員会は、中央行政機関、地方自治体、国会、法院、憲法裁判所、中央選挙管理委員会がこの法に違反したときは、当該機関の長に第１項各号にあたる措置を取るよう勧告することができる。この場合、勧告を受けた機関は、特段の事由がない限り、これを尊重しなければならない。

個人情報保護委員会又は関係中央行政機関の長は、通報、調査などによって個人情報処理者の法違反事実を確認し、その法の違反によって個人情報が侵害されたと判断するに足りる相当の根拠があり、これを放置すれば回復し難い被害を被る恐れがあると認める場合、個人情報侵害行為の中止など個人情報の保護及び侵害防止のために必要な是正措置を命ずることができる[38]。

さらに、個人情報保護委員会又は関係中央行政機関の長は、個人情報保護法第７５条に定める事由にあたる個人情報処理者に（事由に応じて）５千万ウォン以下、３千万ウォン以下、２千万ウォン以下又は１千万ウォン以下の過料を賦課することができる。行政秩序罰である過料は、概ね個人情報保護責任者の未指定、個人情報処理方針の未公開など、個人情報保護法における手続や基準に違反した場合に賦課される。

一方、個人情報保護委員会は、情報通信サービスプロバイダーが個人情報保護法に違反した一定の場合、その違反行為に係る売上高の１００分の３以下にあたる金額（売上高がないか売上高の算定が困難な場合は、４億ウォン以下の金額）を課徴金[39]として賦課することができる（個人情報保護法第３９条の１５）。本規定は、情報通信サービスプロバイダーに限って適用される特例規定であるが、２０２３年９月１５日施行される改正個人情報保護法のもとでは、情報通信サービスプロバイダーに対する特例規定が一括削除されることによって第３９条の１５が削除され、新設規定である第６４条の２に関連内容が移される。

さらに、改正法のもとでは、情報通信サービスプロバイダーに適用される課徴金は個人情報処理者全体に拡大し、３％課徴金の上限額の基準は「違反行為に係る売上高」から「全体売上高」に変わったが[40]、課徴金を算定するときは違反行為と関わりのない売上高は除外される。

---

[38] ２０２３年９月１５日施行される改正個人情報保護法のもとでは、「個人情報が侵害されたと判断する相当の根拠があり、それを放置すれば回復し難い被害が生じる恐れがあると認められれば」という要件を削除し、是正措置要件を緩和する。

[39] 課徴金は、行政法上の義務に違反した者に経済的利益が発生した場合、その利益を奪って間接的に義務の履行を確保するために賦課する制裁的金銭負担の性格を有する。これは、売上高などを考慮して算定され、課徴金の賦課は行政審判や行政訴訟により取消しを請求しなければならない。一方、過料は、過去の義務違反に対して一定の制裁を加えることにより、行政法規の違反に対する処罰を目的とする行政秩序罰の一種であり、可罰性の程度によって過料の限度額が決まり、不服の際に「非訟事件手続法」に基づいて異議申立をしなければならない。

ちなみに、課徴金を賦課した行為に対しては、過料を賦課することができない（個人情報保護法第７６条）。

[40] グローバル立法傾向（ＥＵ及びイギリスは全世界売上高の４％、中国は前年度売上高の５％、シンガポールは前年度売上高の１０％、米国は違反個別件当たり最大１万ドル）に合わせて課徴金の実効性を確保するためである（個人情報保護委員会２０２３年３月７日付けプレスリリース１５頁）。

3) 是正措置命令などの内容及び結果の公表

個人情報保護法第６６条（結果の公表）

① 保護委員会は、第６１条による改善勧告、第６４条による是正措置命令、第６５条による告発又は懲戒勧告及び第７５条による過料賦課の内容及び結果に対して公表することができる。

② 関係中央行政機関の長は、所管法律に基づいて第１項による公表を行うことができる。

③ 第１項及び第２項による公表の方法、基準及び手続などは、大統領令に定める。

個人情報保護委員会又は関係中央行政機関の長は、前述の行政処分及び後述する告発などの内容と結果をインターネットのホームページや一般の日刊新聞などに公表することができる[41]。この制度は、個人情報保護法の違反に対する行政処分結果を公開することにより、個人情報処理者の警戒心を高めるために施行されている。

イ．刑事告発権

個人情報保護法第６５条（告発及び懲戒勧告）

① 保護委員会は、個人情報処理者に同法など個人情報保護に係る法規の違反による犯罪の疑いがあると認められるに足りる相当の理由があるときは、管轄の捜査機関にその内容を告発することができる。

② 保護委員会は、同法など個人情報保護に係る法規の違反行為があると認められるに足りる相当の理由があるときは、責任がある者（代表者及び責任のある役員を含む）を懲戒することを当該個人情報処理者に勧告することができる。この場合、勧告を受けた者は、これを尊重しなければならず、その結果を保護委員会に知らせなければならない。

③ 関係中央行政機関の長は、所管法律に基づいて個人情報処理者に対して第１項による告発をし、又は所属機関・団体などの長に第２項による懲戒勧告を行うことができる。この場合、第２項による勧告を受けた者は、これを尊重しなければならず、その結果を関係中央行政機関の長に知らせなければならない。

個人情報保護委員会又は関係中央行政機関の長は、個人情報の保護に係る法規違反による犯罪の疑いがあると認められるに足りる相当の理由があれば、管轄の捜査機関にその内容を告発することができる。個人情報保護法は、第７０条ないし第７３条において保護法益の重要性、予想される被害の規模及び社会的費用などに応じて４段階（１０年以下の懲役又は１億ウォン以下の罰金、５年以下の懲役又は５千万ウォン以下の罰金、３年以下の懲役又は３千万ウォン以下の罰金、２年以下の懲役又は

[41] ２０２３年９月１５日施行される改正個人情報保護法のもとでは、関係中央行政機関の長の公表権限に関する内容が削除され、個人情報保護委員会が関連処分を受けた者に当該処分を受けたという事実を公表することを命ずることができるという旨が新設される。

２千万ウォン以下の罰金）に分けて刑事罰の規定を置いている。

ただし、経済制裁中心の国際基準[42]とは異なり、個人情報保護責任を企業よりは担当者個人への刑罰中心に規律している問題を改善するために、改正個人情報保護法（２０２３年９月１５日施行）のもとでは、前述のとおり、課徴金の実効性を確保する一方、過度な刑罰規定が一部削除された。

個人情報保護法第７４条（両罰規定）

① 法人の代表者や法人又は個人の代理人、使用人その他の従業員がその法人又は個人の業務に関して第７０条にあたる違反行為をすれば、その行為者を罰する以外にその法人又は個人を７千万ウォン以下の罰金に処する。ただし、法人又は個人がその違反行為を防止するために当該業務に関して相当の注意と監督を怠らなかった場合には、その限りではない。

② 法人の代表者や法人又は個人の代理人、使用人その他の従業員がその法人又は個人の業務に関して第７１条から第７３条までの一にあたる違反行為をすれば、その行為者を罰する以外にその法人又は個人にも当該条文の罰金刑を科する。ただし、法人又は個人がその違反行為を防止するために当該業務に関して相当の注意と監督を怠らなかった場合には、その限りではない。

一方、個人情報処理者の役職員、代理人などの業務処理に対する個人情報処理者の警戒心を高め、管理及び監督を強化するために、個人情報保護法は役職員、代理人などの法違反行為に対して当該行為者だけではなく、個人情報処理者も処罰する両罰規定を設けている。

診療データの二次利用に対する回答

④ 適用法令及び「患者に関する記録」の範囲

患者の健康に関する情報は、一次的に「個人情報保護法」上の敏感情報(個人情報保護法第23条第1項)に該当する。 ただし、個人情報保護法は、個人情報保護に関しては他の法律に特別な規定がある場合を除き、この法律で定めるところに従うと規定し(個人情報保護法第6条)、「**医療法**」は「**患者に関する記録**」に関する規定を設けている。 これと関連して、韓国政府の関連部署である保健福祉部は、医療機関が保有している患者に関する記録を第三者(外部者)に閲覧またはコピー発給などその内容の確認を提供する場合には医療法が優先的に適用されると解釈している(保健福祉部、2022年医療機関開設および医療法人設立運営便覧、217面)。

医療法が適用される患者に関する記録と関連して、医療法は第21条第1項で「(患者)本人に関する記録」の他に具体的な定義規定を設けてないが、保健福祉部は「患者に関する記録」には医療機関が患者の治療·診断過程で保有することとなったすべての記録が含まれ、診断書写本、処方箋写本、診

[42] 注４０を参照。

療確認書、入退院確認書などの諸証明書も含まれると解釈している(保健福祉部、2022年医療機関開設及び医療法人設立運営便覧、237面)。

医療法　第21条（記録閲覧等）

⑤　患者は医療人、医療機関の長及び医療機関従事者に本人に関する記録(追加記載·修正された場合、追加記載·修正された記録及び追加記載·修正前の原本をすべて含む。 以下同じ。）の全部又は一部について閲覧又はその写しの発給等内容の確認を要請することができる。 この場合において、医療関係者、医療機関の長及び医療機関従事者は、正当な理由がなければ、これを拒んではならない。

⑥ 患者に関する記録を二次利用するための要件

i.　医療法上、患者の同意が必要なのか、その他の義務が課せられているのか等

前述したように、医療法が適用される「患者に関する記録」は医療機関が保有する情報に限る。そこで本項目では、研究や医薬品開発などを目的とする第三者に患者に関する記録を医療機関が提供する場合、どのような要件を満たすべきかについて調べる。

まず医療機関は、患者本人でない他の者に患者に関する記録を閲覧させ、又はその写しを出すなど内容を確認できるようにしてはならないことが原則である（医療法第21条第2項）。 ただし、（i）**患者本人が同意した場合**であって、患者の親族又は**患者が指定する代理人が要請する場合**、（ii）患者が死亡し、又は意識がないなど患者の同意を得られないであって、患者の親族が要請する場合、又は（iii）関連法令で特別に定める場合には、例外的に患者に関する記録の内容を患者本人ではなく第三者に提供することができる(医療法第21条第3項)。

医療法　第21条（記録閲覧等）

②　医療人、医療機関の長及び医療機関従事者は、患者でない他の者に患者に関する記録を閲覧させ、又はその写しを出す等の内容を確認することができるようにしてはならない。

③　第二項の規定にかかわらず、医療人、医療機関の長及び医療機関従事者は、次の各号のいずれかに該当する場合には、その記録を閲覧させ、又はその写しを交付する等その内容を確認することができるようにしなければならない。 ただし、医師·歯科医師又は漢方医が患者の診療のためにやむを得ないと認めた場合は、この限りでない。

4. 患者の配偶者、直系尊属·卑属、兄弟姉妹（患者の配偶者及び直系尊属·卑属、配偶者の直系尊属がすべてない場合に限る。）又は配偶者の直系尊属が患者本人の同意書と親族関係であることを示す証明書等を添付するなど保健福祉部令で定める要件を備えて要請した場合
5. 患者が指定する代理人が患者本人の同意書と代理権を有することを証明する書類を添付するなど保健福祉部令で定める要件を満たして要請した場合
6. 患者が死亡したり意識がないなど患者の同意を得ることができず、患者の配偶者、直系

尊属·卑属、兄弟姉妹(患者の配偶者及び直系尊属·卑属、配偶者の直系尊属がすべてない場合に限る。）又は配偶者の直系尊属が親族関係であることを示す証明書等を添付するなど保健福祉部令で定める要件を備えて要請した場合

7. 「国民健康保険法」第14条、第47条、第48条及び第63条により給与費用審査·支給·対象有無確認·事後管理及び療養給付の適正性評価·加減支給等のために国民健康保険公団又は健康保険審査評価院に提供する場合

（以下第5号から第18号までは、第4号と類似して他の法令において特別の規定を設けている場合であって、省略する。）

ただし、このように患者が指定した代理人が患者に関する記録提供を要請するためには、代理人の身分証明書のコピー（すなわち、この時の代理人は自然人を意味するものと解釈される）、患者が自筆署名した同意書及び委任状（施行規則上各書式あり）及び患者の身分証明書のコピーを医療機関に提出しなければならないため（医療法施行規則第13条の3第2項）、患者の同意手続きが個人情報保護法に比べて非常に難しい。 また保健福祉部は、指定代理人は原則として医療機関に直接訪問し、身分証明書の写しの提出及び委任関係を証明しなければならないとみている（保健福祉部、2022年医療機関開設及び医療法人設立運営便覧、227面及び234面）。したがって、通常、研究や医薬品開発等を目的とする第三者が上記の規定により患者に関する記録を提供されることは事実上困難であると考えられる。

ii. 参考: 個人情報保護法の適用による「患者に関する記録」の利用

上記II.A.項で述べたように、患者ではない第三者が医療法上「患者に関する記録」を提供されることは容易ではない。 ただし、医療法ではなく個人情報保護法が適用される領域で患者に関する記録を第三者に提供することも可能であり、以下で項目を分けて調べる。

1. 医療機関 → 患者 → 第三者

医療機関が患者でない第三者に患者に関する記録を提供する上では厳格な要件が適用されるが、上記I.項で見た医療法第21条第1項のように、患者本人は医療機関にいつでも自分の記録閲覧またはコピー発給などその内容の確認を要請することができ、医療機関は正当な理由がない限りこれを拒否できない。 このように患者が提供された本人の記録は、もはや医療法が適用される「医療機関が保有する患者に関する記録」ではないので、患者が当該記録を第三者に提供する場合、これに対しては医療法ではなく個人情報保護法が適用される。

患者が保有する患者に関する記録は、個人情報保護法上の敏感情報(個人情報保護法第23条第1項)に該当し、研究などの目的で患者情報を利用しようとする第3者(個人情報処理者)が患者から敏感情報を収集して利用するためには、患者から他の個人情報の処理に対する同意と**別途の同意**[43]を得なけ

[43] 個人情報処理者は患者に敏感情報の収集·利用目的、収集しようとする敏感情報項目、敏感情報の

ればならない(個人情報保護法第23条第1項第1号)。 この場合、個人情報処理者に対しては個人情報を処理するにあたって適用される諸般の義務(個人情報の目的外利用制限、個人情報処理方針掲示、安全措置義務[44]など)が課される。

2. 仮名処理された患者に関する記録提供（医療機関 → 第三者）

一方、保健福祉部は個人情報保護法第2条第1号の2により仮名処理した患者に関する記録に対しては医療法第21条が適用されず、個人情報保護法上仮名情報の処理に関する特例関連規定により該当情報を利用及び提供が可能であると解釈している(保健福祉部、2022年医療機関開設及び医療法人設立運営便覧、238面)。 したがって、仮名処理された患者に関する記録については医療法ではなく個人情報保護法が適用され、研究などの目的で患者情報を利用しようとする第三者は個人情報保護法の定めるところにより医療機関から仮名処理された患者に関する記録の提供を受けることができる。

個人情報保護法上仮名処理とは、個人情報の一部を削除したり、一部または全部を代替するなどの方法で、追加情報がなければ特定個人を識別できないように処理することをいう(個人情報保護法第2条第1号の2)。 個人情報処理者は統計作成、科学的研究、公益的記録保存などのためには**情報主体の同意なしに**仮名情報を処理することができ(個人情報保護法第28条の2第1項)、これにより個人情報処理者(医療機関)は科学的研究などの目的で患者に関する記録を仮名処理した後、該当仮名情報を第3者(研究等目的で情報を利用する者)に提供することができる。 このように第三者に仮名情報を提供する場合、当該情報には特定の個人(患者)を調べるために使用できる情報(識別子)が含まれてはならない(個人情報保護法第28条の2第2項)。

さらに、仮名情報を処理する個人情報処理者(医療機関)は、元の状態に復元するための追加情報を別途分離して保管·管理するなど、該当情報が紛失·盗難·流出·偽造·変造または毀損されないよう安全性確保に必要な技術的·管理的および物理的措置をしなければならず(個人情報保護法第28条の4第1項)、仮名情報の処理目的、第3者提供時に提供される者など仮名情報の処理内容を管理するために必要な事項に関する関連記録を作成して保管しなければならない(個人情報保護法第2項)。[45]

また、仮名情報を処理する者は特定個人を調べるための目的で仮名情報を処理してはならず、もし仮名情報を処理する過程で特定個人を調べることができる情報が生成された場合、直ちに該当情報の処理を中止し、遅滞なくこれを回収および破棄しなければならない(個人情報保護法第28条の5)。

保有及び利用期間、同意を拒否する権利があるという事実及び同意拒否による不利益がある場合、その不利益の内容を事前に知らせ同意を得なければならない(個人情報保護法第15条第2項)

[44] 敏感情報を処理する個人情報処理システムの場合、個人情報取扱者が個人情報処理システムに接続した記録を2年以上(一般的な場合は1年以上)保管·管理しなければならない(個人情報の安全性確保措置基準第8条第1項)

[45] 2023年9月15日から施行される改正個人情報保護法では、仮名情報を破棄した場合、破棄した日から3年以上保管しなければならない義務も新設される(改正個人情報保護法第28条の4第3項)

※本研究は、JST【ムーンショット型研究開発事業】グラント番号【JPMJMS2293】の支援を受けたものです。

Ⅷ.中国

中国の個人情報保護法制に関する調査

松田侑奈

目次

1　エグゼクティブサマリー

第 4 次産業革命時代を迎え、ハイテク技術により人々の生産・生活方法には大きな変化が生じている。個人情報は、新しい時代の原動力であり、デジタル経済のインフラとして幅広く活用されている。商業活動にも利用され、莫大な経済利益や生活の利便性の向上にもつながっている。一方、情報技術を活用した個人情報の大規模の収集と利用は、個人のプライバシー侵害問題も同伴しており、個人情報保護における法制が重要視されている。個人情報の「保護」と「利用」の均衡は、中国を含む各国の課題でもある。

中国は、2003 年から個人情報保護のための立法を推進してきたが、中々制定までたどり着かずにいたところ、個人情報の漏洩やセキュリティの問題が急増し、大規模なデータ漏洩事件や個人情報の不正利用による社会的な問題が浮き彫りになり、2021 年にようやく「個人情報保護法」が公開された。

中国憲法は、情報自己決定権を明文化していない。また、憲法裁判所制度が存在しないため、憲法解釈を通じた保障もできない状況である。従って、個人情報保護法は、初めて個人情報保護について体系的な規定を設けた法律であるだけでなく、国家機関の個人情報処理を法的に制限した初の法律でもある。

個人情報保護法では、データ主体の権利について定めているが、知る権利と情報自己決定権、個人情報について閲覧・複製・移動を求める権利、不正確・不完全な個人情報に対し訂正や補完を求める権利、個人情報の削除を求める権利、個人情報処理ルールについて説明や解釈を求める権利、個人が死亡した場合近親者が相続できる権利、権利行使の請求が拒否された場合の提訴できる権利が含まれる。

告知・同意のプロセスにおいては、オプトイン方式を採用しており、法律や行政法規で定める特定の場合を除き、個人情報の処理には事前に本人の同意を取得することが必要である。

その他、自動化された意思決定やデータ・ポータビリティ権に関わる規定を設け、監督機関としては、国家インターネット情報弁公室を中心に、分散型モデルを採用している。

救済制度としては、個人や組織は、個人情報関連業務担当省庁に個人情報処理の違法行為をまずは通報でき、担当省庁が多くの人々の個人情報権益の侵害につながると判断した場合は、司法救済として、検察庁や国家インターネット情報弁公室等が指定した組織が公益訴訟を提起することができる。

個人情報保護の法制において、中国は法律の制定を通じ大きく一歩前に進んだが、データ主体の権利や事業者の義務についての規定は抽象的な部分が多く、独立した監督機関の不在や不十分な救済制度等、まだ改善を要する部分が多く残る。

2　個人情報に関わる憲法と法律上の規定

2.1　憲法における個人情報関連規定

憲法の個人情報に対する保護は、EU 基本権憲章のように、憲法の条文で明文化する場合があれば、ドイツやアメリカのように憲法解釈を通じ、個人情報保護を基本権として認める場合もある。

中国の憲法は、日本・ドイツ・アメリカと同様、個人情報の保護に対する明文化した規定を設けていない。また、中国には憲法裁判制度が存在しないため、裁判所が具体的な事件を審理する際に、憲法の条文を根拠として引用することはできない。従って、憲法条文の解釈を通じ、情報自己決定権を導出することも、アメリカのように、個人情報を基本権であるプライバシー権の範疇に入れて保護することもできない。中国で憲法に位置付けは、裁判の根拠ではなく、法律を制定する根拠であるため、憲法違反を根拠に提訴することはできない[1]。

ただ、憲法 33 条と 38 条を個人情報の保護の根拠だと主張している憲法学者は存在する。

中国憲法の基本権条文は、第 2 章の「国民の基本権と義務」に集中されているが、33 条は「国家は人権を尊重・保障する」と、38 条は「国民の人格尊厳は不可侵である」と定めている。33 条を個人情報保護の根拠だと主張する学者は、人権は抽象的な概念であるが、人間として享受すべき全ての権利を網羅しており、個人情報権もその一つだとしている。個人情報は情報漏洩のリスクが高く、個人が企業や国家からの不当な干渉を排除するのも現実的に難しいため、個人情報権への保護を人権保護に含ませるべきとの見解である[2]。また、38 条を根拠とすべきと主張する学者の見解は下記の通りである。人格尊厳は、尊厳と人格に分かれるが、尊厳は人間の尊厳、人格は人格権を意味する。38 条は個人情報保護に関する内容を明示していないが、個人情報権がもつ人格権的特性に鑑みれば、国民の人格尊厳性への保護を通じ、個人情報権も間接的に保護されているといえる[3]。憲法における個人情報保護関連条文は、その他、37 条の身体自由の不可侵、39 条の住居不可侵、40 条の通信の自由と秘密保護権等がある。

2.2　法律における個人情報保関連規定

憲法の条文及び憲法の有効解釈が、情報主体に権利を付与できておらず、国民は自身の権利で政府に対抗することができない。行政分野では、公共機関と個人の権利に不均衡が生じている。

---

[1] 2016 年 6 月 28 日に制定された最高裁判所（最高人民法院）「裁判所の民事裁判文書作成規範（人民法院民事裁判文书制作规范）」第 4 条は、「憲法を裁判の根拠として引用することはできない。」と定めている。

[2] 姚岳绒「情報決定権を基本権利とすることの関する論証（论信息自决权作为一项基本权利在我国的证成）」（政治学法律第 4 期、2012）77～78 頁。

[3] 孫平「政府巨大型データベース時代におけるプライバシー保護（政府巨型数据库时代的公民隐私权保护」（法学第 7 期、2007）24 頁。

中国における個人情報と関わる法律としては、本稿で紹介する民法典と個人情報保護法以外に、2012 年の「インターネット情報保護を強化することに関する決定」、2016 年の「ネットワーク安全法」、2021 年の「データ安全法」がある。ネットワーク安全法はサイバーセキュリティ全般、データ安全法はデータ処理活動のセキュリティ全般について定めている。これらの法律はデータ主体の権利よりは事業者の義務やデータ処理活動ルールに焦点を当てている。

① 民法典

中国の民法典は、2021 年 1 月 1 日より実施されたが、人格権制度を基盤に、情報自己決定権を保護しており、初めて法律の形で個人情報に関する権利を定めた。民法典は、総則編と人格権編で個人情報保護に関する規定を設けている。

総則編 111 条では、なぜ法律で個人情報を保護する必要があるかを論じ、人格権編では、1032～1039 条にかけ、個人情報に対し定めている。

中国民法典ではプライバシーと個人情報を下記の表の通り区分して保護している。

中国は、他国に比べ、個人情報という概念の普及が遅れているため、既存の法律では個人情報よりはプライバシーという表現を使用しており、両者の区別について特段の言及がなかったところ、民法典が初めて両者に区別について明文化した。民法典のプライバシー権は狭義的なプライバシー権であり、個人情報は識別可能性を基準に定義している。事業者の処理活動における指針を提供し、データ主体の閲覧権、複製権、削除権、異議や訂正の申し出ができる権利を含む各種権利についても定めている。

表　民法典における個人情報とプライバシーの区別

	内容	適用する条文
プライバシー（隠私）	私的秘密空間（プライベート空間）	プライバシーに関する規定
	私的秘密活動（プライベート活動）	
	私的秘密情報（プライベート情報）	
個人情報	一般個人情報	個人情報に関する規定
	私的秘密情報	プライバシーに関する規定

② 個人情報保護法

そして、2021 年 11 月 1 日より、個人情報について体系的に定める個人情報保護法が実施されるようになった。当該法律は、「EU 一般データ保護規則」（以下 GDPR：General Data Protection Regulation）をモデルに制定している[4]ため、類似している規定が非常に多い。また、GDPR で

[4] 対外経済政策研究院「中国の個人情報保護法の主要内容と展望」（世界経済フォーカス第 5 期、2022）2 頁。

は認められていない「死者の権利」についても保護規定を設けている。

個人情報保護法 1 条は、「個人情報の権益を保護し、個人情報処理活用を規範化し、個人情報の合理的利用を促すため、憲法に基づき当該法律を定める」としている。立法目的は、ビックデータ時代において、個人情報を保護しつつ十分に活用することである。個人情報保護法は、保護と利用という 2 つの価値を明確にし、両者が均衡を目指している。また、権益という表現を使用しており、データ主体の法的権利と利益の保護を強調している。

3 条は、適用範囲について定めているが、「中国境内の組織または個人が自然人の個人情報を処理する活動を行う際は当該法律を適用する。また、境外の組織または個人であるとしても、①中国境内の自然人に商品やサービスを提供する場合、②中国境内の自然人を分析、評価等をする際は、当該法律を適用する」とした。海外の組織や個人が中国国民の個人情報権益、公共利益や安全を侵害する場合は、国家情報関連省庁により、個人情報提供ブラックリストに登録され、氏名公開とともに、個人情報の提供が禁止または制限される（42 条）。

個人情報保護法は、民法典の個人情報の定義をより広げている。

4 条は、「個人情報とは、電子又はその他の方式によって記録された既に識別されたか或いは識別可能な、自然人と関連する各種情報を指す。匿名処理をした情報は個人情報に含まれない」と定めた。民法典は、識別可能性だけにフォーカスしている反面、個人情報保護法は、識別可能性と関連性両方を意識している。従って、個人情報に該当するか否かを判断する際には、まず、直接または間接的に特定個人を識別する可能性があるかどうか判断し、識別可能性があると判断した場合、当該情報が個人または識別された個人と関連性があるかどうかを再度判断する必要がある。個人情報に特定個人の識別性が求められるため、クッキー情報単体は、原則個人情報にあたらない。中国の個人情報の定義は、GDPR 4 条 1 号「個人データとは、識別された又は識別され得るデータ主体に関するあらゆる情報を意味する」との定義とほぼ同様である。

民法典では、個人に関わる情報を、プライバシーか個人情報に区分して定めたところ、個人情報保護法では、一般個人情報と敏感な個人情報に区分している。ここで言う敏感な個人情報（28 条）とは、「ひとたび漏洩し又は不法に使用されれば、自然人の人格の尊厳の侵害を引き起こしやすい、 又は人身、財産の安全が損なわれやすい個人情報をいい、生物識別、 宗教信仰、特定の身分、医療健康、金融口座、行動履歴等の情報及び 14 歳未満の未成年者の個人情報が含まれる。」 特定の目的と十分な必要性がある場合で、かつ厳格な保護措置を講じている場合に限り、事業者は、敏感な個人情報を処理することができる。

なお、個人情報の処理原則は、GDPR の原則と一致しているため、重複しない。

表　民法典と個人情報保護法における個人情報とプライバシーに関する規定

法律名	使われている用語	内容	適用する条文
个人信息权 民法典	プライバシー（隠私）	私的秘密空間（プライベート空間）	プライバシーに関する規定
		私的秘密活動（プライベート活動）	
		私的秘密情報（プライベート情報）	
	個人情報	一般個人情報	個人情報に関する規定
		私的秘密情報	プライバシーに関する規定
個人情報保護法	一般個人情報	匿名処理をした情報を除く	個人情報に関する規定
	敏感な個人情報	特別情報及び 14 歳未満の未成年者の個人情報	敏感な個人情報に関する規定

3　個人情報保護法制の現状と課題

3.1　データ主体の権利

個人情報保護法では、独立した第 4 章で、データ主体の権利について定めている。ここで、言及されている権利には、知る権利と情報自己決定権、個人情報について閲覧・複製・移動を求める権利、不正確・不完全な個人情報に対し訂正や補完を求める権利、個人情報の削除を求める権利、個人情報処理ルールについて説明や解釈を求める権利、個人が死亡した場合近親者が相続できる権利、権利行使の請求が拒否された場合の提訴できる権利が含まれる。

利用停止請求権として、まずデータ主体は、個人情報処理を拒否する権利を有する。また、データ主体本人が同意を撤回した場合や、目的のために取り扱う必要がなくなった場合等、違反がなくてもデータ主体は個人データの削除を請求できる。同意の撤回については、特段の規定をないため、いつでも撤回ができるようになっている。

言及すべき部分は、33 条は、国家機関が個人情報を処理する際も個人情報保護法を適用すべきと定めている。これは、中国の個人情報保護法制において、初めて国家機関の個人情報処理を法的に制限したこととなる。すなわち、データ主体は国家に相手に、個人の権利を主張できるようになったのである。

一方、中国にも情報銀行（信息银行）の仕組みが存在する。情報銀行とは、情報技術を利用し、パーソナルデータについて保存・管理・処理・分析・読取ができるサービスであり、銀行で現金を預けるように個人の情報を管理できるほか、ユーザーは情報価値がもたらす付加価値サービスも享受できる。中国でこのサービスを最も早く展開したのは、上海電信社であり、2009 年に E 雲というサービスを始めた。E 雲は、ユーザーの設定に従って、パソコンのエンプティタイムを利用し、パーソナルデータを上海電信の E 雲データセンターにバックアップするため、データを紛失した場合でも、本人がインターネットを通じて電信サーバーに接続すれば、いつでもデータの回復ができるようになっている。E 雲は情報銀行として、パーソナルデータに対する本人のコントローラビリティを保障し、本人以外はパーソナルデーにアクセスできないように保護している。

3.2　告知・同意に関する規定

①告知・同意のプロセス

日本において個人情報取扱事業者にあたる企業が個人情報を取得する場合、要配慮個人情報という一定の個人情報については予め本人の同意が必要ですが、通常の個人情報については、予めその利用目的を公表するか、又は個人情報の取得後速やかにその利用目的を本人に通知若しくは公表する必要があるものの、その個人情報の取得自体には本人の同意は必要としないが、中国の個人情報保護法では、法律や行政法規で定める特定の場合を除き、個人情報の処理には事前に本人の同意を取得することが必要とされている。すなわち、オプトイン方式を採用しているが、個人情報保護制度においての「告知・同意」のプロセスは、個人情報処理につい

て、データ主体に十分に告知をしてから同意を得ることが大前提であり、これは、個人情報におけるデータ主体の自己決定権を保障するためである。

データ主体の同意が不要な場合は、以下の 6 つの状況に限る（13 条）。

(一)データ主体を当事者の一方とする契約の締結、履行に必要である場合、或いは法により制定した労働規則制度や法により締結した集団契約に基づいて人的資源の管理を実施するために必要である場合。

(二)法定の職責又は法定の義務の履行に必要である場合

(三)突発的な公衆衛生上の事件に対応するため、又は緊急状況下において自然人の生命、健康及び財産の安全を保護するために必要な場合。

(四)公共の利益のためにメディア報道、世論監督等の行為を実施して、合理的な範囲内で個人情報を処理する場合。

（五）本法の規定に従って、合理的な範囲内で、データ主体が自ら公開した又はその他既に合法的に公開されている個人情報を処理する場合。

(六)法律、行政法規が規定するその他の事由。

また 14 条は、同意の有効条件について定めているが、「個人の同意に基づいて個人情報を処理するとき、当該同意は、データ主体が充分に事情を理解していることを前提に、自発的かつ明確に行わなければならない。法律、行政法規が、個人情報の処理にはデータ主体の個別の同意又は書面による同意を得なければならないと規定している場合は、当該規定に従わなければならない。個人情報の処理目的、処理方法及び処理する個人情報の種類に変更が生じた場合は、改めてデータ主体の同意を得なければならない」と定めている。

データ主体は、個人情報処理活動における同意を撤回でき（第 15 条）、個人情報の処理が商品又はサービスの提供のために必要である場合を除き、事業者は同意の撤回を理由に商品やサービスの提供を拒否してはならない（第 16 条）。

17 条では、事業者が告知すべき事項を定めているが、事業者は目立つ方法により、明瞭かつ理解しやすい表現を用いて、個人に対し、真実のとおり正確かつ完全に以下の事項を告知する必要がある。

（一）事業者の名称又は氏名及び連絡先。

（二）個人情報の処理目的、処理方法、処理する個人情報の種類、保存期限。

（三）データ主体が本法の規定する権利を行使する方法及び手続。

（四）法律、行政法規が告知すべきであると規定するその他の事項。

なお、14 歳未満の未成年者の個人情報を処理する際には、当該未成年者の両親又はその他監護者の同意を取得しなければならない（31 条）。

②プロファイリングの場面に特化したデータ保護の仕組み

告知・同意に関する具体的した規定を設けたには、中国での「ビックデータ殺熟」問題が深刻だったからでもある。「ビックデータ殺熟」とは[5]、ビッグデータをもとに購入履歴や消費傾向を分析し、ユーザーが知り得ないアルゴリズムによって商品やサービスの値段を変えてしまう行為を指すが、これは、サイトの会員やヘビーユーザーであるほど損をする場合が多いとされる。個人情報保護法では、この問題への対策として「自動化された意思決定」に関する規定を設けている。

73 条は、「自動化された意思決定とは、コンピュータプログラムを通じて個人の行動習慣、興味、嗜好又は経済、健康、信用状態等を自動的に分析、評価したうえで意思決定する活動をいう」と定めているが、「事業者が個人情報を利用して自動化された意思決定を行う場合には、意思決定の透明度及び結果の公平性・公正性を保証するものとし、取引価格等の取引条件において、データ主体に対して不合理な差別的待遇を行ってはならない」としている（24 条 1 項）。

また、「自動化された意思決定の方法によりデータ主体に対して情報のプッシュ通知、商業的なマーケティングを行う場合は、その個人的特徴に向けられたものではないオプション項目も同時に提供するか、データ主体に対して簡便な拒否方法を提供しなければならない。自動化された意思決定の方式により、データ主体の権益に対し重大な影響をもたらす決定を行う場合、データ主体は、事業者に対して説明を求める権利を有し、かつ事業者が自動化された意思決定の方式のみによって決定を行うことを拒否する権利を有する」（24 条 2 項）と定めている。当該規定は、データ主体に対し個人情報を処理するアルゴリズムを拒否できる権利やアルゴリズムに対し説明を求める権利を付与している。これは、GDPR22 条のプロファイリングを含む個人に対する自動化された意思決定規定と、13 条の自動化された意思決定の際のデータ主体の説明要求権と内容が一致している。

③データ・ポータビリティ権への保障

データ・ポータビリティ権については、45 条にて、「データ主体は、事業者からその個人情報を閲覧し、複製する権利を有する…データ主体がその個人情報の閲覧、複製を請求した場合、事業者は速やかに提供しなければならない。データ主体が個人情報をその指定する事業者に移転することを要求した場合で、国家インターネット情報弁公室が規定する条件に合致している場合、事業者は移転の手段を提供しなければならない。」と定めている。この規定により、データ主体は事業者に個人情報の副本や他者への転送を求められるようになった。個人情報保護法は、データ・ポータビリティ権について定めた初の法律である。ただし、データ・ポータビリティ権の範囲や転送方法等については定めておらず、まだ要補完の部分が多く残る。

この条文は、中国でこれからデータ・ポータビリティ権を保障するという宣言に該当し、具体的に保護措置は、実施細則や別途の法律で詳しく定める必要がある。

---

[5] CRI 日本語「ビックデータ殺熟」（2021 年 11 月、https://japanese.cri.cn/20211101/ea5ce9fb-92e1-cee5-6b6a-7c1491d4277e.html）を参照。

プラットフォーム経済の急速発展により、大手プラットフォーム事業者の独占問題や不正競争が蔓延している。典型的な例として、上述したプラットフォーム事業者による「ビックデータ殺熟」問題や「二者択一」独占行為（取引先に対して、競合他社とは取引しないよう迫る行為）が挙げられる。「二者択一」行為は、排他的な提携協議の締結、パケット制限等の方式で排他的提携協議が保障され実施されることが一般的である。データ・ポータビリティ権によって、ユーザーのデータにおける自主権が強化され、事業者の間でのデータ流動の自由が保障されるようになったので、公平競争の促進につながると思われる。公平競争の促進のため、個人情報保護法が制定された直後である 2021 年 2 月、国務院独占禁止委員会は「プラットフォーム経済における独占禁止に関する指針」も合わせて公開した。

④第 3 者への個人情報提供

21 条の規定によると、事業者が個人情報の処理を第 3 者に委託する場合、個人情報の処理方法、目的、期間、個人情報の種類、個人情報への保護措置を約定するとともに、受託者による個人情報処理活動に対して監督を行わなければならない。

また、第 3 者へ情報を提供する場合は、データ主体に、受領者の名称又は氏名、連絡先、処理目的、処理方法及び個人情報の種類を告知し、データ主体から個別同意をえる必要があり、受領者は、上記の処理目的、処理方法及び個人情報の種類等の範囲内において個人情報を処理すべく、もしも従来の処理目的、処理方法を変更する場合には、改めてデータ主体の同意を取得する必要がある（23 条）。

⑤敏感な個人情報の処理

2.2 で敏感な個人情報の定義について述べたが、事業者が、敏感な個人情報を処理する場合、データ主体の個別同意が必要であり、法律や法規で書面同意が必要であると定めている場合は、書面同意を得る必要がある（28 条）。

3.3　告知・同意プロセスの限界と対策

なお「告知―同意」にプロセスの限界は、中国でも指摘されている。

事業者は、契約締結において、個人情報の保護より法的責任を避けることにフォーカスを当てているため、免責条文を多く入れる可能性が高く、契約内容が冗長になる恐れがある。また、個々の年齢、専門知識、教育水準によって理解能力の差は大きいため、データ主体が告知・同意の内容を十分に理解したとは断言できない。告知・同意規則は、契約を締結する双方が合理的な能力を有することを前提にするが、全てのデータ主体が情報処理の危険性、例えば、告知の具体的な内容や同意した場合もたらす結果等について十分に認識しているとは言えない。同意に多くのコスト・時間がかかるため、データ主体は同意疲れを感じる場合も多く、プライバシーポリシーも流し読みが多いと思われる。従って、告知・同意の具体的な内容を把

握しているデータ主体は非常に少ない恐れがある。統計によると[6]、データ主体が告知・同意説明書を十分に読む場合年間平均 244 時間が所要され、丁寧に読まない場合も年間 154 時間が必要となる。データ主体は、告知・同意の内容を十分に把握できていないまま、時間の余裕がない等で同意するケースが多い。

その改善策として、既に一部の企業で導入しているが、告知・同意プロセスにプライバシー設計を追加する方法が挙げられている。この方法はより実効的な告知になるとの主張が存在する[7]。製品設計は個人情報保護の要求を満たす必要があるため、告知・同意のプロセスにプライバシー設計の要求を追加すると、告知内容の費用や難易度を下げることができ、データ主体の認識も高められるため、事業者とデータ主体の認識のすれ違いが最小化しつつ、データ主体の個人情報への自己決定権を高められとされる。例としは、中国の BiliBili アプリケーションは、ユーザーがテストに合格した場合のみ、アプリケーションの利用が可能になるよう設計されている。テストの内容には、個人情報の保護や製品の使用ルール等が含まれるため、効果的な告知となっている。類似している例で、電子製品を使用する場合、データ主体に動画で個人情報の収集・利用・結果を伝え、最後テストを行う方法がある。

もう一つの方法としては提言されているのは、GDPR が 2021 年標準契約の約款テンプレート[8]制定したように、中国政府が各種業界における標準計画書を予め設計し、事業者が統一した契約書を作る方法である。政府が契約書に対し解釈を行いつつ、宣伝活動に取り組める紛争が起きたとしても有効に解決できるという主張である[9]。中国政府の強みの一つは政策の柔軟性と普及の速さであり、中央の政策は短時間で地方まで伝わるため、実効性の高い方法になると思われる。

3.4　個人情報保護法を執行する監督機関の組織と権限

60 条 1 項の規定により、個人情報の保護法を執行する中央の監督機関は、国家インターネット情報弁公室(国家互**联**网信息**办**公室)となる。国家インターネット情報弁公室は、個人情報の保護に関わる管理監督業務全般を総括・調整する。

国家インターネット情報弁公室が行うべき業務には以下の事項が含まれる（62 条）

（一）個人情報保護の具体的なルール、基準を制定する。

---

[6] Omriben-Shahar & Carle.Schneider, *The failure of Mandated Disclosure*, 159 University of Pennsylvania Law Review, Vol. 52, 2011, pp.658-659.

7 張翱鵬「中国の個人情報保護制度に関する研究」（忠北大学博士論文、2022 年 2 月）218～219 頁。

[8] European Commission, Standard Contractual Clauses (SCC), https://ec.europa.eu/info/index_en

[9] 張翱鵬「中国の個人情報保護制度に関する研究」（忠北大学博士論文、2022 年 2 月）219～220 頁。

（二）小規模な事業者、敏感な個人情報の処理及び顔認識、人工知能等の新テクノロジー、新アプリケーションを対象に、専門の個人情報保護ルール・基準を制定する。
（三）安全で便利な電子身分認証技術の研究開発と応用の普及を支援し、オンライン身分認証のための公共サービスの構築を促進する。
（四）個人情報保護の社会的サービス体系の構築を推進し、関係機構による個人情報保護の評価、認証サービスの展開を支援する。
（五）個人情報保護に関する苦情申立て、通報業務のメカニズムを完備する。

また、国務院の関連部門は、各自の職責の範囲内において、個人情報保護及び監督管理業務の責任を負うように定められている（60 条 2 項）。従って、個人情報保護への監督業務は、非常に多くの省庁に分散されている。例えば、消費問題になると工商行政省庁が担当し（消費者権益保護法第 32 条）、信用情報や郵便関連問題は、中国銀行と国家郵便局が担当する（通信とネットユーザー個人情報保護規定 17 条、ネットワーク安全法 8 条）。なお、中国は、国家（中央）、省、市、県の 4 級行政体系を取っているため、各階級においても、これから監督機関が存在する（例：○○省インターネット情報弁公室、○○市工商行政局等）。そして、これらの個人情報保護監督業務に携わる省庁を全て「個人情報関連業務担当省庁」と称する。

個人情報関連業務担当省庁の職責は下記の通りである（61 条）。
(一)個人情報保護の宣伝教育を展開し、事業者による個人情報保護業務を指導、監督する。
(二)個人情報保護に関する苦情の申し立て、通報を受理し、処理する。
(三)アプリケーションプログラム等の個人情報保護情況について測定・評価を実施し、測定・評価の結果を公表する。
(四)違法な個人情報処理活動を調査し、処理する。
(五)法律、行政法規が規定するその他の職責。

また、個人情報関連業務担当省庁は、職責を履行するにあたり、以下の措置を取ることができる（63条）。
(一)関係当事者に対し質問し、個人情報処理活動に関する状況を調査する。
(二)個人情報処理活動と関係する当事者の契約、記録、帳簿及びその他の関係資料を閲覧、複製する。
(三)現場検査を実施し、違法が疑われる個人情報処理活動について調査を行う。
(四)個人情報処理活動と関係する設備、物品を調査する。違法な個人情報処理活動に用いられている設備、物品であることを証明する証拠があるものについては、当該部門の主要責任者に対して書面で報告したうえで許可を得て差押え又は押収することができる。

64条の規定により、個人情報関連業務担当省庁が職責を履行する中で、個人情報処理活動に比較的大きなリスクが存在すること、又は個人情報安全事件が発生したことを発見した場合は、当該事業者の法定代表者又は主要責任者に対して事情の聞き取りを行うか、或いは事業者に対して、専門機構に委託してその個人情報処理活動についてのコンプライアンス監査を依頼するよう要求することができる。事業者は、要求に基づき措置を講じ、改善を実施し、隠れた

危険を取り除かなければならない。個人情報関連業務担当省庁が職責を履行する中で、個人情報の違法な処理が犯罪を構成する疑いのあることを発見した場合は、速やかに公安機関に移送して、公安機関の法による処理に委ねる必要がある。

中国の場合、独立した個人情報保護機関を設置する代わりに、既存の国家インターネット情報弁公室を監督業務総括省庁と指定し、多くの省庁に業務を分担させる仕組みを選択した。このような分散モデルは、実際の運用において難点が多く、各監督機関の業務の重複、責任の回避、行政資源の浪費等がおきうる。場合によっては、監督機関をどこにすべきか指定することも難しいかもしれない。また、4つの階級に監督機関が分かれているが、県級は規模が小さく業務遂行能力に有していない場合もある。個人情報保護法は、地方の個人情報関連業務担当省庁が違法事件等を解決できない場合の補完方法について定めておらず、慣例により、上級省庁に報告すると思われるが、段階別報告の末に中央にたどり着いた場合は、既に事件解決のタイミングを逃してしまう恐れがある。また、地方政府は責任回避のため、情報を隠蔽するか虚偽報告を行う可能性もないとはいえない。独立した監督機関の設置は、今後と課題であると思われる。

3.5　司法的救済の仕組み

65条の規定に基づき、いかなる組織、個人も、違法な個人情報処理活動について、個人情報関連業務担当省庁に対して苦情を申し立て、通報する権利を有している。個人情報関連業務担当省庁は、法に基づいて速やかに処理を行うとともに、処理の結果を苦情申立人や通報者に告知し、個人情報保護の職責を履行する部門は、苦情や通報を受け付ける連絡先を公表する義務がある。

また、70条は「事業者が本法の規定に違反して個人情報を処理し、多くの個人の権益を侵害した場合、人民検察院（検察庁）、法律が規定する消費者組織及び国家インターネット情報弁公室が指定した組織は、法に基づき人民法院（裁判所）に訴訟を提起することができる」としている。

70条の規定により、個人情報の侵害について、集団訴訟の可能性もあるようには見えるが、これ以上の詳細な規定は見当たらない。個人や組織は、個人情報関連業務担当省庁に個人情報処理の違法行為をまずは通報でき、担当省庁が多くの人々の個人情報権益の侵害につながると判断した場合は、検察庁や国家インターネット情報弁公室等が指定した組織が公益訴訟を通じ、司法救済を得ることが可能になっている。

3.6 研究・医薬品開発を目的とした診療データの二次利用

結論から述べると、研究目的で患者の診療データを利用したい場合は、①患者本人の明示的な同意を得るか、あるいは、②個人を特定できないかつ復元不可能になるように匿名処理を行う必要がある。従って、匿名処理を行っていれば、本人の同意がなくても利用できる。

中国には、日本の「次世代医療基盤法」のように、個人の医療データの利用・活用について定めている特別法は存在せず、一般法からその根拠を探る必要がある。

「情報安全技術―個人情報安全規範[10]（以下、「規範」とする、2020 年 10 月 1 日より施行）」によると、患者の医療データは、3.2 の敏感な個人情報に該当し、一旦改ざん、破壊、漏出または不正取得、不正利用されると、人身と財産安全、個人名誉、心身の健康に危害を及ぼすか差別待遇に繋がる可能性が高いデータの範疇に属している。従って、患者の診療データや記録への活用に対して、政府の立場は慎重である。国家衛生健康委員会医政司の副局長は、診療データの活用について「個人情報について匿名処理を行ったとしても患者の診療データは公共資源であり、医療機関、医療人員（関係者）は、関連部門の授権なしに取り扱う権限がない[11]」と強調し、医療データ扱いに対する中央政府の基本的な見方を示した。

「ネットワーク安全法[12]（2017 年 6 月 1 日より施行」42 条では、「ネットワークプロバイダは、自らが収集した個人情報を漏えい、改竄、毀損してはならない。提供者の同意を経ずに、他人に対し個人情報を提供してはならない。ただし、処理を経て特定の個人を識別するすべがなく、なお且つ復元不能である場合を除く。」と定めている。上記法律の施行ガイドラインとして「インターネットにおける個人情報安全保護指南[13]（以下「指南」とする、2019 年 4 月 10 日より施行）」が続いて公開されたが、「指南」6.3 二次利用 a）では、「個人情報の二次利用において、利用の範囲は、データ主体と締結した契約や協議内容に準ずる。契約や協議内容を超える範囲での個人情報の利用は認めない。ただし、匿名処理により、個人を特定できないかつ復元が不可能な個人情報については、契約や協議内容の範囲を超えての利用ができる。しかし、この場合でも適切な保護措置を講じる必要がある。」とした。

翌年に公開された、「規範」7.3 個人情報使用の目的制限では、「個人情報を利用する際には、個人情報を収集する時に提示した利用目的または関連範囲を超えてはならない。ここでいう関連範囲とは、個人情報を学術研究や自然、科学、社会、経済等の現象の全体状況の説明等に利用する場合を指す。ただし、対外に学術研究や説明結果を提供する場合は、結果の中に含まれている個人情報に対し、匿名処理を行うべきである。」と補足した。

従って、研究の目的で患者の個人情報を利用するルートは、患者の明示的な同意を得て利用するか、患者の診療データについて匿名処理を行い利用することになる。

では、患者の個人情報が漏洩された場合はどのなるのか。

まず、指南 6.6 の共有と移転では、「個人情報について共有、移転する際は、個人情報安全影響評価を行うべき。」としているが、指南はガイドラインに過ぎず、法的拘束力は有しない。

---

[10] 全文：情報安全技術―個人情報安全規範
http://www.100ec.cn/detail--6571570.html

[11] 2019 年 3 月、国家衛生健康情報化及び知恵病院設立における発表会でのコメントを参照。
https://www.sohu.com/a/315775037_658347

[12] 全文：ネットワーク安全法 https://www.jetro.go.jp/ext_images/world/asia/cn/law/pdf/others_005.pdf

[13] 全文：インターネットにおける個人情報安全保護指南
https://m.thepaper.cn/baijiahao_4000821

「ネットワーク安全法」42 条 2 項では、「個人情報の漏えい、毀損又は紛失が発生するか、発生する恐れのある状況においては、直ちに救済措置を講じ、規定に従い遅滞なく使用者に告知し、なお且つ関係所管機関に対し報告しなければならない。」としている。また、「オンライン診療管理弁法（暫定）[14]」20 条、「オンライン病院管理方法（暫定）[15]」23 条では「患者の個人情報、医療データの漏洩があった場合、医療機関は、主管衛生健康行政部門に報告し、有効な対応措置を取るべきである。」と定めている。医療機関の報告義務や適切な事後措置義務について抽象的に定めているものの、それ以上は記載がない。

診療データを二次利用する際に、どのような義務が課せられるか。

「規範」11.4 二次利用データ安全編では、医療データの二次利用における各プロセスで守るべき規定が定められている。

政府部門、研究者、企業等（以下申請者とする）は、非営利目的での医療データの二次利用ができる。データ量が大きく、全てのデータ主体に連絡できない、あるいは連絡コストが高すぎる場合は、下記プロセスで、データを有している機関（医療機関、地域の衛生情報プラットフォーム、医療連合体、医療学術団体等）を通じ、データを取得し、二次利用することができる。

①データ準備段階：データを有している機関は、二次利用に提供しようとするデータの目録やデータに対する説明を用意すべきである。

②二次利用申請者資格：申請時は、機関ベース（例：○○大学）で申請を行うのが望ましい。個人で申請を行う場合は、レベルの高い研究者に限る。（例：複数件のファンディングプロジェクトに採択されたことのあり、当該研究分野で高い専門知識を有する、かつ社会信用評価が A レベルであること）。データを有する機関は、申請者の申請歴史を漏れなく記録すべきである。

③データ審査段階：データを有している機関は、データ委員会を立ち上げるか独立した第三機関に審査を依頼し、申請者のデータ利用目的の正当性やデータの安全性等について審査を行う。審査員は、専門家データベースよりランダムに選ぶことが望ましい。データ委員会は章程、審査プロセス、審査記録等を制定すべきである。

④匿名処理：データを有する機関は、データを提供する前に、匿名処理を行うべきであり、最小計数原則（匿名処理を行った後、同条件を満たす人が最低でも 5 人になる必要がある）を遵守すべきである。例：今年 A 病院で子宮がんに診断された患者が 4 人であれば、病名を明かしてはならない。

⑤契約締結：データを有する機関と申請者は、データ送付前に、使用契約を締結し、データ保護措置、データが漏洩した場合の対策、データ使用期限等を明確に定める必要がある。

---

[14] オンライン診療管理弁法（暫定）全文：
https://baike.baidu.com/item/%E4%BA%92%E8%81%94%E7%BD%91%E8%AF%8A%E7%96%97%E7%AE%A1%E7%90%86%E5%8A%9E%E6%B3%95%EF%BC%88%E8%AF%95%E8%A1%8C%EF%BC%89/22876322?fr=ge_ala

[15] オンライン病院管理方法（暫定）全文：
https://baike.baidu.com/item/%E4%BA%92%E8%81%94%E7%BD%91%E5%8C%BB%E9%99%A2%E7%AE%A1%E7%90%86%E5%8A%9E%E6%B3%95%EF%BC%88%E8%AF%95%E8%A1%8C%EF%BC%89/22876336?fromModule=lemma_inlink

⑥データ送付時のデバイス：識別可能性が低いデータは、パスワードつきの e-mail や USB 等で送付できるが、患者の個人情報等が含まれており、識別可能性が比較的に高いデータは、遠隔操作等よるダウンロード等、安全性の高い方法を利用しなければならない。

⑦データの削除：申請者はデータ利用が終わり次第書面にて、データを有する機関に通知を行い、使用期限後の 30 日以内にデータを削除し、削除証明を、データを有する機関に送付する必要がある。データを有する機関は通知を受け取り次第検証作業に取り組むべきである。

中国国務院は、2018 年 4 月 28 日に「『オンライン＋医療健康』の発展を推進することに関する意見[16]」で、オンライン診療の普及とともに、オンオフライン医療サービスの一体化推進、2025 年までの「マイ健康 QR コード[17]」の導入を目指していると明かした。

医療オンライン化の推進に伴い、個人情報保護への懸念の声も高まっている。安全性の高い医療データベースやプラットフォームの構築だけでなく、患者の個人情報の保護における法律や政策の基盤も合わせて整えていく必要がある。

以上、中国の個人情報保護法制について述べてきたが、個人情報保護法は、未成年者の年齢を14歳以下指定し、死者の個人情報についても保護する等、GDPRと異なる部分があるとはいえ、類似して内容のほうが圧倒的に多い。中国で個人情報保護法はまだ新生法律であるため、実施細則等も公開されていなく、抽象的な内容や説明不足の箇所が多々あるが、引き続きこれからの動向をフォローしていきたい。

[16]全文： https://www.gov.cn/zhengce/content/2018-04/28/content_5286645.htm

[17] 日本でいえば、マイナンバーカードの医療バージョンのようなものであるが、一人一 QR コードで、スキャンすれば、その人とあらゆる健康情報、診療データが見られるものである。

参考資料

①程啸、“我国《民法典》中個人信息保護制度的創新與発展”、 财政法学、 第 4 期、2020

②程啸、“民法典编纂视野下的個人信息保護”、 中国法学、 第 4 期、2019。

③丁晓東、“個人信息私法保護的困境與出路”、 法学研究、 第 6 期、2018。

④丁晓東、“論数据携带权的属性、影响與中国应用”、 法商研究、 第 1 期、2020。

⑤韩旭至、“個人信息保护告知同意的困境与出路”、 经贸法律評論、 第 1 期、2021。

⑥張翱鹏、「中国の個人情報保護制度に関する研究」、忠北大学博士論文、2022。

⑦張恩典、“大数据时代的算法解释权: 背景、逻辑与构造”、 法学论坛、 第 4 期、2019。

⑧張新宝、“从隐私到個人信息: 利益再衡量的理論與制度安排”、 法学研究、 第 3 期、2015。

⑨張新宝、“個人信息收集: 告知同意原则适用的限制”、 比较法研究、 第 6 期、2019。

⑩張新宝、“互联网生态‘守門人’個人信息保护特別義務設置研究”、 比較法研究、 第 3 期、2021。

⑪趙宏、“信息自决权在我国的保护现状及其立法趋势前瞻"、 中国法律評論、 第 1 期、2017。

⑫張里安·韩旭至、“大数据时代下个人信息的私权属性”、 法学論壇、第 3 期、2016。

⑬趙万一、“从民法與憲法关系的视角谈我国民法典制定的基本理念和制度架构”、中国法学、第 1 期、2006。

⑭朱広新、“民事行为能力制度的完善——以中华人民共和国《民法总则(草案)》为分析对象”、当代法学、 第 6 期、2016。

⑮周汉華、“個人信息保護的法律定位”、 法商研究、 第 3 期、2020。

⑯田姬娟、「中国の個人情報保護法制の改善方案に対する研究」、成均館大学博士論文、2022。

⑰松尾 剛行「中国の個人情報保護法とデータ運用に関する法制度の論点」、総務省 学術雑誌『情報通信政策研究』 第 5 巻第 2 号、2021。

重要条文

民法典　第六章　プライバシー権及び個人情報
第 1032 条【プライバシー権】自然人はプライバシー権を有する。いかなる組織又は個人も密偵、侵入、漏えい、公開等の方式により他人のプライバシー権を侵害してはならない。 2　プライバシーとは、自然人の私生活の平穏及び他人に知られたくない私的秘密空間（プライベート空間）、私的秘密活動（プライベート活動）、私的秘密情報（プライベート情報）をいう。
第 1033 条【プライバシー権侵害の禁止】法律に別段の規定があり又は権利者の同意がある場合を除き、いかなる組織又は個人も次に掲げる行為を実施してはならない。（一）電話、ショートメール、インスタントメッセージ、電子メール、ビラ等の方式 により他人の私生活の平穏を侵すこと（二）他人の住宅、宿泊客室等の私的秘密空間に侵入し、撮影、盗視すること（三）他人の私的秘密活動を撮影、盗視、盗聴、公開すること（四）他人の身体の私的秘密部位を撮影、盗視すること（五）他人の私的秘密情報を処理すること（六）その他の方式により他人のプライバシー権を侵害すること。
第 1034 条【個人情報保護】自然人の個人情報は、法律の保護を受ける。 2　個人情報とは、電子又はその他の方式によって記録された、単独で又はその他の情報と結合して特定の自然人を識別することができる各種情報をいい、自然人の氏名、生年月日、身分証明書番号、生体識別情報、住所、電話番号、メールアドレス、健康情報、 移動履歴情報等を含む。 3　個人情報中の私的秘密情報については、プライバシー権の関係規定を適用する。規定がない場合、個人情報保護の関係規定を適用する。
第 1035 条【個人情報の処理に関する原則】個人情報を処理する場合、合法、正当、必要の原則に従わなければならず、かつ次に 178 掲げる条件に適合しなければならない。（一）当該自然人又はその後見人の同意を得ること。但し、法律、行政法規に別段の規定がある場合を除く。（二）情報の処理に関する規則を公開すること。（三）情報を処理する目的、方式及び範囲を明示すること。（四）法律、行政法規の規定及び双方の約定に違反しないこと 2 個人情報の処理には、個人情報の収集、保存、使用、加工、伝送、提供、公開等を含む。
第 1036 条【個人情報処理の免責事由】個人情報の処理が、次のいずれかに該当する場合、行為者は民事責任を負わない。（一）当該自然人又はその後見人が同意する範囲内で実施する行為（二）当該自然人が自ら公開し、又はその他の既に合法的に公開された情報を合理的に処理するとき、但し、当該自然人が明確に拒絶する場合、又は当該情報の処理により重大な利益侵害となる場合を除く。（三）公共利益又は当該自然人の合法的権益を維持保護するため、合理的に実施するその他の行為
第 1037 条【個人情報主体の権利】自然人は、法に基づき情報処理者からその個人情報を閲覧又は複製することができる。 情報に誤りがあることを発見した場合、異議を提出し、かつ速やかに訂正等の必要な措置を講じるよう請求する権利を有する。 2 自然人は、情報処理者が法律、行政法規の規定又は双方の約定に違反して当該個人情報を処理していることを発見した場合、情報処理者に対して速やかに削除するよう請求 する権利を有する。
第 1038 条【個人情報処理者の安全保護義務】情報処理者は、その収集、保存する個人情報を漏えい、改

ざん、毀損してはならない。自然人の同意を得ずに、個人情報を他人に対して違法に提供してはならない。但し、加工を経て特定個人を識別することができず、かつ復元できない場合を除く。 2 情報処理者は、技術的措置及びその他の必要な措置を講じて、その収集、保存する個人情報の安全を確保し、情報の漏えい、改ざん、紛失を防止しなければならない。個人情報が漏えい、改ざん、紛失する状況が発生し又は発生するおそれがあるときは、速やかに救済措置を講じ、規定に基づいて自然人に告知し、かつ関係主管部門に報告しなければならない。
第 1039 条【国家機関等の秘密保持義務】国家機関、行政職能を担当する法定機関及びその職員が、職責履行過程において知った自然人のプライバシー及び個人情報については、その秘密を保持しなければならず、 漏えい又は他人に対して違法に提供してはならない。

個人情報保護法　第四章 データ主体の（個人）権利
第 44 条【知る権利・決定権】 個人は、その個人情報の処理について知る権利、決定権を享受し、他人がその個人情報を処理することを制限又は拒否する権利を有する。法律、行政法規に別段の定めがある場合は、この限りではない。
第 45 条【閲覧・複製・情報移動権】 個人は、個人情報処理者からその個人情報を閲覧し、複製する権利を有する。本法第十八条第一項、第三十五条の規定する事由が存在する場合は、この限りではない。 個人がその個人情報の閲覧、複製を請求した場合、個人情報処理者は速やかに提供しなければならない。個人が個人情報をその指定する個人情報処理者に移転することを要求した場合で、国家インターネット情報部門が規定する条件に合致している場合、個人情報処理者は移転の手段を提供しなければならない。
第 46 条【訂正・補充を求める権利】 個人は、その個人情報が不正確又は不完全であることを発見した場合、個人情報処理者に対し、是正、補充を求める権利を有する。個人がその個人情報の是正、補充を請求した場合、個人情報処理者はその個人情報について確認したうえで、速やかに是正、補充しなければならない。
第 47 条【削除権】 以下に掲げる事由のいずれか一に該当する場合、個人情報処理者は自発的に個人情報を削除しなければならない。個人情報処理者が削除しない場合、個人は、削除を要求する権利を有する。(一)処理目的が既に実現した場合、実現不可能な場合、又は処理目的の実現のために必要ではなくなった場合。 (二)個人情報処理者が商品又はサービスの提供を停止した場合、 又は保存期限がすでに満了した場合。 (三)個人が同意を撤回した場合。 (四)個人情報処理者が法律、行政法規に違反し、又は約定に違反して個人情報を処理した場合。 (五)法律、行政法規が規定するその他の事由。 法律、行政法規が規定する保存期限が満了していない場合、又は個人情報の削除が技術的に困難である場合、個人情報処理者は、保存と必要な安全保護措置の実施を除き、それ以外の処理を停止しなければならない。
第 48 条【解釈・説明を求める権利】 個人は、個人情報処理者に対してその個人情報処理ルールについて解釈、説明を行うよう要求する権利を有する。
第 49 条【個人情報相続権】 自然人が死亡した場合、その近親者は、自身の合法、正当な利益のために、

死者の関連する個人情報について本章に規定する閲覧、複製、更生、削除等の権利を行使することができる。死者の生前に別段の取り決めがあった場合を除く。
第 50 条【訴訟提起権】 個人情報処理者は、個人からの権利行使の申請を受理、処理するための簡便なシステムを構築しなければならない。個人による権利行使の請求を拒否する場合は、その理由を説明しなければならない。個人情報処理者が、個人による権利行使の請求を拒否した場合、 個人は、人民法院（裁判所）に訴訟を提起することができる。

※本研究は、JST【ムーンショット型研究開発事業】グラント番号【JPMJMS2293】の支援を受けたものです。

IX. カナダ

山本健人（北九州市立大学）

はじめに

本報告書は、ムーンショット型研究開発事業の一つである「データの分散管理によるこころの自由と価値の共創」（プロジェクトマネージャー：橋田浩一）のディレクターのひとりである山本龍彦より依頼を受け、カナダの個人情報に関する法令調査を行ったものである。調査は依頼時の質問リスト（山本龍彦、飯田匡一、佐藤太樹作成）に基づき行った。本報告書では質問リストに回答する形式をとっている[1]。

本調査の対象であるカナダの個人情報保護法は連邦法と州法に分かれているが、本調査では、主に連邦法を対象とし、州法については補足的に触れるに留める。これは連邦法と州法で相違はあるものの連邦法が標準形であることによる。また、カナダでは個人情報保護の包括立法が公的部門を対象とするものと民間部門を対象とするものに分かれている。よって、本調査が主たる調査対象とするのは、連邦の公的部門を対象とするプライバシー法（*Privacy Act*, R.S.C. 1985）と、民間部門を対象とする個人情報保護及び電子文書法（*Personal Information Protection and Electronic Documents Act*, S.C. 2000 以下 PIPEDA）[2]である。なお、PIPEDA は州が PIPEDA と実質的に類似する法律を制定していない限り、当該州内においても適用される。現在、PIPEDA と実質的に類似する州法を有するのは、ケベック州、アルバータ州、BC 州の 3 州である。この他、個人健康情報（personal health information）についてのみ PIPEDA と実質的に類似する州法を有する州として、オンタリオ州、ニューブラウンズウィック州、ノバスコシア州、ニューファンドランド・ラブラドール州の 4 州がある。さらに、民間部門については、デジタル憲章実施法案（*Digital Charter Implementation Act*, 2022）が提案されており、消費者プライバシー保護法

[1] 同報告書の記述は、山本龍彦ほか編『個人データ保護のグローバル・マップ（仮）』（弘文堂、2024 年刊行予定）〔山本健人執筆部分〕と重なる箇所がある。また、以下の先行研究・先行調査に助けられたところも多い。石井夏生利「カナダのプライバシー・個人情報保護法」情報法制研究 1 号（2017 年）11 頁以下、消費者庁「諸外国等における個人情報保護制度の監督機関に関する検討委員会・報告書」（2011 年 3 月）〔河井理穂子執筆部分〕、消費者庁「諸外国等における個人情報保護制度の実態調査に関する検討委員会・報告書」（2009 年 3 月）〔佐藤信行執筆部分〕。

[2] PIPEDA は、民間組織が商業活動の過程で取り扱う個人情報の収集、使用、開示に関するルールを確立することを目的としており（3 条）、民間部門のあらゆる個人情報の取扱いではなく、商業活動の過程での個人情報の取扱いを規律することを想定している。

（*Consumer Privacy Protection Act*）、個人情報及びデータ保護審判所法（*Personal Information and Data Tribunal Act*）、AI データ法（*Artificial Intelligence and Data Act*）の導入が審議されている。同法案が可決されれば（現在連邦下院の第 2 読会を通過している）、PIPEDA の個人情報保護部分が消費者プライバシー保護法に置き換えられる。これらは現行法ではないが、法改正が成立すればカナダの個人情報保護法体系を大きく変更するものであるため、本調査の対象に含めている。

質問リストへの回答

1. 憲法と個人情報保護制との関係性

Q1-①. プライバシー権ないし情報自己決定権が、憲法上（条文または判例上）保障されているかどうか。またその際、プライバシー権と情報自己決定権との異同が意識されているかどうか。

憲法上の権利を規定する 1982 年の「カナダの権利及び自由に関する憲章」は明文でプライバシーの権利を規定していない。現在、カナダにおける憲法上のプライバシーは、不合理な捜索及び押収からの保護を規定する憲章 8 条によって保護されると解されている。表現の自由（憲章 2 条(b)）、民主的権利（憲章 3 条）、生命、自由及び身体の安全の権利（憲所 7 条）も憲法上のプライバシー保護にかかわるが、現時点では憲法上のプライバシー保護の中心は憲章 8 条である。

カナダ最高裁判所は、Spencer 判決[3]で、憲章 8 条が保護するプライバシーの利益を次のように整理している。まず、大きく①身体的プライバシー（自分の体、体液、そこから得られた物質、場合によっては所持品にも及ぶ）、②領域的プライバシー（私的な活動を行う場所に関するもので、最も中心的なものは住居だが、自家用車、職場、ホテルの部屋のような一時的な私的空間にも及びうる）、③情報プライバシーが区別される。そして、情報プライバシーについては、コントロールとしてのプライバシーが注目されてきたが、それだけに留まらないとして、さらに㋐秘密としてのプライバシー（医師と患者の間など、信頼及び信用関係の中で情報が共有されている場合に関わる）、㋑コントロールとしてのプライバシー（自分に関する情報がいつ、どのように、どの程度他者に伝達されるかを自ら決定する個人、集団、又は機関の主張に関連する）、㋒匿名としてのプライバシー（個人が、公共の場やオンライン上で他者から観察される可能性のある情報を共有したり活動を行ったりする際に、その活動を行った主体が誰かを特定されることなく活動できることを保護する）に細分化されている。

Q1-①の「プライバシー権」と「情報自己決定権」に必ずしも対応していないかもしれないが、カナダ最高裁は憲章 8 条のプライバシーを複合的な利益と捉えている、と回答することができる。これはプライバシー権と情報自己決定権あるいは

[3] *R. v. Spencer*, [2014] 2 S.C.R. 212

自己情報コントロール権を別の権利として分けるのではなく、プライバシー権という単一の権利のなかで、様々なプライバシーの利益の共存あるいは相補的な関係を認める方向性を示唆しており、興味深い。

Q1-②. プライバシー権ないし情報自己決定権が憲法上の権利として保障されている場合、かかる権利が、個人情報保護法の目的規定のなかに読み込まれているかどうか。別言すると、個人情報保護法が、プライバシー権などの憲法的価値を実現する法令として位置付けられているかどうか。

カナダの個人情報保護法は「準憲法的法律」と位置づけられている。これはカナダ最高裁が創り出したカテゴリーであり、個人情報保護法のほかに人権法（*Canadian Human Rights Act,* R.S.C. 1985）や情報アクセス法（*Access to Information Act* , R.S.C. 1985）などが準憲法的法律に位置づけられている。カナダ最高裁は、Lavigne 判決でプライバシー法を[4]、UFCW Local 401 判決で PIPEDA と実質的に類似するアルバータ州の個人情報保護法（*Personal Information Protection Act*, S.A. 2003）を準憲法的法律とした[5]。UFCW Local 401 判決によって、実質的に類似する連邦の PIPEDA も間接的に準憲法的法律と位置づけられたことになる。さらに、BC 州のプライバシー法（*Privacy Ac*t, R.S.B.C. 1996）[6]を準憲法的法律とした Douez 判決の法廷意見では、「プライバシー立法」が準憲法的地位にあるとされており[7]、これは「全てのプライバシー保護立法」が準憲法的法律であると述べたものだとする理解も示されている[8]。

カナダ最高裁によれば、準憲法的法律は「我々の社会の特定の基本的な目標」を反映したものであり、「その根底にある広範な政策的考慮を促進するように」解釈されなければならない[9]。準憲法的法律と位置づけることの効果は、「その特別な目的を認識」し[10]、通常は憲法上の権利の解釈に用いられる広く寛大な目的論的解釈を行うことを正当化するというものである[11]。カナダ最高裁はどのような特徴をもつ法律が準憲法的法律になるかについて明確な基準を打ち出してはいないが、「憲

[4] *Lavigne v. Canada (Office of the Commissioner of Official Languages), [2002] 2 S. C. R. 773,* at para.24-25.
[5] *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, [2013] 3 S.C.R. 733 at para.19.
[6] この法律はいわゆる個人情報保護法ではなく特定のプライバシー侵害行為を不法行為であるとする法律である。
[7] *Douez v. Facebook, Inc.*, [2017] 1 S.C.R. 751 at para.59.
[8] Andrea Slane, "There Is a There There: Forum Selection Clauses, Consumer Protection and the Quasi-Constitutional Right to Privacy in Douez v. Facebook" (2019) 88 S. C. L. R. (2d) 87 at 99.
[9] *Thibodeau v. Air Canada*, [2014] 3 S.C.R. 340 at para.12.
[10] *Lavigne v. Canada, supra* note 4, at para.24.
[11] Vanessa MacDonnell, "A Theory of Quasi-Constitutional Legislation" (2016) 53 Osgoode Hall Law Journal 508 at 510.

法が定める価値や権利と密接に結びついている」ことを準憲法的法律とすることの根拠として指摘しており[12]、学説では準憲法的法律は「憲法上の要請を実施するための法律」であると理解すべきだとの整理がなされている[13]。

この点に関して、①準憲法的法律は憲章8条が保障する権利の具体化ではなく、その背後にあるプライバシーに関する憲法的価値の具体化であること、②それゆえ、憲法上の権利としての具体化と、準憲法的法律としての具体化が分岐していることに注意が必要である[14]。なお、ここで想定されるプライバシーの憲法上の価値は、便宜的に㋐民主主義に関連するものと、㋑個人の自律に関連するものに整理できる。たとえば、Dagg判決のラフォレスト裁判官の反対意見（この点については多数意見を形成）で、アメリカの憲法学者ウェスティンの著作[15]などを引用しつつ、「プライバシーの保護が現代の民主的国家にとって基本的価値であること」、「プライバシーは、身体的及び道徳的な自律性、すなわち自分自身の考え、行動、決定に関わる自由に基盤を持つこと」が述べられている[16]。Lavigne判決はこの反対意見を引用し、これらの価値を再確認している（para.25）。さらに、UFCW Local 401判決は、「活力ある民主主義のもとでのプライバシー保護の重要性は、いくら強調してもしすぎることはない」という（para.22）。また、同判決は「個人が自分の個人情報をコントロールする能力は、個人の自律性、尊厳、プライバシーと密接に関係している。これらは民主主義の根幹をなす基本的価値である」ともいう（para.19）。

以上の通り、カナダにおいては憲法的価値と個人情報保護法の連関を読み取ることができ、これを憲法実施法であると捉える見解も有力である。

個人情報保護法を準憲法的法律として位置づけている点は、個人情報保護法と憲法の関係性が希薄と思われる日本と比べたとき示唆的である。とくに、カナダ最高裁が、もともと憲法実施法として制定されたわけではない個人情報保護法を、事後的に憲法的価値と関連性をもつ準憲法的法律として認めていった道程は[17]、日本における個人情報保護法と憲法のこれからの関係を考える上で参考になると思われる[18]。また、カナダ最高裁が民間部門を対象とする個人情報保護法も準憲法的法律としている点も重要である。この傾向は、私人間での個人情報保護を憲法的価値のもとで行っていく方向性を示しているといえるだろう。

---

[12] *Lavigne, supra* note 4, at para.25.
[13] MacDonnell, *supra* note 11, at 510-511.
[14] 厳密にいえば、公的機関を対象とする準憲法的法律は部分的には憲章8条の具体化として捉える余地もある。
[15] Alan F Westin, *Privacy and Freedom* (Atheneum, 1970).
[16] *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403, paras.65-66.
[17] 国家目標の具体化という観点からカナダの試みを再構成することもできるかもしれない。石塚壮太郎「社会国家・社会国家原理・社会法」法政論究101号（2014年）197頁以下参照。
[18] 異なるアプローチではあるが、實原隆志「個人情報保護法制と憲法」情報法制研究12号（2022年）38頁以下も参照。

2. 個人情報保護法制の現状と課題

Q2-①. 個人情報保護法を制定するにあたってモデルとした国はあるか。

プライバシー法、PIPEDA はともに、1980 年の OECD のガイドライン[19]に強い影響を受けているとされる[20]。とくに、PIPEDA は、OECD8 原則を参照してカナダ規格協会（the Canadian Standards Association）が作成した 10 原則（PIPEDA の別表 1）の遵守を原則とし、本体ではその例外を定めるという建付けになっている。また、PIPEDA 制定の背景としては、EU データ保護指令が採択されたことの影響もある。

Q2-②. クッキー情報は個人情報保護法制における「個人データ（個人情報）」のなかに含まれているか。個人情報保護法上保護の対象となる「個人データ（個人情報）」の定義。

プライバシー法も PIPEDA もその保護する「個人情報」は「個人を識別可能な情報」である。プライバシー法 3 条は、あらゆる形態で記録された個人を識別可能な情報を保護する。同条(a)~(i)号は、ここでいう個人情報に含まれる情報を列挙しており[21]、また、同条(j)~(m)号は同法の「個人情報」に含まれない情報を列挙する[22]。ただし、Dagg 判決でカナダ最高裁は、プライバシーの憲法的価値に言及したうえで、プライバシー法の「個人情報」は広く拡張的に定義されなければならないとしている[23]。よって、少なくともプライバシー法上の「個人情報」はプライバシー法自体が列挙している情報に限らず、広く保護の対象となりうる。

PIPEDA も個人を識別可能な情報を保護対象とする（2 条）。プライバシー法との違いの 1 つが、PIPEDA の場合は情報が記録されているか否かにかからず保護の対象に含まれる点である。OPC[24]のウェブページでは、年齢、氏名、ID 番号、収入、民族的出身、血液型、意見、評価、コメント、社会的地位、懲戒処分歴、ローン記

[19] Organisation for Economic Co-operation and Development, “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” (23 September 1980).
[20] Barbara von Tigerstrom, *Information & Privacy Law in Canada* (Irwin Law, 2020) at 233-234, 294.
[21] 本人の人種、国籍、民族的出身、肌の色、宗教、年齢、婚姻状況に関する情報、個人の学歴、病歴、犯罪歴、職歴に関する情報、個人が関与した金融取引に関する情報、個人に付与された識別番号、記号、個人の住所、指紋、血液型、個人の私的な意見などの情報が挙げられている。
[22] 過去又は現在連邦政府の職員であること、死後 20 年以上経過した個人に関する情報などが挙げられている。
[23] Dagg, *supra* note 16, para. 68.
[24] OPC はプライバシー法及び PIPEDA の監督機関であり、Office of the Privacy Commissioner の略称である。詳しくは Q2-④で説明する。

録、医療記録などが保護の対象に含まれるとされている[25]。

PIPEDA はクッキー情報について直接言及していないが、OPC のガイドラインによれば、個人に対してターゲティング広告を行うための「オンライン上での追跡及びターゲティングに関わる情報は、一般的に個人情報に該当する」としている[26]。このガイドラインに従えば、クッキー情報は PIPEDA の保護する個人情報となり、その収集、利用、開示には少なくとも黙示の同意が必要となる。

Q2-③. データ主体の権利と事業者の義務

Q2-③(a). 利用停止請求権の範囲

プライバシー法は、公的機関の事業又は活動の運営に直接関係する場合にのみ個人情報の収集を許容し（4 条）、目的外利用を禁止し（7 条）、公的機関に対して情報の正確性を維持することを義務付けるが（6 条）、公的機関の記録から個人情報の削除を求める権利は認めていない[27]。プライバシー法が規定するのは、自己情報の開示及び訂正を請求する権利、訂正請求を行ったが訂正がなされなかった場合、訂正の請求があった事実を当該情報に付記する権利である（12 条 2 項(a),(b)）。政府は、請求がなされた場合、通常 30 日以内に請求に対応する[28]。なお、プライバシー法に基づき、政府保有の自己情報の開示を請求できるのは、カナダ国民及び移民難民保護法[29]によって永住権を認められた者である（12 条 1 項）。

PIPEDA は、第 9 原則として個人のアクセスを挙げている。同原則によれば、個人には PIPEDA の適用対象となる組織（以下単に「組織」という場合もこの意味での「組織」を指す）が有する自己の個人情報に対する開示及び修正を請求することができる。請求者が組織の保有する個人情報が不正確ないし不完全であると証明した場合、組織は当該情報を修正しなければならない。この修正は情報の性質に応じて、情報の訂正、削除、又は追加（the correction, deletion, or addition of information）によって行われる（別表 1, s.4.9, 4.9.5）。

Q2-③(b). 同意の位置付け（オプトイン方式かオプトアウト方式か）。本人の同意が要求される場面は。事業者が個人データを取得する場合に当該個人の同意を得ることが義務付けられているかどうか。また、個人データが第三者に提供される場

[25] OPC, “PIPEDA in brief” (May 2019). 本報告書におけるウェブサイトの最終閲覧日はすべて、2023 年 9 月 13 日である。
[26] OPC, “Guidelines on privacy and online behavioural advertising” (December 2011; Revised: August 2021).
[27] Tigerstrom, *supra* note 20, at 242.
[28] OPC, “The Privacy Act in brief” (August 2019). Tigerstrom, *supra* note 21, at 241.
[29] *Immigration and Refugee Protection Act*, S.C. 2001, c. 27, s.2(1).

合、当該個人の同意を得ることが義務付けられているかどうか。

プライバシー法については、個人情報の収集、利用、（第三者への）開示に原則として事前の同意が必要である（8条1項）。同法8条2項は第三者への開示に本人の同意が必要ない場合として、大別して以下の5つを規定している。①収集された当初の目的又はその目的に合致した使用のために開示する場合、②連邦法で開示が許可されている場合、③裁判所または情報を強制する権限を持つその他の機関の令状又は命令に従う場合、④開示が明らかに個人の利益になる場合、⑤開示の公益がプライバシーの侵害を上回る場合[30]。

PIPEDAは、その第3原則が同意であり、個人情報の収集、利用、開示に原則として事前の同意を要求する。また、この同意のためには、個人情報の利用目的、使用・開示のされ方について合理的に理解できるような通知がなされなければならない。この点は、2015年のデジタルプライバシー法による改正でより明確にされた。同改正で追加された6.1条は、個人の同意は、個人情報の収集、利用又は開示の性質、目的、結果を理解することが合理的に期待できる場合にのみ有効である、としている。プライバシー慣行の重大な変更、個人情報の利用目的の追加・変更、新たな第三者への開示を行う場合も同意を得ることが求められる。子どもの個人情報については親あるいは保護者の同意を得る必要がある。同意の方法としては様々な方式が許容されているが、センシティブ情報については明示的な同意が必要だとされる。ただし、同法は医療記録や所得記録はほとんどの場合センシティブ情報に該当しうるとしつつも、個別具体的には文脈に依存するとしており、何がセンシティブ情報になるかについて明確な規定を置いていない。また、個人は、「法律上または契約上の制限および合理的通知に従い、いつでも同意を撤回できる」（別表1, s. 4.3.8）。なお、4条2項及び2015年の改正で追加された4.01条ではPIPEDAの適用除外が規定されており、同条項に該当する事項にはPIPEDAが適用されない。さらに、7条は個人情報の収集、使用、開示に（通知と）同意が必要ない場面を詳細に規定する。

Q2-③(c). ＜通知＝同意＞モデルの限界とその対策。個人の認知限界という観点から＜通知＝同意＞モデルの限界（同意疲れやプライバシーポリシーの流し読み）が予てから指摘されている。こうした課題に対して、各国の個人情報保護法制がどのように対応しているか（事業者に対して実効的な告知方法を義務付けるなど）。

カナダでも「意味のある同意」をどのようなものと考えるかは大きな論点となっている。

たとえば、OPCは2016年に「同意とプライバシー」についてディカッションペ

[30] *See,* OPC, "The Privacy Act in brief" (August 2019)

ーパーを公表し[31]、2018年には「意味のある同意を得るためのガイドライン」を公表している[32]。これらの取り組みは、まさに、冗長で法律的なプライバシーポリシーが使用されていることによって、個人情報のコントロールおよび個人の自律が、往々にして幻想に過ぎないものとなっている、との問題意識の下で行われている。

2018年のガイドラインでは、OPCがプライバシーポリシーのひな型を提案する案を否定し、組織こそが、法的義務だけでなく、顧客との関係の性質を尊重する同意プロセスを開発するための革新的かつ創造的な解決策を見出すのに最も適している、と述べている。このような前提のもと、このガイドラインでは組織がよりよい同意プロセスを設計する際に考慮すべき指針を挙げている。それは、①重要な情報を強調すること、②個人が、いつ、どのレベルの詳細な情報を得るかをコントロールできるようにすること、③「同意する」・「同意しない」の明確な選択肢を個人に提供すること、④革新的・創造的であること、⑤消費者の視点に立つこと、⑥同意を動的かつ継続的なプロセスにすること、⑦アカウンタビリティを果たすこと、の7点である。

一部簡単に補足すると、①は以下の4つの要素についてはプライバシーポリシーや利用規約のなかで埋もれてしまわないように強調する必要があるとする。それは、㋐どのような個人情報が収集されるか、㋑個人情報の共有先、㋒個人情報の収集、使用、開示の目的、㋓危害およびその他の結果に関するリスク、である。ただし、現時点では、どのような形でこれらの要素を強調すべきかの正解はないとされる。さまざまな分野でのベストプラクティスの出現が期待されている。②は、利用者の情報接触のさまざまな傾向――プライバシーポリシーなどの概要をざっと見たいだけの人、事前／事後に深く読み込みたい人など――に対応することが望ましいとされる。情報をレイヤー形式で表示することなどの工夫が求められる。④では、必要な情報を適時に表示することや、使用されるインターフェイスに適した同意プロセスの設計を奨励している。⑦では、「組織が有効な同意を取得していることを証明するためには、プライバシーポリシーに埋もれた項目を指摘するだけでは不十分」とし、「組織は、……個人から同意を得るためのプロセスがあり、そのプロセスが法律に定められた同意義務に準拠していることを証明できなければならない」としている。上記の通り、PIPEDAは、同意のために、個人情報の利用目的、使用・開示のされ方について合理的に理解できるような通知がなされることを要求している。⑦はこの点の確認でもあるが、OPCは単に冗長なプライバシーポリシーでこれらについて記述しているだけでは不十分であるとしているのである。同ガイドラインは、①～⑦のほかに、同意の撤回を尊重すべきこと、同意が銀

[31] OPC, "Consent and privacy: A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act" (May 2016).
[32] OPC, "Guidelines for obtaining meaningful consent" (May 2018; Revised: August 13, 2021).

の弾丸ではないことにも注意を促している。

法律レベルでは、原則同意を要求しつつも、同意が不要な場合の例外を幅広く認めようとする方向性を模索していると思われる。PIPEDA 自体もそうだが、とくに、消費者プライバシー保護法は、個人情報の収集、利用、開示について原則明示的な同意を求める枠組みを採用しつつも、同意が不要な場合などの例外を認めている。匿名加工情報の取扱いなどをも含め同意の例外を広範に例示することで、自己情報のコントロールと利便性のバランスを図ろうとしているものと思われる。

Q2-③(d). 情報銀行や PDS(Personal Data Store)のように、パーソナル・データに対する本人の controllability を補助するための仕組みや制度はどのように社会実装されているか。

プライバシー法は個人情報バンク（personal information banks）の仕組みをもつが、これは、各公的機関の長に対して、当該公的機関が管理する個人情報のうち、㋐行政目的のために利用された、利用されている、又は利用することができるもの、㋑個人の名前、個人に割り当てられた識別番号、符号、その他の特定の方法で整理され、検索できるようにされているもの、について、すべて個人情報バンクに登録させ、バンクの概要（当該情報を取り扱う趣旨、目的、情報の種類など）を一般公開する仕組みである。プライバシー法上の個人情報バンクは日本の個人情報保護法でいうところの個人情報ファイルの仕組みに近いものである。

一方で、PIPEDA には同様の仕組みはない。そのため、個人情報のコントロールは対公的部門では強く保障されているが、対民間部門ではコントロールを補助するための仕組みに課題があるといえる。

Q2-③(e). AI の利活用やプロファイリングの場面に特化したデータ保護の仕組みが存在するかどうか。

AI の利活用に特化した仕組みは現行法上ないが、AI データ保護法が成立すれば、AI の利活用に特化したデータ保護の仕組みが導入されることになる。

同法提案の狙いは、カナダの価値に沿う信頼できる AI 規正の枠組みを提示すると同時に、政府が責任あるイノベーションを阻害したり、AI の開発者、研究者、投資家、起業家を不必要に排除したりすることのないアジャイルなアプローチを採用しようとするものだとされている[33]。同法の目的は、AI システムの設計、開発、使用について、カナダ全土に適用される共通の要件を定めることにより、AI システムの国際的及び州間の商業活動を規律すること、及び AI システムに関連して、

[33] Innovation, Science and Economic Development Canada, “The Artificial Intelligence and Data Act (AIDA) – Companion document” (March 2023).

個人又は個人の利益に重大な損害を与えるおそれのある特定の行為を禁止することである。なお、同法は連邦の公的機関には適用されない。同法は EU の AI 規則案と同じくリスクベースアプローチを採用している。同法の仕組みは、AI システムを利用する企業に対して、当該 AI システムが「高影響システム（high-impact system）」かどうかを評価させ、高影響システムである場合には、設計、開発、使用可能にすること、または当該システムの管理について追加的な義務を課すというものである。何が高影響システムであるかは、別途規則で定める要素との適合性から判断され、その要素は、健康及び安全に対するリスクと人権に対するリスクの観点から設定される。さらに、①AI 開発のために不法に取得したデータを用いること、②深刻な身体的又は心理的危害を与える可能性のある AI システムを利用可能にし、当該 AI システムによって損害が引き起こされた場合、③公衆を騙すあるいは個人に実質的な経済的損失を与える意図をもって AI システムを使用することなど、に対して刑事罰を科しており、法人の場合は最高で 1,000 万ドルもしくは前会計年度の世界収益の 3%のいずれか大きい額の罰金となる。また、同法の監督などのために AI データコミッショナーが設置される。

プロファイリングに関する明文の規定は現行法上ない。しかし、PIPEDA の 5 条 3 項は「合理的な人が状況に応じて適切であると考える目的のためにのみ、個人情報を収集、使用、開示することができる」と規定しており、この規定は個人情報を扱う目的によっては同意を得たとしても組織が扱ってはならない「立入禁止区域（No-go zones）」を設定していると解されている[34]。OPC のガイドラインによれば、人権法が規定する事由に関する差別をもたらすような方法でおこなわれるプロファイリングは、5 条 3 項の適切な目的に該当しないと解されている[35]。

Q2-③(f). データ・ポータビリティ権は保障されているか。またこの権利は具体的にどのような場面で社会実装されているか。

現行法上はないと思われる。消費者プライバシー保護法はデータ・ポータビリティ権を規定している。

Q2-④. 個人情報保護法を執行する監督機関の組織と権限（制裁や告訴の仕組み）。

プライバシー法及び PIPEDA の監督機関は、プライバシー法によって設置されたプライバシー・コミッショナー及びコミッショナーを長とする OPC（Office of the Privacy Commissioner）である。

[34] OPC, "Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)" (May 2018).
[35] OPC, *ibid.*

コミッショナーは形式的には総督によって任命されるが、この任命にあたって連邦上院および下院の決議で任命の承認が行われる必要がある。コミッショナーの任期は 7 年であり、再任も可能である。現在のコミッショナー（2022 年 6 月 27 日～）は、人権問題、行政法、憲法を専門とする Philippe Dufresne 氏である。彼の前職は、法務サービスの提供や立法支援などを職務とする連邦下院の the Law Clerk and Parliamentary Counsel である。OPC の組織[36]は、大きく、①コンプライアンス部門、②政策推進部門、③組織管理部門に分かれており、各部門を担当する副コミッショナーによって監督されている。現在、3 名の副コミッショナーが置かれている。また、コミッショナー直属の④法務サービス部門が設置されている。それぞれ簡単に補足すると、①コンプライアンス部門は、プライバシー法及び PIPEDA に基づく調査を行う部門であり、市民からの苦情に基づく調査だけでなく、自己付託により調査を開始する場合もある。この部門には、プライバシー法部局、PIPEDA 部局、コンプライアンス・苦情受付・解決部局が置かれている。②政策推進部門は、プライバシーに関する一般的な情報やガイダンスの作成と普及、各業界・組織へのアドバイスなどを行う部門である。この部門には、政府助言部局、企業助言部局、政策・調査・議会部局、技術分析部局、コミュニケーション部局の 5 つの部局が置かれている。③組織管理部門は、OPC の組織内部の事務および管理を担う部門であり、人材部局、財務・経理部局、情報管理・情報技術部局、事業計画・業績・監査・査定部局が置かれている。④法務サービス部門は、法的助言を行うことで OPC の業務活動を支援する部門である。また、これらの他に内部監査委員会も置かれている。

コミッショナーは、個人情報の不適切な利用、個人情報へのアクセス拒否などの苦情を受付け、調査を行う権限などを有する。調査は職権によって行うこともできる。公的機関への立入調査を行う権限なども付与されており、調査結果や勧告を公的機関の長に報告するが、その判断に拘束力はない（29~35 条）。プライバシー法は同法違反に対する損害賠償を求めることができる規定も持たない。個人情報の開示拒否の場合は、調査結果の報告を受けた後、当該個人及びコミッショナー自身も個人の同意に基づき、連邦裁判所に審理を求めることが可能である（41, 42 条）。この申請は、調査結果の受領後 45 日以内もしくは裁判所が認める期間内におこなわなければならない。

PIPEDA に関しても、コミッショナーはプライバシー法の場合と同様の権限を有しており、調査結果に法的拘束力はなく、PIPEDA 違反に対して制裁金や損害賠償を命じる権限はない。コミッショナーによる調査報告書もしくは調査の中止の通知の受領後、個人は連邦裁判所に審理を求めることが可能であり、コミッショナーも個人を代理してこれを行うことができる（14, 15 条）。連邦裁判所への申請の期限は、報告書もしくは調査中止の通知の受領後、1 年以内もしくは裁判所が認めた

[36] *See*, OPC, “Organizational Structure” (August 2023).

それ以上の期間内である（14 条(2)）。連邦裁判所は、PIPEDA に適合するように組織の慣行を是正するよう命じることや、組織に損害賠償を命じることなどを含む救済を与えることができる（16 条）。また、2015 年のデジタルプライバシー法による改正によって、コンプライアンス協定という仕組みが導入されている。これは、コミッショナーが、ある組織が PIPEDA 違反ないし別表 1 の遵守事項の不履行となる作為・不作為を行った・行おうとしている・行う可能性が高いと合理的根拠に基づき判断した場合、PIPEDA を遵守することを目的とするコンプライアンス協定を締結することができる、というものである。コンプライアンス協定は組織に PIPEDA の遵守に同意することを求めるが、その代わりに、協定を締結した場合、コミッショナーは 14 条・15 条に基づく連邦裁判所への申請を行うことができなくなる。ただし、組織がコンプライアンス協定に違反した場合は、組織に協定の内容を遵守するよう求める命令を裁判所に申請することができる。

プライバシー・コミッショナー及び OPC は、「『プライバシーと他の法益の衝突に直面した場合には、プライバシーの保護を優先させる』という一般的傾向性」を持つと指摘されており[37]、カナダのプライバシー保護にとって重要な役割を担っているが、その権限自体は強力なものではない。消費者プライバシー保護法はプライバシー・コミッショナーの権限強化にも取り組もうとしている。

Q2-⑤．司法的救済の仕組み（訴訟要件、集団訴訟の可能性）

プライバシー法および PIPEDA に基づく司法的救済の仕組みは上記（A7）の通りであるが、若干の補足をしておく。

プライバシー法については、個人の情報アクセス制限に対してのみ裁判所への提訴を認めているが、近時の下級審のなかには、プライバシー法に反する個人情報の収集についても司法審査の対象としたものがある[38]。また、クラスアクションについては、連邦裁判所規則の Part 5.1 に従い認められるかが判断される[39]。PIPEDA については、同法 14 条に基づく手続においてクラスアクションが認められるかが争点となっているようである[40]。

なお、個人情報及びデータ保護審判所法は、個人情報及びデータ保護を専門的に扱う審判所を設置することを構想している。同審判所は、消費者プライバシー保護

[37] 佐藤・前掲注（1）181 頁。
[38] Union of Canadian Correctional Officers - Syndicat des Agents Correctionnels du Canada - CSN (UCCO-SACC-CSN) v. Canada (Attorney General), [2017] 3 F.C.R. 540
[39] *e.g.*, *Canada v. John Doe*, 2016 FCA 191. 直近では、カナダ政府のオンラインアカウント（カナダ歳入庁の「マイアカウント」・「マイサービスカナダ」）の使用に伴い発生した権利侵害の可能性についてクラスアクションが提起されている。*See,* Government of Canada, "Notice of Certification: Government of Canada Privacy Breach Class Action" (August 2023).
[40] *See*, *Haikola v. The Personal Insurance Company*, 2019 ONSC 5982.

法に基づく申立て、同法に基づくペナルティの賦課について管轄権を有する。審判所は 3～6 名の構成員からなり、最大任期は 5 年である（ただし再任は可能）。構成員は同法の担当を指名された大臣の推薦に基づき、総督によって任命される。構成員のうち少なくとも 3 名は情報・プライバシー法の分野での経験を有する者でなければならないとされている。

プライバシー法や PIPEDA に基づく司法救済とは別に、コモンローあるいは、特定の行為をプライバシー侵害とする州法[41]に基づいてプライバシー侵害を理由とした救済を求める仕組みもある[42]。

Q2-⑥．診療記録等を医薬品開発などの研究目的で利用する場合に、データ主体である患者の同意は要請されるのか？診療データを二次利用するにあたって、匿名加工などの一定の義務が課せられるか？

本質問項目は追加質問として示されたされたものであり、短期間で調査することは困難であったため回答不能である。以下では参考までに、カナダにおける個人健康情報に関する法制度の概要と、オンタリオ州の個人情報保護法の規定について若干の紹介をするが、不十分な調査であることをお断りしておく。

カナダにおける個人健康情報の取扱いはかなり複雑である。多くの州で個人健康情報を特別に扱う法律が存在しており（→はじめにを参照）、また、公的部門に適用されるものと民間部門に適用さるものが分かれている場合もある。さらに、個人健康情報の商業的利用については PIPEDA の適用もある。このように入り組んだ体系となっているため、実態把握のためには実質的には各州法を調査する必要があるので、本調査期間内で調査することは困難であった。

オンタリオ州の個人情報保護法（*Personal Health Information Protection Act*, S.O. 2004）に関する規律を紹介しておく。

同法によれば、個人健康情報[43]の研究目的での開示については一定の条件の下、本人の同意を得る必要はない（44 条）。その条件として、まず、①個人健康情報の保管・管理者（health information custodian、以下単に「管理者」とする）に、書面で、研究計画書及び当該研究計画を承認した研究倫理委員会の審査結果の写しを提出することが求められる。研究計画には、㋐研究に関与する人物の所属、㋑研究の性質・目的、および研究者が予測する研究の公益または科学的利益などの記載が

41 e.g., *supra* note 6.
42 *See*, Tigerstrom, *supra* note 20, ch2.
43 同法の定義する「個人健康情報」は個人を識別する情報であり、個人の身体的または精神的健康に関する情報、個人に対するヘルスケア提供に関する情報、個人に関する医療費の支払いに関する情報、個人の健康番号などが含まれる。また、「識別する情報」には、単独で識別可能なものだけでなく、他の情報と合わせて使用することで識別が可能となり、その状況が合理的に予測できる情報も含まれる（4 条）。

求められる。倫理審査では、以下の観点を含む関連事項が考慮されなければならない。ⓐ個人健康情報の開示対象となる個人のプライバシーを保護し、情報の機密性を保持するための適切な保護措置が講じられるかどうか、ⓑ研究を実施することの公益性、および個人健康情報が開示される個人のプライバシーを保護することの公益性があるかどうか、ⓒ個人健康情報が開示される個人の同意を得ることが非現実的であるかどうか。次に、②個人健康情報を開示する前に情報の取扱いについて管理者の課す条件に研究者が従うことに同意する契約を結ばなければならない。この他、③研究者には、倫理委員会から承認された目的のためにのみ情報を利用すること、個人の識別が合理的に可能になる形で情報公開しないことなどの遵守事項が課せられている。

以上。

※本研究は、JST【ムーンショット型研究開発事業】グラント番号【JPMJMS2293】の支援を受けたものです。

X. アメリカ

米国の連邦プライバシー法とカリフォルニア州プライバシー権法の概説

Jesse Woo

アメリカ合衆国のプライバシー法体系は、教義的にも実務的にも、あらゆる管轄の中でも最も複雑なものの一つである。この複雑性は（欧州の一般データ保護規則のように）データの収集と処理に関するほとんどの側面を規制しようとする単一の法令体制に起因しているのではなく、むしろその逆が原因となっている。米国の消費者プライバシー法は断片的で、包括的な準拠法が欠けている。本レポートでは、米国の連邦プライバシー法と、本稿の執筆時点では国内において消費者を最も包括的に保護するプライバシー法であるカリフォルニア州消費者プライバシー法（CCPA）およびカリフォルニア州プライバシー権法（CPRA）の概要を提供する。

本レポートの第 1 節では米国の連邦レベルと州レベルでのプライバシー法の大まかな概要を提供し、自主規制モデルの実際的な重要性、そして同意に関連して浮かび上がっている課題について述べる。第 2 節では執行に関する課題を取り上げる。

1.1 米国憲法

情報プライバシーとは直接関係していない一部の特筆すべき例外を除くと、米国憲法は私的訴訟よりも政府の権力を規制している。米国人（国民および永住権保持者）に「憲法上の権利」があると言う場合、これは一般的に政府による何らかの行動に対する権利、または少なくとも特定の私的訴訟への政府の支持に対する権利のことを意味している。[1] 「プライバシー（privacy）」という用語も、憲法の本文には明記されていない。

それでも、プライバシーに関連する概念は（中でも）修正第 1 条、修正第 4 条、および修正第 5 条、ならびに司法的に導出される実質的な適正手続き（substantive due process）の法理から生じているといわれている。修正第 1 条は表現の自由の権利を守っており、最高裁判所は自由な表現には、そのような表現に従事する特定の団体には匿名性の権利が求められると判示している。[2] これはかなり現実的な意味で情報プライバシーの一形態であるが、政府が団体に属する匿名のメンバーが誰であるか開示するよう強制しようとする場合などの、限られた状況にしか適用されない。修正第 5 条は刑事被告人が自らを罪に陥れることから守り、私有財産を保護しているが、学者らはこれをプライバシーの権利の一種として特徴づけている。加えて、実質的な適正手続きの法理は、個人の自律性を保護するプライバシー権の一種として捉えられている。

[1] 例えば、人種制限約款という形の随意契約は、政府の措置を施行する必要があったため、憲法修正第 14 条の平等保護条項に基づいて違憲であるという判示が下されている。Shelley v. Kraemer 334 U.S. 1 (1948).
[2] NAACP v. Alabama ex. Rel. Patterson 357 U.S. 449 (1958).

産児制限手段へのアクセス、異人種間結婚、そしてごく最近までは中絶する権利も実質的な適正手続きにより守られていた。

情報プライバシーに最も直接関係している憲法の条項は修正第 4 条であろう。修正第 4 条は政府の捜査官による不合理な捜索および押収から個人を守っており、刑事訴追の文脈において援用されることが最も多いが、他の政府関係者にも広く適用される。修正第 4 条の本文は「身体、家屋、書類、所持品」の不合理な捜索および押収を扱っているものの、政府による電子データへのアクセスを規制するようにもなっている。例えば最高裁判所は、政府が携帯電話の内容をデジタルに捜査する前、[3] ならびに携帯電話の記録に基づいた人の位置の記録にアクセスする前 [4] に令状を取得しなくてはならないと判示している。既存の資料が同条について詳しく言及している。米国憲法のプライバシーへの適用は、政府による行動の範囲を超えると限られていると言える。いくつかの州の憲法も明示的にプライバシー権を列挙しており、一部の事例では州の権利が連邦政府の憲法による権利よりも強いことが示唆されているものの、実際には連邦憲法にも州憲法にも情報自己決定権のようなものは何もない。

1.2 米国プライバシー法：連邦レベル

一般的に適用可能な連邦政府の消費者プライバシー法や包括的なデータ保護法はない。代わりに、米国では「セクトラル」アプローチを採っており、特定の業界または業種がそれぞれの適用範囲が限られる法律により統治されている。例えば、ヘルスケアプライバシーは医療保険の携行性と責任に関する法律（HIPAA）が、金融のプライバシーはグラム・リーチ・ブライリー法（GLBA）または米国公正信用報告法、政府記録は連邦プライバシー法により統治されている。これらの法律の適用範囲は一般的に特定の組織に制限されており、例えば HIPAA は診療所とその「業務提携先」などの法律で定義されている「対称事業体」により処理される特定のデータに適用されている。診療データを保持しているもののこれらの定義のどれにも該当しない組織は、HIPAA が定める制約に拘束されない。同様に、特定の規制機関がその管轄範囲内にある組織を統治する規則を発行することがある。米国保健福祉省は、HIPAA の法文をさらに定義するためにプライバシー規則を発行している。一方で、児童オンラインプライバシー保護法（COPPA）は設定または産業にかかわらず 13 歳未満のすべての子供のデータを保護しているが、事業体が子供のデータを保持している、または自社のサービスを子供に仕向けているという「実際の知識」を有している場合のみに適用される。

連邦レベルでの主なプライバシー規制者は連邦取引委員会（FTC）であり、「通知と選択」制度を執行している。[5] FTC は「第 5 条（Section 5）」と呼ばれる、商業における「不公正で欺瞞的な慣行」を規制する権限を FTC に付与する権限法によりその権限が与えられている。

---

[3] Riley v. California 573 U.S. 373 (2014)
[4] Carpenter v. United States, 138 S.Ct. 2206 (2018)
[5] Federal Trade Commission, “Protecting Consumer Privacy in an Era of Rapid Change”, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf

プライバシーに関しては、FTC は一般的に欺瞞的慣行の疑いのある企業の調査を実施し、適宜「同意判決（consent decree）」と呼ばれる、企業が罰金を支払い訴訟を回避するためにその行動を変更することに合意するという交渉による合意の一種を発布する（これは、有罪を認めるようなものである）。同意判決書は公開され、連邦レベルでのプライバシーについて限定的なコモン・ローを形成する。ここでは再掲しないが、FTC のプライバシーに関する同意判決については数多くの文献レビューが行われている。政治史に関係するいささか難解な理由により、FTC は通常は第 5 条による権限に基づいて規則を発行することがないものの、議会が COPPA などの別の法律により権限が与えられている場合には規則を発行する。このように権限が限られていることにより、FTC は主に企業が欺瞞的に行動した場合に行動する（事実と異なる公式声明をプライバシー方針に記載している場合など）。

これらのことは、ヘルスケアや金融などの厳しい規制を受けている業界を除く他の企業にとって、連邦政府のプライバシー法に準拠するために行わなくてはならないことが比較的少ないことを意味している。これらの企業は一般公開されている方針を打ち出しているべきであり、その方針に記載した条件に守らなければならない。一般的に、方針は「ベストプラクティス」に基づいており、企業に行動するための自由を与えるような書き方がなされる。これらの方針が曖昧であること、または理解しづらいように書かれていることが多いのは、このためである。企業は消費者にプライバシー方針という形で「通知」し、その方針の条件を受諾するかどうかという形で「選択」を与えなくてはならない。情報自己決定が憲法上で保障されていないのと同じように、連邦レベルでのデータ保護法もないため、規制においては、企業による個人データを収集、処理、移転する能力について極めて寛容な姿勢をデフォルトで示している。

1.3 州のプライバシー法：CPRA

複数の州が一般的に適用される消費者プライバシー法を制定しているが、最も強い影響力を持ち、最も多くの保護を保障しているのはカリフォルニア州のプライバシー権法（CPRA）である。CPRA は前身のカリフォルニア州消費者プライバシー法（CCPA）と呼ばれるプライバシー法を改正したものであり、これらはまとめて米国の消費者プライバシー法における大きな転換点として見られることが多い。同法はカリフォルニア州で事業を運営しており、年間総売上額が 2500 万ドルを超える法人、10 万人以上の消費者の情報の売買ならびに共有を行っている法人、または消費者情報の販売または共有が自社の売上額の 50%以上を占めている法人に適用される。[6] カリフォルニア州は米国内の州の中でも最大の人口と経済規模を誇るため、CPRA の影響も連邦法ではないにもかかわらず極めて大きい。

同法は特定の消費者の権利、すなわち①アクセス権、②訂正権、③削除権、④情報が販売または共有される方法を知る権利、ならびに⑤データの販売を防ぐ権利を保障している。CPRA の下では、消費者は企業が消費者に提供している財やサービスを届けるために必要な目的に沿って当該企業が「機微な個人情報」を利用または開示することを制限する権利も有している。企業は、他のいかなる方法によってもこの情報を利用することについて同意を取得しなければならない。[7] GDPR で規定されているような処理やプロファイリング、またはデータ・ポータビリティに対し異議を申し立てる具体的な権利はない。

また、企業は個人データの収集、利用、保持、共有を収集した目的に沿って必要かつ比例的である程度に制限しなければならない。[8]

[6] California Civil Code 1798.140 (d).
[7] California Civil Code 1798.121.

8 California Civil Code 1798.100 (c).

収集主体との合意の下で個人データを取得する第三者も、これらの権利や制限を尊重しなくてはならない。

CPRA は個人情報を以下のとおり定義している：

特定の消費者または世帯を識別し、関連し、記述し、合理的に関連付けることが可能であり、または直接的もしくは間接的に合理的に関連付けることが可能である情報。個人情報には、特定の消費者または世帯を識別し、関連し、記述し、合理的に関連付けることが可能であり、または直接的もしくは間接的に合理的に関連付けることが可能である場合、以下のものが含まれるが、これらに限定されるものではない。

(A) 本名、偽名、郵便住所、固有の個人識別子、オンライン識別子、インターネットプロトコルアドレス、電子メールアドレス、アカウント名、社会保障番号、運転免許証番号、パスポート番号、またはその他の類似の識別子などの識別子。

(B) 第 1798.80 条（e）に記載される個人情報。

(C) カリフォルニア州法または連邦法に基づく保護対象階級の特徴。

(D) 個人資産、購入、入手、検討した製品またはサービス、あるいはその他の購入または消費の履歴または傾向に関する記録を含む商業情報。

(E) 生体認証情報。

(F) 閲覧履歴、検索履歴、消費者とインターネットウェブサイトアプリケーションまたは広告との相互作用に関する情報を含むが、これらに限定されない、インターネットまたはその他の電子ネットワーク活動情報。

(G) ジオロケーションデータ。

(H) 音声情報、電子情報、視覚情報、熱情報、嗅覚情報、またはこれらに類似する情報。

(I) 職業上または雇用関連の情報。

(J) 教育情報。家族教育権とプライバシー法（20 U.S.C. Sec. 1232g; 連邦規則集第 34 巻パート 99）で定義される、公に入手可能な個人を特定できる情報ではない情報として定義される。

(K) 消費者の嗜好、特性、心理的傾向、素質、行動、態度、知能、能力、および適性を反映する消費者に関するプロフィールを作成するために、本細則で特定される情報のいずれかから引き出される推論。

(L) 機微な個人情報。

CPRA では一般公開されている情報、公共の関心事、または集約あるいは非識別化された情報をこの定義から除外している。[9] これは米国プライバシー法における最も細かく包括的な個人情報の定義の一つとなっており、クッキーやその他のオンライン上の識別子も含まれる可能性が高い。また、他の情報から導出される推論も含めることで、機械学習の重要性も予期しているようである。機微な個人情報は GDPR の特殊カテゴリに分類されるデータの定義と似た別のカテゴリのデータであるが、同時に「正確なジオロケーションデータ」も包含している。[10]

また、同法は、法律を執行し、曖昧さを解消し、新たな問題に対処する規則を発行するためにカリフォルニア州プライバシー保護局を設立している。しかし、同法のほとんどが引き続き通知と同意に依存している点は重要である。企業は自社によるデータの利用方法について消費者に通知し、変更について同意を取得しなければならない。州法としてカリフォルニア州の消費者にサービスを提供する企業に適用されるが、位置により差別化することは難しいため、多くの企業が広範に適用することを選択している。

CCPA と CPRA は、特に消費者の権利やデータ最小化の原則を重視するという点において GDPR からある程度のヒントを得ているようであり、EU の法体系から借りている用語である「必要かつ比例的」という文言にこのことが窺える。消費者データを保護する義務はデータを保有する者が代わる場合にも契約上データとともに移らなければならないが、データの「管理者」及び「処理者」という同じ文言は用いていない。[11] 一般的に GDPR ほど包括的であることを目指しておらず、AI などの台頭しつつある分野を明示的に規制することを遠慮している（すなわち、自動処理に関する規定が定められていない）。

1.4 プライバシーの基準と自主規制

すべての管轄において（そして特に米国のような明示的なプライバシー法が定められていない管轄において）、業界の基準や自主規制がプライバシー保護の重要な源泉となっている。最も一般的な一連の基準は公正情報取扱原則（Fair Information Practices、「FIPs」）である（稀に Fair Information Privacy Practices または FIPPs とも呼ばれる）。経済協力開発機構（OECD）は 1980 年代に最も引用されているバージョンの FIP を明確にしている。[12] FTC も同様の内容を記した独自の原則を策定している。[13] FIP は、優れたプライバシーを構成する要素に関する広範な原則またはガイドラインである。FIP の原則は次のとおりである：

1. **収集制限の原則。**個人データの収集には制限を設け、いかなる個人データも、適法かつ公正な手段によって、及び必要に応じてデータ主体に通知し、又は同意を得た上で収集すべきである。
2. **データ内容の原則。**個人データは、利用目的の範囲内において利用し、かつ利用目的の達成に必要な範囲内で正確、完全及び最新の内容に保つべきである。

[9] California Civil Code 1798.140 (v)
[10] California Civil Code 1798.140 (ae).
[11] California Civil Code 1798.100 (d)(2).
[12] OECD, “Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data”, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188
[13] FTC “Privacy Online: Fair Information Practices in the Electronic Marketplace”, https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf

3. **目的明確化の原則。**個人データの収集目的は、データが収集された時点よりも前に特定し、当該利用目的の達成に必要な範囲内における事後的な利用又はその他の目的での利用は、その利用目的に矛盾しない方法で行い、利用目的を変更するにあたっては毎回その利用目的を特定すべきである。
4. **利用制限の原則。**個人データは、第 9 項（上記③目的明確化の原則）により特定された目的以外の目的のために開示すること、利用可能な状態に置くこと又はその他の方法で利用すべきではない。ただし、以下の場合はこの限りではない。
    a. データ主体の同意がある場合。
    b. 法令に基づく場合。
5. **安全保護の原則。**個人データは、その滅失若しくは不正アクセス、き損、不正利用、改ざん又は漏えい等のリスクに対し、合理的な安全保護措置を講ずるべきである。
6. **公開の原則。**個人データの活用、取扱い、及びその方針については、公開された一般的な方針に基づくべきである。その方法は、個人データの存在及び性質に応じて、その主要な利用目的とともにデータ管理者の識別及び通常の所在地を認識できる方法によって示すべきである。
7. **個人参加の原則。**個人は次の権利を有する。
    a. データ管理者が自己に関するデータを保有しているか否かについて、データ管理者又はその他の者から確認を得ること。
    b. 自己に関するデータを保有している者に対し、当該データを、i. 合理的な期間内に、ii. 必要がある場合は、過度にならない費用で、iii. 合理的な方法で、かつ、iv. 本人が認識しやすい方法で、自己に知らしめられること。
    c. 上記（a）及び（b）の要求が拒否された場合には、その理由が説明されること及びそのような拒否に対して異議を申立てることができること。
    d. 自己に関するデータに対して異議を申し立てること及びその異議が認められた場合には、そのデータを消去、訂正、完全化、改めさせること。
8. **責任の原則。**データ管理者は、上記の諸原則を実施するための措置を遵守する責任を有する。

学者らは FIP の有用性について議論しているものの、[14] これらは「優れた」プライバシーの基準として頻繁に引用されている。多くの企業のプライバシー方針が、これらの原則に言及する形で作成されている。企業が「優れた」プライバシー慣行について語る場合、多くの場合何らかの形で FIP を参照しているのである。

1.5 同意とダークパターン

前述のとおり、米国のプライバシー法は主に「通知と選択」、または同意に基づくモデルに従って運用されている。しかし、デジタル・インターフェースにおいて消費者に自己のプライバシーを犠牲にして企業の利益に有利な選択肢へと消費者を微妙にナッジできるような選択アーキテクチャや行動心理学的な手法が普及していることから、近年の研究では同意を効果的に行使する消費者の能力の限界に注目している。[15]

---

[14] Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 Md. L. Rev. 952 (2017). https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=3759&context=mlr

[15] Jen King, Adriana Stephan, *Regulating Privacy Dark Patterns in Practice – Drawing Inspiration from California Privacy Rights Act*, 5 Geo. L. Tech. Rev. 250 (2021). https://georgetownlawtechreview.org/wp-content/uploads/2021/09/King-Stephan-Dark-Patterns-5-GEO.-TECH.-REV.-251-2021.pdf.

全体的に、これらの手法は「ダークパターン」として知られている。この取り組みはまだ始まったばかりであるが、米国法における情報自己決定権に最も近い類似の概念であると思われる。

2010 年代以前も、FTC は理解不足が利用者側によるインフォームドコンセントを弱体化させていたことを指摘している。[16] Effen Ads や Vizio の同意判決などのように、委員会はその第 5 条による権限を利用して隠れた手数料を請求したりデータ収集慣行を不明瞭にするような欺瞞的な慣行を行ってきた企業に対して頻繁に執行してきた。[17] しかし、FTC が正式な方針としてダークパターンに対する取り締まりを強化することを発表したのはごく最近の 2021 年のことである。[18] このような規制上の立場の強化は歓迎すべき知らせであるが、同意モデルの侵食は 20 年以上にもわたり発生しており、法的権限がないことが大きな足枷となって委員会はそれを抑止できていない。

CPRA はより強固な同意要件を課し、ダークパターンに直接対処しようとしている。州司法長官の下に結成された新しい執行機関はカリフォルニア州プライバシー保護局（CPPA）と呼ばれ、CPRA における諸問題の中でも同意要件を明確にし詳しく説明する規則を提案している。CPPA は、同意が「自由に与えられ、具体的で、十分な情報に基づいており、消費者の希望を明確に示すもの」でなくてはならず、ダークパターンを利用してはならないことを明記している。[19] また、同意を取得する際におけるダークパターンの利用に対処するための追加の規制も認めている。[20] 規制の草案では、同意が①理解しやすいこと、②選択の対称性を反映していること（「はい」よりも「いいえ」と言う方が難しくないこと）、③紛らわしい言葉遣いやインタラクティブな要素を避けること、④巧みに操られた言葉遣いやアーキテクチャを避けること、⑤実行しやすいことを義務付けるであろう。[21] その他のすべての同意の仕組みはダークパターンと見なされる。
別の取り組みでありつつもある程度関係しているものとして、米国プライバシー法に忠実義務（duty of loyalty）を導入するという提案がある。忠実義務は、企業が利用者データの収集と処理を行う際に、利用者の最善の利益に沿って行動することを要求する学術的な概念である。[22] 例えば、利用者情報を収集するウェブサイトは、利用者がそのウェブサイトにデータを託していることから、そのデータを利用者の最善の利益のために利用することが義務付けられる。さらに、第三者へのデータの販売などといった一部の活動もそれ自体が不義な行為を構成するものになる。忠実義務は理論としてまだ新しいものの、いくつかの立法案に取り込まれている。[23] この取り組みはプライバシー理論の最先端を代表しており、

---

[16] Federal Trade Commission, “Protecting Consumer Privacy in an Era of Rapid Change”, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf
17 Effen Ads, LLC (iCloudWork) https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3202-effen-ads-llc-icloudworx. Vizio Inc. and Vizio Inscape Services, LLC https://www.ftc.gov/legal-library/browse/cases-proceedings/162-3024-vizio-inc-vizio-inscape-services-llc.
[18]FTC to Ramp up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions, https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap-consumers-subscriptions
[19] California Civil Code 1798.140 (h)
[20] California Civil Code 1798.185 (a)(20)(C)
[21] California Privacy Protection Agency, Text of Proposed Regulations, Section 2004. https://cppa.ca.gov/meetings/materials/20220608_item3.pdf
22 Neil M. Richards, Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 Wash. U. L. Rev. 961 (2021). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3642217
23 2021 年データケア法（Data Care Act）を参照： https://www.congress.gov/bill/117th-congress/senate-bill/919. マサチューセッツ州も忠実義務を基にしたプライバシー法を提案している： https://malegislature.gov/Bills/192/HD2664.

消費者が実際に同意の通知とどのように接しているのかをほとんどまたはまったく考慮していない同意に基づいた規制モデルの失敗を是正する試みを表している。

2.1 執行

上述のとおり、FTC は一般的な消費者プライバシーの主な執行機関であり、セクトラルなプライバシー法については各分野の機関がその管轄範囲内で責任を持つ。FTC の主な執行ツールは同意判決と呼ばれ、これは米国の刑事における有罪答弁の行政法版に似たものである。同意判決では、FTC が一定期間にわたり企業のビジネス慣行に様々な条件を課している（例えば、対象企業が特定の方法によりデータを収集または処理することを控える、など）。企業は一般的にこれらの合意において罪または責任を認めないが、FTC が同意判決に違反したという結論に至れば、FTC は追加の罰金を課し、さらには合意の期間も延長できる。委員会は同意判決の前に非公式の調査を実施し企業との相談を行い、不正行為の証拠が十分にある場合に正式に苦情を申し立てることもある。苦情のほとんどは解決され、同意判決という結果に至っている。[24]

州レベルでは CPPA が公布した規制の執行が 2023 年 7 月 1 日に開始されたが、最近の裁判所の判決がその日付を 2024 年 3 月 29 日まで延期させている。しかし、司法長官事務所（OAG）は既に発効している CCPA や CPRA の古い規定を執行している。[25] OAG による執行は FTC と同様の方法で運用されており、ほとんどの苦情が規定合意（stipulated agreement）と呼ばれる和解方法により解決している。一部の都市や自治体では独自のプライバシー関連の立法や執行に取り組んでいるが、[26] それらの取り組みは本レポートの範疇を超えるものである。

2.2 司法手続き

上述のとおり、政府によるプライバシーの執行による司法判断は稀である。プライバシー関連の私的訴訟も珍しいが、発生することがある。連邦レベルでもプライバシー法がいくつか制定されているものの、これらは私的訴権を許可していない。[27] 私的訴訟を許可している法律の場合でも、本稿の紙面に収まりきらないほどのニュアンスが含められているため、[28] 本レポートでは全体的な課題に言及する。この種の訴訟における主要な障害物の一つが、多くのウェブサービスやプラットフォームによる利用規約が私的仲裁を優先して訴訟を禁止していることが多い点である。これは個別の訴訟だけでなく、集団訴訟も阻害している。さらに、プライバシー関連の訴訟事件における損害は、個人がなりすましの被害やその他の金銭的損失に遭ったデータ漏洩などの状況以外では、証明することが極めて難しい。
州レベルでの訴訟の場合はすべての州や領土が独自の民事訴訟手続きの規則やコモン・ローの法体系を制定しているため、さらに複雑である。さらに、本稿を執筆する時点では九つの州が独自の包括的な消費者プライバシー法を成立させており、それぞれ私的訴訟の扱い方が異なっている。サミュエル・ワラントとルイス・ブランダイスが 1890 年に初めて列挙したコモン・ローのプライバシー侵害 [29] は州法において広く認められているが、これらの請求では勝訴が困難であり、デジタル時代においてプライバシーを保護するための効果的な措置としては一般的に見なされていない。

---

24 Daniel J. Solove, Woodrow Hartog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 610 (2014). https://cyberlaw.stanford.edu/sites/default/files/SSRN-id2312913.pdf.
25 OAG はより広範に CCPA 執行行為（https://oag.ca.gov/privacy/ccpa/enforcement）と私的執行行為（https://oag.ca.gov/privacy/privacy-enforcement-actions）のリストを別々に維持している。
26 Ira Rubinstein, *Privacy Localism*, 93 Wash. L. Rev. 1961 (2018).
27 連邦の最も「強力」なプライバシー法の一つである HIPAA では、違反に対する私的訴権を提供していない。
28 例を一つ挙げると、一部の連邦訴訟は、通常は政府によるスパイ行為やデータへのアクセスに対処するものである通信傍受法（Wiretap Act）と通信記録保管法（Stored Communications Act）に基づいた訴因を提起している。
29 Samuel D. Warren, Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

CCPA／CPRA はデータセキュリティ侵害の法的損害賠償とともに私的訴権を創設しているが、[30] 同法律における他の規定については創設していない。執行は OAG 次第である。また、診療記録プライバシー法などといったカリフォルニア州の他のプライバシー法も私的訴訟を可能にしている。

※本研究は、JST【ムーンショット型研究開発事業】グラント番号
【JPMJMS2293】の支援を受けたものです。

[30] California Civil Code 1798.150