KGRI
Keio University Global Research Institute

KGRI Working Papers

No.7

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

Version3.0

2025 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）

　　: Alexander Frammersberger　（パッサウ大学）

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　　（慶應義塾大学 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

※各原稿の原文は 2024 年 3 月までに提出されたものである。

＜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
訳・荒川稜子（慶應義塾大学 KGRI 客員所員）

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の憲法上の位置づけ

欧州におけるデータ保護法は、個人が自己に関する個人データを管理すべきであるという仮説に基づいている。こうした個人データの管理は、多くの場合「情報自己決定（informational self-determination）」[1]と呼ばれ、EU 基本権憲章８条における個人データの保護という基本権を理論的根拠としている。これは自己に関するどの情報を、誰に対して、どのような目的のために開示するかを明らかにする個人の権利に関連すると理解されており[2]、EU 法には適用されない概念であるデータプライバシーの自己管理とは異なる。こうした独自の方針は、監督を伴う分権化された執行構造を通じて権利の広範な官僚化を支え、プライバシーに関する世界的に最も重要な分断の一つを生み出した。米国法もある程度こうした考えへと移行している（例えば、現在米国内では７つの州がデータプライバシー法を制定した[3]）が、結局は EU 的価値観のアンチテーゼとなる価値観を支持し続けている。

個人データの保護の権利は、EU 機能条約 16 条および EU 基本権憲章８条に定められていることから、EU 法における一次法であり、国家レベルおよび EU レベルの広域な施行制度を必要とする[4]。各加盟国にはデータ保護法の適用を監視するデータ保護機関（以下、DPA）が設けられ、データ保護法違反に対する異議や、広範囲に及ぶ適用されうる手続きや救済措置を扱う。その概要は以下の通りである。

基本権憲章 52 条（３）は、基本権憲章と欧州人権条約の両文書にそれぞれ対応する権利が含まれている限り、基本権憲章に定められている権利の意味と範囲は、欧州人権条約に定められているものと同様であると規定している。しかしながら、この規定は EU 法がより広範な保護を与えることを妨げるものではなく、EU 法はプライバシーに関して特筆に値する独自の理解を発展させてきた。欧州人権裁判所は、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が追加で必要であるとしているが、この点において、EU 法は欧州人権条約と概念的にも実質的にも密接に結びついているものの、より広範囲の権利を自律的に付与していると言える。

（２）個人情報保護法の憲法上の意義

一般データ保護規則（以下、GDPR）１条（２）によれば、「本規則は、自然人の基本的な権利及び自由、並びに、特に、自然人の個人データの保護の権利を保護する」ことを目的としており、また基本権憲章８条は個人データの保護を規定している。EU 法において基本権憲章はリスボン条約以降、拘束力のある権利の源泉となっており、これはデータ保護の権利への言及も含む。基本権憲章は欧州人権条約の

[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, accessed 30 June 2023.
[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/, accessed 26 June 2023.
[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 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? (Springer 2009) https://link.springer.com/book/10.1007/978-1-4020-9498-9#toc.

影響を強く受けており、欧州人権条約はEU法の基礎として重要な法源となっている。これは、現在も存続している条約が、EU加盟国に対して欧州人権条約への批准を定めていることによる。また、欧州司法裁判所は、欧州のデータ保護法の発展に影響を与えるにあたり、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概要

（１）他国の法制度による影響

OECDや欧州評議会など、いくつかの世界的および国際的な機関が初のプライバシー条約を締結したことは広く知られているが、欧州各国はプライバシーに関する規則を早期の段階で採択したことで特別な地位にあるといえる。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制定さ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、欧州評議会は個人データの自動処理に係る個人の保護に関する条約第108号を採択し、世界初のデータ保護条約としてEU法に影響を与えた。ここでは他国がEU法に与えた影響を辿るのではなく、GDPRとして具体化されたプライバシーに関する世界基準を通じて、EUが他国の基準に影響を与えようとしている点に留意することが重要であるといえるだろう[6]。

（２）「個人データ（個人情報）」の定義と範囲

一般的にCookie規制として知られるePrivacy指令は2002年に成立し、2009年に改正され、2018年にGDPRの発効と同時にePrivacy規則として成立することが期待されていたが、現在も採択に至っていない。2021年に提案されたePrivacy規則では、Cookie（ユーザーのブラウザー由来のID識別子）の使用に関して、より厳格な規制の導入が試みられた。GDPRにおいて、Cookie IDは個人データと見なされる。Cookieに関する法律は、EU離脱後の英国がGDPRにおける特定の重要な保護措置の削除を検討する際の、広域な根拠の基盤となっている。

（３）データ主体の権利と個人データ処理者（data processor）の義務

個人は、例えば、データ処理の目的を達成するためのデータが不要となった場合、データ管理者（data controller）に自身のデータの削除を要求することができる。2014年、欧州司法裁判所は画期的な判決とされるGoogle Spain判決（Case C-131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317）にて、いわゆる「忘れられる権利（right to be forgotten）」を規定し、この権利は現在GDPRの17条に明記されている。Google対CNIL判決（Case C-507/17, *Google LCC v. CNIL*, ECLI:EU:C:2019:772）において、欧州司法裁判所は忘れられる権利の地理的適用範囲（territorial scope）を明示することが求められ、EU圏外における検索結果のアクセス防止、もしくは少なくとも深刻に阻止する手段に関連したEU全域で参照されない（de-referencing）一般規則が確立された。この概念は世界的に普及し、こうした

[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] 例えば、2017 Communication from the European Commission, 'Exchanging and Protecting Personal Data in a Globalised World' COM 2017 7 final.

判例はEU法を象徴とみなされているが、その履行、検索エンジンの透明性、そして公的人物に関して多くの議論が引き起こされている[7]。

b）個人情報保護法における同意の位置付け（オプトイン方式かオプトアウト方式か）

法律によって明示的に許可されている場合、またはデータ主体（data subject）が処理に同意した場合を除いて、個人データの処理は一般的に禁止されている。同意は、個人データ処理においてよく知られた法的根拠である一方で、実際にはGDPRに言及されている６つの根拠のうちの一つに過ぎない。GDPR６条（１）には、その他の根拠として、契約の履行、法的義務、データ主体の生命に関する利益、公共の利益、そして正当な利益が明記されている。法的に有効な同意の要件はGDPR７条に定義されており、前文32でさらに定義されている。同意は自由に与えられ、特定され、事前に説明を受け、不明瞭ではないものでなければならず、自由に与えられた同意を得るためには、その同意が自発的に与えられたものでなくてはならない。Planet49判決（Case C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH*, ECLI:EU:C:2019:801）では、欧州司法裁判所はGDPR６条（１）について、同意は明らかに肯定的な行為（clear affirmative act）によって与えられなければならないと判示しており、こうしたEU法における権利中心型の見解は重要であるといえる[8]。

c）＜通知＝同意＞モデルの限界とその対策

上述の通り、同意はGDPRの運用における中心的な原則である。その個人主義と人間中心的なプライバシーの適用がGDPRの運用を支配しており、これはソロブが概説している原則のアンチテーゼであるともいえる。

d）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

PDSは複雑な部類のテクノロジーの代表であり、GDPR上の責任に対して多くの興味深い不確実性を提起している。特別な種類の個人データの処理は、例外が適用されない限りGDPR９条（１）によって禁止されており、ここでの例外とは、商業的な文脈においては一般的に明確な同意が与えられた場合を指す[9]。職務的もしくは商業的な活動と関連性がない「自然人によって純粋に私的な行為又は家庭内の行為の過程において行われる場合」は「私的な又は家庭内の行為に対する例外（personal and household exemption）」にあたるため、そのデータ処理にGDPRは適用されないが、この例外は狭義に解釈される。

もっとも、プラットフォームは自らの意図に基づきユーザーのデータを処理することで商業的な目的を追求することができるため、PDSはGDPRにおける課題を提起している。PDSは同意志向であり、ユーザーの同意を適切に取得するための補助手段を提供する可能性があるといえるだろう[10]。全体として、

---

[7] 以下を参照。 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), https://doi.org/10.1093/oso/9780198868422.003.0006, accessed 22 May 2023.

[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.

[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). Available at: https://policyreview.info/articles/analysis/personal-data-ordering-context-interaction-meso-level-data-governance-regimes [Accessed: 22 May. 2023].

PDS と GDPR は、個人データの処理に対してさらなる透明性とコントロールをもたらし、個々のユーザーに権限を与えることを目指している点で類似しているといえる。

e）プロファイリングに対して異議を述べる権利（GDPR21 条）といったプロファイリングに対する規制

GDPR22 条に基づき、データ主体は法的もしくは重要な影響を及ぼすプロファイリングを含む、もっぱら自動化された取扱いに基づいた決定の対象とされない権利を有する。２項に規定された条件に則り、自動化された意志決定が例外的に認められた場合、データ管理者は、データ主体に対し、人間の関与を得る権利、データ主体の見解を表明する権利及びその決定を争う権利の保護を確保するための適切な措置の実装が求められる（GDPR22 条（３））。

プロファイリングとは、「自然人と関連する一定の個人的側面を評価するための、特に、当該自然人の 業務遂行能力、経済状態、健康、個人的嗜好、興味関心、信頼性、行動、位置及び移動に関する側面を分析又は予測するための、個人データの利用によって構成される、あらゆる形式の、個人データの自動的な取扱い」を意味する（データ保護法執行指令３条（４）、GDPR４条（４））。そのため、プロファイリングはそれ自体が自動的な意志決定の一形態である。GDPR21 条は、データ主体に対し、自己の特別な状況と関連する根拠に基づき、第６条第１項（e）又は（f）に基づいて行われる自己と関係する個人データの取扱いに対し、それらの条項に基づくプロファイリングを含め、いつでも、異議を述べる権利を規定している。

EU のデータ保護法は、体系的または個別的な予防的警察活動（predictive policing）アプリケーションの使用が法律で規定されている場合、その使用を禁止しない。しかしながら、さまざまな規定や条件によってその法律の確実性を損ない、有用性をさらに制限する可能性がある[11]。

f） GDPR20 条などでデータ・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？

GDPR20 条はデータ・ポータビリティ権を規定しているが、この権利の行使に関しては依然として明確化が必要であるとされている。これは、この権利を狭義に解釈した場合、個人への利益が限られる一方で、広義の解釈をした場合、データ管理者にとって懸念となりうるからである。その定義が明確化されていないにも関わらず、オンライン評価といった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は GDRP20 条の対象外となる可能性がある。これは GDPR20 条の文言がデータ・ポータビリティ権の範囲を大幅に制限しているためと言われている。

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に対してのみ適用されることから、事業者は GDPR20 条の権利を行使することができない。GDPR20 条におけるデータ・ポータビリティ権は、その曖昧さや他のデータ主体の権利や自由といった内在的な限界によって、意図した結果を出すことができないおそれがある。データ・ポータビリティ権は、市場参入の促進や、高額な切り替え費用の抑制、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といった点で、多くの影響をもたらす[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）

GDPR75 条以降は、文献レビューで概説している通り、GDPR における監督の仕組み、権限、手続きに関して広範に規定されている。Budapesti Elektromos Művek 判決（Case C-132/21, *Budapesti Elektromos*

[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, accessed 30 June 2023.
[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.

Mūvek, ECLI:EU:C:2023:2）において、欧州司法裁判所は法的救済に関する GDPR の条項の、一貫して均質な（consistent and homogeneous）適用を保証することは加盟国に委ねられているとしつつ、基本権憲章 47 条を違反しないことを保証するなどの保護措置を提供しなければならないとしている。

また、GDPR80 条に基づき、公共の利益に属する制定法上の目的をもち、かつ、データ主体の権利及び自由の保護の分野において活動する非営利の組織、団体又は協会は、DPA に対してデータ主体の代わりに異議を申立てること、司法救済の権利、並びに、データ主体の代わりに賠償金を受ける権利を行使することができる。欧州司法裁判所は近年、GDPR80 条（２）に基づき、消費者保護団体が GDPR 違反に対する訴訟手続きを取ることは、国内法によって認められる可能性があると判示している。（Case C-319/20, *Meta Platforms Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände*, ECLI:EU:C:2022:32）

オーストリアポスト訴訟（Case C-300/21, *UI v Österreichische Post AG*, ECLI:EU: C:2022:756）において、GDPR82 条違反による無形の損害（non-material damages）の性質に関する予備的問題（preliminary questions）についての意見書が法務官によって提出された。特に、侵害の結果データ主体が感じる可能性のある単なる動揺は、無形の損害への賠償には含まれないものと法務官は結論付けている。

GDPR83 条（５）および（６）によれば、深刻な GDPR の侵害によって課される罰金の上限は 2000 万€もしくは事業者の直近の会計年度における全世界での売上額の４パーセントのどちらか高額な方であり、これは 2023 年に下された非常に重要な決定である[13]。

（５） 司法的救済の仕組み（訴訟要件、集団訴訟の可能性）

GDPR 前文 143 で概説されている通り、GDPR78 条以降の規定によって非常に幅広い司法的救済が適用される点について、本稿でも概説する。GDPR における監督機関は、GDPR に基づいた個人の権利の侵害に対する異議を検討し、また効果的な罰則のために管理者や処理者に対して非常に上限が高額な罰金という形態で罰則を課すための権力が委任されている。結果として、こうした機関は任期が定められ、早期解任に対する法的保証があり、調査と決定が委ねられた事項について完全な管轄権を有する、独立機関として加盟国によって設立されなければならない。

データ保護監督機関は EU 法における「法廷（tribunals）」としての要件を満たさないため、彼らによる決定は GDPR78 条に則り裁判所による司法審査を受けなければならない。77 条から 79 条にかけての目的は、国内法のもとで存在する可能性のあるいかなるその他の救済に関係なく、国内法において効果的に達成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）

78 条（１）は、国内法のもと、監督機関による法的拘束力のある決定を不服として裁判所に控訴する機会の設置が義務付けられている。また、78 条（２）では、異議を申し立てられた監督機関の不作為に対する司法救済を得る権利が定められている[14]。

当該問題について判決を下すにあたり必要であると判断した国内裁判所は、欧州司法裁判所に対し、この規則を含む EU 法の解釈に関する予備的判決を下すよう要求することが可能であり、または、EU 機能条約 267 条に規定されている場合には、こうした要求をしなければならない[15]。国内裁判所は理事会

[13] 以下を参照。 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’ https://edpb.europa.eu/system/files/2023-05/final_for_issue_ov_transfers_decision_12-05-23.pdf.

[14] 事実、欧州司法裁判所は、監督機関はそうした異議を「十分な注意を払って」調査する義務があると強調している。詳しくは以下を参照。Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650, para 5.

[15] Case C-645/19, *Facebook Ireland Ltd and Others v Gegevensbeschermingsautoriteit*, ECLI:EU:C:2021:483.

の決定を無効と宣言する権限を有していないが、決定を無効とみなす場合、欧州司法裁判所の解釈に則って EU 機能条約 267 条に従い、有効性の問題を欧州司法裁判所に付託しなければならない。

（５）司法的救済の仕組み（訴訟要件、集団訴訟の可能性）

GDPR が注目を集める主な理由として、EU 競争法に着想を得たとされる新しい制裁措置にあると考えられる。EU データ保護条例（DPD）が違反への制裁を加盟国に委ねていたのに対し、GDPR では「効果的であり、比例的であり、かつ、抑止力のある処罰」を義務付けており、行政罰が事業者の全世界における年間売上額の最大４パーセントに及ぶ可能性があると規定している。

前述のとおり、GDPR80 条に基づき、公共の利益に属する制定法上の目的をもち、かつ、データ主体の権利及び自由の保護の分野において活動する非営利の組織、団体又は協会は、DPA に対してデータ主体の代わりに異議を申立てること、司法救済の権利、並びに、データ主体の代わりに賠償金を受ける権利を行使することができる。

（６）研究を目的とした診療データの二次利用

a）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。

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り、それぞれの要素は利害のバランスが含まれている。研究者が被験者と直接連絡を取ることのできる単独の研究では、セキュリティやデータの最小化基準（例えば、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、そして保管すること）が明確でなくてはならず、データ主体はプロジェクトの全体が通知され、データ主体の権利が尊重されていなければならない。より複雑なデータ共有の手順は、GDPR を通しての交渉がより難しいと言われている（例えば、当初の同意が新しい処理に対して有効かどうかなど）[16]。

データガバナンス法（DGA）と GDPR を併せた、欧州保健データスペース（以下、EHDS）に関する規則の提案は、EU における保健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、EU におけるデータの単一市場の創出や、保健を含むいくつかの戦略的分野で共通の欧州データスペースを確立し、データが経済や社会で活用できるようになることを目的としつつ、管理下にあるデータを生成している個人を保護している[18]。依然として、

---

[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> (accessed 1 July 2023).

[18]また、デジタルサービス法（DSA）に基づき、オンラインプラットフォームとオンライン検索エンジンは、その設計、機能、使用が、公衆衛生、未成年者の保護、および個人の心身の健康への重大な悪影響に及ぼすリスクを評価しなければならない。デジタル市場法

EU のデータ保護法における、あるいはデータ保護法の欠如による、これらの問題は権利中心型の性質を有しているがゆえに、多くの議論を引き起こしている[19]。

議論の大部分は意思決定のプライバシーに関するものであり、個人による有効な選択とみなされるためには、その選択がどれほどの情報に基づいて行われなければならないかという点を巡って、例えば多くの最先端の生物医学研究の方法論などで、重大かつ複雑な議論がされている[20]。EHDS 以前は、GDPR 7 条（３）によってデータ主体は自己の同意をいつでも撤回する権利が与えられているにも関わらず、それに関連するデータ管理者の義務は明示されていなかった。EHDS は、科学以外を目的とした保健データの二次利用も正当な理由として追加しており、これには開発及び革新の活動、アルゴリズムや AI プロジェクト、個別化医療のアプリケーションなどが含まれる（EHDS34 条（１）（f）及び（g））。GDPR からさらに規則が発展した EHDS は、保健データの二次利用に関する条項を定め、「社会の一般的な利益」への貢献を目指している。34 条では、二次利用のために処理できる目的として、アルゴリズムの訓練、試験及び評価が挙げられている。他の条項では、例えば、科学的研究、公衆衛生、保健・健康分野に関する統計、教育活動、そして個別化医療の提供といった目的が挙げられている。個人または社会全体にとって悪影響を及ぼす、又は有害な活動のための二次利用は禁止されている。

b）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？

保健データアクセス機関（以下、HDABs）は、データ許可証（data permit）を発行することで保健データの二次利用へのアクセスを許可し、これは例えば、欧州 AI 法に基づく保健分野における AI システムの開発、訓練、試験及び評価の支援などに利用される[21]。全 DPA に対する調査とプライバシー関連の組織の専門家へのインタビューによって構成された、30 ヶ国（EU 加盟国 27 ヶ国と欧州自由貿易連合及び欧州経済地域の加盟国 3 ヶ国）で実施された実証実験によれば、アクセスの権利の対象となりうるさまざまな種類の潜在的に「有意義な情報（meaningful information）」と、データ主体への影響に関する複数の種類の情報が評価されたものの、実際にはこうした種類の情報の多くはほとんど提供されていないか、まったく提供されていなかったことが明らかになっている[22]。

c）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、データ主体は自己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

（DMA）において、欧州委員会は公衆衛生を理由にゲートキーパーに例外を認め、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/>(accessed 1 July 2023).

[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] 以下を参照。 Teodora Lalova Spinks, ‘People Have the Power: Patient empowerment in the European Health Data Space proposal (Part I)’ 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 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/> (accessed 1 July 2023).

[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.

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 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で個人データを受け取る権利と、その個人データの提供を受けた管理者から妨げられることなく、別の管理者に対し、それらの個人データを移行する権利があることが明記されている。EHDS では、３条（８）にてデータ・ポータビリティ権が定められている[23]。これは患者が複数の医療提供者の間で公的または民間の管理者によって処理された自己の一次保健データを交換し、アクセスを提供することを可能にするための、保健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）（iv））[24]。「電子保健データ（electronic health data）」の定義と前文 12 によれば、GDPR と異なり、EHDS における一次データ・ポータビリティは推定データ（inferred data）も対象としている。

欧州司法裁判所は 2023 年 1 月 12 日の RW v Österreichische Post 訴訟[25]にて、GDPR15 条（１）（c）はデータ主体が要求した場合、管理者に対して個人データの取得者の具体的な身分を開示することを義務付けているが、データ主体のかかる要求が明らかに根拠のない、または過剰である場合、取得者のカテゴリに関する情報のみで十分であると判示している。2023 年には、ニコラス・エミリウ法務官が FT v DW 訴訟（Case C-307/22）の意見書において、GDPR12 条（５）と 15 条（３）は、データ主体がデータ保護とは無関係な目的のために複製物を要求している場合の手続きも、データ主体がデータ管理者に対して自己の個人データの複製物の提供を要求していると解釈しなければならないとしている[26]。この訴訟では、医療過誤を疑った歯科医院の患者が、訴訟に備えて歯科医院が所有する彼に関するすべての医療記録の複製物を無償で提供するよう歯科医院に要求していた。

※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ある。

[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 (accessed 1 July 2023).
[24] See Teodora Lalova Spinks, ‘People Have the Power: Patient empowerment in the European Health Data Space proposal (Part I)’ 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).
[25] Case C-154/21, *RW v Österreichische Post*, ECLI:EU:C:2023:3.
[26] Case C-307/22, *FT v DW,* ECLI:EU:C:2023:315.

Ⅱ．ドイツ

ドイツにおける個人データ保護法についてのレポート

Meinhard Schröder＝Alexander Frammersberger
(パッサウ大学)
訳・新井貴大（新潟県立大学）

1. 憲法と個人データ保護法との関係

①プライバシー権ないし情報自己決定権の憲法上の地位

「プライバシーの権利ないし情報的自己決定の権利（例えば、個人データの取扱いにおける自己決定権や情報自己決定権）は憲法上の権利として保障されているか？　仮に保障されている場合、プライバシーの権利は情報的自己決定の権利とは異なるものと解釈されているか？」

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」として引き合いに出される[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とは、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、各人に個人性が〔守られるために〕退避する空間を保障する。すなわち、各人は「私事に関して放っておかれる」[9]権利、〔肖像権や氏名権のような〕「自分で自分

---

[1] おそらく別の見解に立つものとして、*Kube*, in: HStR VII, § 148 Rn. 108.

[2] 同様の保障は、とりわけ歴史的解釈から生じる――ヘレンキームゼー草案の２条の文言は次のようになっていた。「何人も、法秩序及び善良の風俗という制限の範囲内で、他者に危害を加えない限りのあらゆることを行う自由を有する。」参照、JbÖffR, NF Bd. 1 S. 55――ほか、制限の規律が広いことを考慮した体系的解釈からも生じる。

[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] 民事の判例に関連して、BVerfGE 34, 269 (278); すでにエルフェス判決では、基本法２条１項が基本法１条と結びつけられていた。BVerfGE 6, 32 (41)を参照。

[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; 早くにそう述べていたものとして、*Dürig*, JR 1952, 259 (261)も参照。

[9] *Starck*, in: v. Mangoldt/Klein/Starck, GG, 7. Aufl. 2018, Art. 2 Abs. 1 Rn. 85.

を所有する」[10]権利を有する。この権利は、ある程度までは、匿名を求める権利も含んでいる[11]。レーバッハ判決において、連邦憲法裁判所はこのことを明確に表現している。すなわち、「何人も、自分の生活像全体または生活における特定の出来事を、はたして他者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、原則として、自ら単独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、情報自己決定権を展開させた[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」決定[15]、「離婚文書」決定[16]、「医療記録」決定[17]、「レーバッハ」判決[18]および「依存症患者相談所」決定[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契機として、情報的自己決定という形で人格権から特殊な形態を導出し、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に入れた[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、一般的人格権の本来的な形態として、憲法上の地位も有する。しかし、一般的人格権からの派生であることと、それに伴う特有の保護方向のゆえに、憲法上で明示的に記述されてはいない。

c）異同

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、それらの異同よりも、特殊性について述べなければならない。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人性を発展させ、保持する」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

---

[10] *Arndt*, NJW 1967, 1845 (1846).

[11] これにつき参照、*Neumann-Duesberg*, Juristen-Jahrbuch VII, S. 138. 次の文献も参照、*v. Mutius*, Anonymität als Element des allgemeinen Persönlichkeitsrechts – terminologische, rechtssystematische und normstrukturelle Grundfragen, in: Bäumler/v. Mutius, Anonymität im Internet, 2003, S. 12 ff. さらに参照、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; これについては *Jarass*, in: Jarass/Pieroth, GG, 17. Aufl. 2022, Art. 2 Rn. 40 も参照。

[22] BVerfGE 141, 186-220, Rn. 32; BVerfGE 35, 202 (220); BVerfGE 79, 256 (268); BVerfGE 90, 263 (270); BVerfGE 117, 202 (225).

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。原則として、個人関連データの処理からの保護も、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。つまりこれによって、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、一般的人格権から具現化された独立の形態として理解されるべきであり、データ処理に関する特別な要求ないしそれに伴う危険に適応するよう彫琢されたものである。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、当事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 個人データ保護法の憲法上の意義

「プライバシー権や情報自己決定権が何らかの意味で憲法上保護されている場合、かかる権利は、個人データ保護法の指導原理として定義ないし規定されているのか？　換言すれば、個人データ保護法は、プライバシー権などの憲法的価値ないし規範を実現する法令として位置づけられているのか？」

DSGVO〔Datenschutz-Grundverordnung：EU 一般データ保護規則。以下、英語での略称である「GDPR」に統一する〕1 条 2 項は、GDPR の目標が、自然人の基本権を保護することであると明示的に定めている。その代表的なものは、個人関連データの保護を求める権利である。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]。

---

[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.); 基本法 10 条か基本法 13 条かの境界に関して、例えば、*Starck*, in: Mangoldt/Klein/Starck, GG, 7. Aufl. 2018, Art. 2 Abs. 1 Rn. 92 を参照。

[25] BVerfGE 80, 367 (375).

[26] BVerfGE 47, 46 (73 f.).

[27] 例えば、自動車番号の自動読取りに関して、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.

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]。〔個人データの処理と〕関連する憲法上の地位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することを試みており、データが取得される場合でも、諸利益にかなった方法でのデータの取扱いを保障している。つまりこの限りにおいて、データ保護に関する諸原則により、データ対象者の基本権保護は最大化される。

憲法は、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が、この観点からすると、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。ここで、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 2.③(b)も参照）、まさに公的機関によるデータ処理の場合、自由意思に基づいていない可能性があるため、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 2.③(c)も参照）。

2. 個人データ保護法の概要

① 他国の法制度の影響

「個人データ保護法を制定するにあたり、モデルとして参照した国はあるか？」

ドイツの連邦諸州は、現代的な自動データ処理に対する法的規律の必要性を、世界で初めて認識した。例えば、1970 年 9 月 30 日に、ヘッセン州データ保護法によって、データ保護法の世界的な礎石が築かれた[34]。それに続いて、ラインラント・プファルツ州も 1974 年に州のデータ保護法を制定したが、この法律は、技術上のデータ安全に加えて、初めて個人の利益も含めて考慮した[35]。このような足跡の下、1977 年に「データ処理における個人関連データの濫用から保護するための連邦法」が成立した[36]。この法律により、現行の規律と同様、データ保護は、データの表示形式にかかわりなく「あらゆる個人関連データ」に及ぶようになった[37]。このように、データ保護法の発展の大部分はドイツに起源をもつものであり、それゆえ、基本理念において、当初は他国の考え方に基づくものではなかった。国内のデータ保護法は、時の経過とともにデータ保護法の欧州化が進展したことにより、決定的な影響を受けた。このため、まずはデータ保護指令（95/46/EC）を国内法として実施しなければならなかった。そこから 20 年以上の時を経て、この指令は GDPR に取って代わられた。GDPR は、もはや指令としてではなく、今度は規則としての立法化がなされたことによって、国内のデータ保護法にとっても第一次的な準拠点を構成している（EU 運営条約 288 条を参照）。そのため、国内的な規律は後景に追いやられ、規則でカバーされていない分野、ないしは開放条項によって、独自の立法の余地がある分野を規律するのみである。さらに、管見の限りで

---

[31] その他の関連する基本権に関して、*Buchner*, in: Kühling/Buchner, 3. Aufl. 2020, Art. 1 Rn. 13 f.

[32] この点につき例えば、*Wolff*, in: BeckOK Datenschutzrecht, Stand 01.11.2021, Einl. Rn. 6 ff. を参照。

[33] BVerfGE 65, 1 (42).

[34] GVBl. I 1970 S. 625.

[35] GVBl. I 1974 S. 31.

[36] GVBl. I 1977 S. 201.

[37] これに関して参照、*Wolff/Brink*, in: BeckOK Datenschutzrecht, Stand 01.02.2022, Einleitung zur DSGVO Rn. 5.

は、GDPR は他のデータ保護法の考慮に基づいていない。逆に、基本権に基づくモデルであることをいくぶん強調して言い表される GDPR は、中国やアメリカの規律とは対比的である[38]。

②「個人データ」の定義と範囲

「クッキーや他のオンライン識別子は個人データ保護法における個人データに含まれるか？　個人データ保護法における個人データの定義とは何か？」

a）個人データ保護法における個人データの定義

GDPR の 4 条 1 号によれば、個人関連データとは、識別された、または識別可能な自然人に関連するあらゆる情報を意味する。すなわち、識別可能な自然人とは、とりわけ、名前などの識別子、識別番号、位置データ、オンライン上の ID、または、その自然人の身体的、生理的、遺伝的、精神的、経済的、文化的または社会的なアイデンティティの現れとしての一または複数の特別な特徴への割り当てによって、直接的または間接的に、識別されうるものをいう。刑事司法指令と、それを国内実施する BDSG46 条における〔個人関連データの〕定義は同一である。

GDPR4 条 1 号の法的定義には、いわゆる「事実上の匿名」[39]の場合もかなり含まれている。これはすなわち、必ずしも個人を識別することを意図していないが、（少なくとも事後的に）個人を識別することができる場合のことである。すなわち、この点で、GDPR もリスクベースのアプローチに従っている。しかし、情報と個人との結びつきの確立を可能とするための手助けとなる「追加知識」を、識別可能性の問題においてどの程度考慮すべきかは、議論のあるところである。文献上の（少数）意見は、「絶対的な個人関連性」説に従い、概して、識別に必要な追加知識がどこかに存在すれば十分であるとする[40]。しかしこれでは、GDPR の考慮理由〔前文〕26 の第 5 文が、データ保護法の対象とならない匿名情報も存在することを明らかに前提としているのに、ほぼすべてのデータが個人との関連性を示すことになってしまうため、説得力に欠ける。まさに（広い意味での）「鍵」の所有者と〔その他の〕大多数の人々を区別するという仮名化と暗号化の目的に対しても、疑問の目が向けられることになってしまうだろう。それゆえ、大方の判例は、データ処理に責任を持つ者がいかなる可能性を有していたかということに照準を合わせている[41]。したがって、これらの判例は、まさに、〔データ処理の〕管理者（Verantwortliche）が、個人関連性を確立できる状況にあるか否かに焦点を合わせるという、相対的な個人関連性の説に従っている[42]。この考え方からすれば、同じデータが、ある人については個人関連性を示しうるが、別の人については逆に個人関連性を示し得ないということになる。これは、まさに GDPR でも認められている仮名化と暗号化の目標を踏まえると、説得的なものである。欧州のデータ保護法の解釈に最終的な権限を有する EU 司法裁判所も、動的 IP アドレスの個人関連性が問題となったブライヤー事件において、（傾向としては）この見解に同調している。すなわち、たしかに EU 司法裁判所は、データ対象者を確定するために第三者の追加知識を（客観的に）使用できる場合には、そうした追加知識を考慮に含めたものの[43]、データ対象者の

---

[38] *Kühling/Raab*, in: Kühling/Buchner, DSGVO, 3. Aufl. 2020, Einl. Rn. 1.

[39] *Hornung/Wagner*, CR 2019, 565, Rn. 7; GDPR の考慮理由〔前文〕26 も参照。

[40] この学説については、特に、*v. Lewinski/Rüpke/Eckhardt*, DaSR, 2. Aufl. 2022, § 10 Rn. 30 を参照。

[41] これについては例えば、BGH GRUR 2015, 192 (194).

[42] この学説につき、ここでは *v. Lewinski/Rüpke/Eckhardt*, DaSR, 2. Aufl. 2022, § 10 Rn. 30 を挙げておく。相対的な〔個人関連性の〕学説については、例えば、*Brauneck*, EuZW 2019, 680 (683 f.); *Karg,* in: Simitis/Hornung/Spiecker, gen. Döhmann (Hrsg.), Datenschutzrecht, 1. Aufl. 2019, Art. 4 Nr. 1 DSGVO Rn. 64. 今のところこうした相対的な個人関連性〔の学説〕をはっきりと採用するものとして、EuGH, Urt. v. 26.4.2023 - T-557/20 (SRB/EDSB), ECLI:EU:T:2023:219, Rn. 97 ff.

[43] EuGH, C-582/14, ECLI:EU:C:2016:779 – Breyer, Rn. 43.

識別が法律で禁止されているか、または現実的に実行不可能であり、したがって識別リスクが事実上無視できる場合には、EU 司法裁判所は識別可能性を否定し[44]、それに伴い、個別事例に関連した、ある程度まで主観的な（その場合は具体的な管理者に関連している）要素を付け加えた[45]。

b） クッキーやその他のオンライン識別子は、個人データ保護法における個人データのなかに含まれるか？

通常の場合、クッキー上のデータレコードから、個人を帰納的に推論することはできない。しかし、クッキーが設置される前または後に、本人がその他の識別特徴を追加した場合、クッキー上のデータレコードは、ユーザーの識別特徴に紐づけることができ、したがって、個人関連データを構成する[46]。

動的 IP アドレスを個人関連データとして分類するのも、同様に評価することができる。原則として、どの IP アドレスが、いつ、どのユーザーに割り当てられたかは、各ユーザーのインターネットプロバイダのみが知っている。 したがって、プロバイダにとって、動的 IP アドレスは常に個人関連データである[47]。それ以外のすべての当事者にとって、動的 IP アドレスが個人データになるのは、他の情報と組み合わせて個人を識別できる場合に限られる[48]。

電子メールアドレスに含まれる実名のように、明らかな識別特徴の場合、個人関連データとして分類されることに問題はない[49]。

③ データ対象者の権利および個人データ処理者の義務

a） 個人データの削除権（e.g.， GDPR 17 条）または利用停止請求権

個人関連データの削除に関する規律は、データ対象者の利益を満たすように形成された、データ保護法の中心的要素の一つである。GDPR17 条 1 項には、管理者に対するデータ削除の義務づけと、データ対象者が自己に関する個人関連データの遅滞なき削除を管理者に対して要求する権利との両方が含まれている。

この削除は――GDPR17 条 3 項において〔他の利益との〕衡量が必要とされる場合があるという例外を別にして――GDPR17 条 1 項で限定列挙された理由のいずれかに該当する場合に、実施されなければならない。すなわち、目的達成のための必要性の欠如（a）、〔データ処理の根拠としての〕同意の撤回およびその他の法的根拠の欠如（b）、データ対象者による異議（c）、データの違法な処理（d）、法的義務の履行（e）、児童に対する情報社会サービスとの関係での〔データ〕取得（f）。例外の場合の衡量については、EU 司法裁判所[50]とドイツの裁判所[51]に若干の判例がある。

削除権は、GDPR17 条の見出しでは「忘れられる権利」とも呼ばれている。しかし、GDPR17 条 2 項は、

---

[44] EuGH, C-582/14, ECLI:EU:C:2016:779 – Breyer, Rn. 46.

[45] その全体に関する最近の文献として参照、*Schröder*, DVBl. 2023, 794 (796).

[46] これにつき参照、EuGH, Urt. v. 01.10.2019, C 673/17, ECLI:EU:C:2019:801 – Planet 49; *Klar/Kühling*, in: Kühling/Buchner, DSGVO, 3. Aufl. 2020, Art. 4 Rn. 36.

[47] EuGH Urt. v. 24.11.2011 – C-70/10, ECLI:EU:C:2011:771 Rn. 51 – Scarlet Extended; *Klar/Kühling*, in: Kühling/Buchner, DSGVO, 3. Aufl. 2020, Art. 4 Rn. 35.

[48] ウェブサイト運営者に関する個人関連性は、この運営者が、インターネットアクセスプロバイダにデータを要求する法的手段を有する場合に限られる。参照、EuGH (2. Kammer), Urteil vom 19.10.2016 – C-582/14 (Breyer/Deutschland).

[49] *Klar/Kühling*, in: Kühling/Buchner, DSGVO, 3. Aufl. 2020, Art. 4 Rn. 39.

[50] 基礎的なものとして、EuGH, Urteil vom 13.5.2014, C-131/12 – Google und Google Spain; EuGH, Urteil vom 8.12.2022 – C-460/20 (TU).

[51] BVerfGE 152, 216 Rn. 141; BGH, NJW 2020, 1595; BGH, NJW 2020, 3444.

この点に技術的な問題があることに注意を促している。すなわち、完全な忘却は、データ処理に関わる自然人の記憶だけでなく、データの公開によっても妨げられることがある（「インターネットは何も忘れない」）。管理者が個人関連データを公にし、GDPR の 17 条 1 項に従って削除義務を負う場合、その管理者は、GDPR17 条 2 項により、そのデータを処理している管理者に対して情報提供を行う義務がある。その目標は、特に検索エンジンでデータがヒットしないようにすることである（「検索結果からの削除（De-Listing）」）。公開されたデータを回収することはできないため、削除権、したがって同時に、忘れられる権利は、法的な限界のみならず、事実上の限界にも突き当たる[52]。この点で、個人関連データが公開されている場合、削除権はなまくらな剣になり果てる。データが公開されておらず、個別の第三者にのみ送信された場合は、GDPR19 条が適用される。

データ対象者は、削除権のほかに、GDPR18 条に基づき、処理制限を求める権利も有する。ここでは、データについて削除が求められているわけではないが、これ以上別に処理されてはならないことが意図されている（「凍結」）。制限の対象となるデータファイルには、GDPR4 条 3 号〔「『処理制限』とは、データの将来的な処理を制限する目的で、保存された個人関連データに印をつけることをいう。〕の意味における印を付けなければならない。削除よりも控えめである処理制限が関連する場合とは、例えば、削除がデータ対象者の利益と対立する場合（〔18 条〕1 項 b、c）や、削除請求の検討に一定の時間を要する場合（〔18 条〕1 項 a、d）である[53]。

b）個人データ保護法における同意の位置づけと意義（オプトインかオプトアウトか？）
個人データ保護法において、本人の同意が必要となるのはどのような場合か？　事業者が個人データを取得する際に、本人（データ対象者）の同意を得る必要があるか？　個人データを第三者に提供する場合、本人の同意を得ることは必要か？

aa）同意の意義

同意の意義とは、自由意思に基づき、特定の事案に関して、情報を与えられ、かつ不明瞭ではないかたちで、データ対象者によって発された意思表示と定義され、この意思表示は、データ対象者が、自身を対象とする個人関連データの処理を了承していることを示す表明の形式またはそれを認める他の明確な行為の形式で行われる（GDPR4 条 11 号）。GDPR において、この定義よりも重要なものはないであろう[54]。GDPR6 条 1 項 1 号に基づく適法なデータ処理の許可要件としての同意は、データ処理を許可するための中心的な作用メカニズムであるだけでなく、同時に、個人関連データを「はたして」処理することが許されるか、そして「どのように」処理することが許されるか、ということの決定可能性を通じて、データ対象者の情報的自己決定を実定的に表すものでもある[55]。さらに、同意はデータ対象者の基本権的地位の確保を顧慮するだけでなく、特定性と明示性に関する広範な要求にも基づき[56]、データ処理者に必要な法的安定性を保障する。

GDPR4 条 11 号に従い、同意は（それが GDPR9 条 2 項にいうセンシティブデータでない限りで）明示的のみならず黙示的にも行われうる。ただし、黙示的な行動も、能動的な行いによってなされなければなら

---

[52] 例えば、次の文献も参照、*Dix*, in: Simitis/Hornung/Spiecker, gen. Döhmann (Hrsg.), Datenschutzrecht, 1. Aufl. 2019, Art. 17 Rn. 21. 検索結果からの削除の領域的な射程に関して参照、EuGH, 24.9.2019 – C-507/17, BeckRS 2019, 22051.

[53] 例えば、*Herbst*, in: Kühling/Buchner, 3. Aufl. 2020, Art. 18 Rn. 1.

[54] アルプレヒトも「データ保護の決定的な支柱」として、同様の評価を下している。参照、*Albrecht*, CR 2016, 88 (91).

[55] *Roßnagel/Pfitzmann/Garstka*, DuD 2001, 253 (258); *Buchner/Petri*, in: Kühling/Buchner, DSGVO, 3. Aufl. 2020, Art. 6 Rn. 17.

[56] *Buchner/Petri*, in: Kühling/Buchner, DSGVO, 3. Aufl. 2020, Art. 6 Rn. 18 f.

ない（かつ、同意に向けられたものでなければならない）[57]。このことから、データ対象者はウェブサイトを開く際に「オプトイン表明」のかたちで個人関連データ（特にクッキー）の処理について能動的に同意を与えなければならない[58]という結論が導かれる。この同意は――GDPR が施行される前の法的状況とは異なり[59]――、単なる無為（非オプトアウト）では、もはや十分ではない。この背景には、EU 司法裁判所の判例によれば､同意の要求が単に見落とされたという可能性を排除しえないということがある[60]。この限りではないかもしれないのは、例えば、催し事での写真撮影について知らされた後も、誰かがその場にとどまり続けるような事例である。センシティブデータを処理する場合、GDPR9 条 2 項 a は、明示的な同意を命じている。

bb）個人データ保護法のもとで本人の同意が必要とされるのはどのような場合か？

GDPR6 条 1 項 1 文の体系に従い、同意は、個人関連データの適法な処理のための複数の許可要件の一つである。すなわち、原則として、個人関連データの処理が、データ対象者との契約の履行のため（GDPR6 条 1 項 1 文 b 前段)、またはデータ対象者の求めに応じて契約前の措置の実施のために必要である場合（同 b 後段）か、または、法的義務の履行（同 c)、生命にとって重要な利益の保護（同 d)、任務の遂行に資する場合（同 e）か、または、管理者や第三者の優越する利益のためである場合（同 f）には、いずれにせよ同意が必要である。体系的な描写に反して、一部では[61]、GDPR6 条 1 項 1 文 a に基づく同意は、それがより緩やかな手段であるため[62]、前述の許可要件よりも優先される[63]と考えるものもいる。

cc）事業者が個人データを取得する際、本人（データ対象者）の同意を得る必要があるか？

上述したように、GDPR6 条 1 項の他の許可要件のいずれかを満たしている場合、事業者が個人関連データを取得するのに、データ対象者の合意は必ずしも必要ではない。事業者がデータ処理を行う場合、通常は、GDPR6 条 1 項 1 文 b の許可要件が問題となる。また、インターネット上で誰でも自由にアクセス可能なデータを処理する場合など、状況によっては GDPR6 条 1 項 1 文 f も関係する場合がある。

一部で主張されている同意の包括的優先に関する見解や、契約前の措置を実施する場合などの証拠のために、念のために同意を得ることが推奨されることもあるが、これに問題がないとはいえない。というのも、同意は、GDPR7 条 3 項に従っていつでも撤回することができ、その場合は、処理に関する別の法的根拠が必要となるためである。

dd）個人データを第三者に提供する場合、本人の同意を得る必要があるか？

個々のデータ処理過程ごとに法的根拠が必要である。これは、データを提供する者にも、受領者にも、データ処理のための法的根拠が必要であることを意味する。この点で、「二重扉モデル」[64]とも呼ばれ、データ送信にも、受領および追加的処理にも法的根拠が必要であることを指す。原則として、同意はその両方に関連しうる。ただし、同意は「特定の事案」（4 条 11 号）ごとにのみ行われることに注意しなけれ

---

[57] EuGH, Urt. v. 01.10.2019, C 673/17, ECLI:EU:C:2019:801 – Planet 49, Rn. 52.

[58] GDPR の考慮理由〔前文〕32; EuGH, Urt. v. 01.10.2019, C 673/17, ECLI:EU:C:2019:801 – Planet 49, Rn. 54 ff.

[59] 例えば、BGH, NJW 2010, 864 を参照。

[60] EuGH, Urt. v. 01.10.2019, C 673/17, ECLI:EU:C:2019:801 – Planet 49, Rn. 55.

[61] このため、包括的な優先があると考えないものもある。参照、*Buchner/Kühling*, in: Kühling/Buchner, DSGVO, 3. Aufl. 2020, Art. 7 Rn. 16; *Schulz*, in: Gola/Heckmann, DSGVO, 3. Aufl. 2022, Art. 6 Rn. 10.

[62] Vgl. *Schantz*, in: Simitis/Hornung/Spiecker, gen. Döhmann (Hrsg.), Datenschutzrecht, 1. Aufl. 2019, Art. 6 Rn. 11.

[63] はっきりとそのように述べるものとして、*Roßnagel/Pfitzmann/Garstka*, DuD 2001, 253 (258).

[64] BVerfGE 141, 220 Rn. 305.

ばならない。これには対象となる個人関連データ（4 条 1 号）だけでなく、管理者（4 条 7 号）およびその他のデータを受領しうる者（4 条 9 号）も含まれる。すなわち、データ対象者が第三者への提供および第三者による処理に明示的に同意する場合、再度の同意は必要ない[65]。逆に、第三者への提供などは、通常は黙示的同意の対象とはならない[66]。また、第三者へのデータ提供について法律で定められている場合にも、同意は必要ない（GDPR6 条 1 項 c）。この例が、個人関連データの開示を官庁によって命じられた場合などである[67]。また、GDPR6 条 1 項 b の場合にも、〔第三者提供に〕同意が不要となりうる。というのも、この規範は、同意の点で、データ対象者の契約相手方について、何ら言及していないためである〔つまり、契約相手方が必ずしも管理者である必要はない〕。GDPR6 条 1 項 b の文言に加えて、GDPR49 条 1 項 b との体系的な比較からも、この帰結は自然である[68]。最後に、提供には、GDPR6 条 1 項 f の正当な利益も存在する可能性がある。ここでも、法的根拠はすべての処理過程ごとに関連していなければならないことに注意を払う必要がある。

c）通知と同意モデルの限界およびその対策

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。「〔アメリカのプライバシー法は〕人々に自身のデータがどのように管理されるか決定できるようにする一連の権利を提供する。これらの権利は主に、個人データの収集、使用および開示に関する通知、アクセスおよび同意の権利から成る。この一群の権利の目的は、人々が自身の個人データをコントロールできるようにすることである。……経験的・社会的な科学研究が示すように、認知の問題は、個人データの収集、使用および開示に同意することのコストと利益について、情報を与えられた上で合理的な選択を行う個人の能力を損なう。」

それゆえ、人間の認知能力の限界という観点から自己管理モデルに限界があるとすれば、あなたの国の個人データ保護法は、どのようにこれらの課題に対処しているのだろうか？　例えば、企業には効果的な通知が要求されているのだろうか？

ドイツでの理解によれば、情報的自己決定は、段階的な形態で実現される。すなわち、最上ないし最良の段階は、データ処理に対する同意である。この場合、第三者がデータを処理してよいか否かを「自分で決定する」ことになる。この形態の自己決定は、データ処理が別の根拠に基づいている場合は後景に退き、それどころか、〔データの〕処理がデータ対象者の意思に反して実施される際には、無視されることさえある。このような場合、自己決定の別の側面がより重要になる。すなわち、各人は、自身について誰がどのような機会に何を知っているのかをわかっていなければならない[69]。

この理念は GDPR でも実現されている。GDPR14 条、15 条とあわせて、GDPR13 条で規定されている通知義務は、個人関連データの公正かつ透明な処理のための基礎となる（参照、GDPR5 条 1 項 a：透明性）。これをすでに GDPR13 条 2 項が表現している。通知義務の目標は、データ処理過程についてデータ対象者に知らせることであり、そのほかに、〔処理に〕関連する他の意図や法的効果についてデータ対象者に教示することも目標としている[70]。GDPR13 条以下に規定されている通知義務は、GDPR12 条により、基本的な枠組み規定が置かれている。例えば、通知は、正確で、透明性があり、理解しやすく、かつ容易にアクセ

---

[65] これにつき参照、*Klement*, in: Simitis/Hornung/Spiecker, gen. Döhmann (Hrsg.), Datenschutzrecht, 1. Aufl. 2019 Art. 7 Rn. 68.

[66] *Frenzel*, in: Paal/Pauly, DSGVO, 3. Aufl. 2021, Art. 6 Rn. 11.

[67] この点およびこうした見解への反対意見に関して、*Buchner/Petri*, in: Kühling/Buchner, DSGVO, 3. Aufl. 2020, Art. 6 Rn. 78.

[68] これについては、*Schantz*, in: Simitis/Hornung/Spiecker, gen. Döhmann (Hrsg.), Datenschutzrecht, 1. Aufl. 2019, Art. 6 Rn. 22.

[69] BVerfGE 65, 1 Rn. 146.

[70] *Paal/Hennemann*, in: Paal/Pauly, DSGVO, 3. Aufl. 2021, Art. 13 Rn. 4.

スできる形態で、明確かつ平易な言葉により伝達されなければならない。したがって、少なくとも理論的には、データ対象者は、誰がどのデータをどのような目的で保有しているのかについて、可能な限り平易かつアクセスしやすい方法で、その概要を入手する。この情報提供に加えて、データ対象者は、GDPR13 条 2 項に従って、特に削除および異議を申し立てる権利などについても教示される。少なくとも理論的には、通知義務に、開示請求権、削除権および同意の撤回権が組み合わされることで、データ対象者にとって十分な程度の透明性と権利保護の可能性が実現される。GDPR13 条に従った告知義務は任意ではないにせよ、GDPR23 条、85 条および 88 条の開放条項による制限だけは免れない[71]。

通知義務の最大の弱点は、データ対象者側の専門技術的理解の欠如、および／または単純な関心の欠如である。GDPR13 条、14 条に従って伝えられるべき情報は、通常は非常に広範囲に及ぶため[72]、多くのデータ対象者はそれに必要な時間を費やすことを望まないか、あるいは費やすことができず、そのために低いデータ保護の水準に甘んじてしまう[73]。 それとは逆に、多くのデータ対象者は、データ保護の水準が適切であるか強い懸念を抱いている。この文脈では、しばしば「プライバシーのパラドックス」[74]が語られる。前述の GDPR12 条に加え、GDPR7 条 2 項もこの問題に対処しようとしている。この規定では、同意は原則として複雑な契約全体の一部ではあるが、他の定めとの対比において、同意が後景に退けられてはならないことが定められている。したがって、同意は容易に理解でき、他の定めと区別できなければならない[75]。とはいえ、これによって、データ対象者にとっての認知的な荷重負担という事実上の問題[76]が左右されるわけではないであろう。それでも、GDPR12 条 7 項は、例えば、情報の理解を容易にするためのピクトグラムについて定めることで、情報的自己決定を改善しようとしている。それにもかかわらず、現行のデータ保護法は、この問題を満足に解決できていない。こうした状況に応じて、文献には、改正についての最初の提案が見うけられる[77]。

以上に加えて、透明性の義務づけには、それを貫徹する上である種の弱点がある。通知義務に違反した場合、GDPR83 条 5 項 b に基づき、制裁金による制裁が科されうることは事実である。しかし、それ以上に、通知義務が〔それに反した行為が無効とはなるわけではない〕秩序規定なのか、データ処理の適法性の要件なのかは明らかでない[78]。GDPR13 条に違反しても、〔データ〕処理全体がひとまとめに違法になることはないとの解釈が有力である[79]。それによれば、特に、同意の場面で事前に提供されるべき情報と、データ取得の枠内で提供されるべき情報とは、別に考慮される[80]。しかし、同意の要求が通知とともになされる場合、誤りは同意の無効につながりうる。この点で、通知義務違反がデータ処理の違法性とは無関係である可能性があることは、通知義務に与えられた保護効果も弱めている[81]。

---

[71] *Schmidt-Wudy*, in: BeckOK Datenschutz, Stand 01.05.2023, Art. 13, 任意性については Rn. 33、開放条項については Rn. 8 f.

[72] これに関して包括的に述べたものとして、*Ebner*, Weniger ist Mehr?, S. 104 ff.

[73] そのように述べるものとして、*Ebner*, Weniger ist Mehr?, S. 44; *Pollmann/Kipker*, DuD 2016, 378.

[74] これにつき例えば、*Specht*, in: Specht/Mantz (Hrsg.), 2019 § 9 Rn. 6.

[75] *Klement*, in: Simitis/Hornung/Spiecker, gen. Döhmann (Hrsg.), Datenschutzrecht, 1. Aufl. 2019, Art. 7 Rn. 75.

[76] これについては、*Van Ooijen/Vrabec*, Journal of Consumer Policy 2019, 91 (95).

[77] ひとつの提案を提示するものとして、*Ebner*, Weniger ist Mehr?, S. 314 ff. を参照。

[78] *Bäcker*, in: Kühling/Buchner, DSGVO, Art. 12 Rn. 13, 18, 27, Art. 13 RN. 61 ff., 80 ff.; *Schantz*, in: Schantz/Wolff, DatenschutzR, 2017, Rn. 1176; *Paal/Hennemann*, in: Paal/Pauly, DSGVO, 3. Aufl. 2021, Art. 13 Rn. 9a.

[79] *Paal/Hennemann*, in: Paal/Pauly, DSGVO, 3. Aufl. 2021, Art. 13 Rn. 9a およびそこで掲げられている文献を参照。

[80] そのような見解として *Heckmann/Paschke*, in: Ehmann/Selmayr, DSGVO, 2. Aufl. 2018, Art. 12 Rn. 5; 異なる見解として、*Bäcker*, in: Kühling/Buchner, DSGVO, 3. Aufl. 2020, Art. 13 Rn. 66.

[81] これについては、*Bäcker*, in: Kühling/Buchner, DSGVO, 3. Aufl. 2020, Art. 13 Rn. 61 ff.; 同様のものとして、*Dix*, in: Simitis/Hornung/Spiecker, gen. Döhmann (Hrsg.), Datenschutzrecht, 1. Aufl. 2019, Art. 13 Rn. 26.

d）個人データの本人による管理可能性を支援するために、Personal Data Store（PDS）のような仕組みやアーキテクチャはどのように活用されているか？

クッキーの不用意な受け入れ（「クッキークリック疲れ」）を避けるために、ドイツの立法者は、電気通信・テレメディアデータ保護法（TTDSG）26 条 2 項 3 号 b において、個人管理情報システム（Personal Management Information Systems：PIMS）に関する規律を初めて成立させた。これは、事前に設定されたシステムが質問画面に自動的に記入することによって、ユーザーがクッキーバナーにかかわることなく、ウェブサイトを開くことができるようにすることを意図している[82]。しかし、質問への記入が標準化されているため、データ対象者が処理目的ごとに個別に同意していない限りで、同意に必要な目的決定に問題があると見なされるかもしれない。ただし、これと似た代理の場合においては、以上のことは必ずしも当てはまらない。これについては GDPR8 条を参照されたい。

以上のように、PIMS のようなシステムは国内のデータ保護規律の中に入ってきているが、そうしたシステムによって、欧州のデータ保護法の要求が満たされるか、そしてどのように満たされるかは、まだ明らかではない。

e）プロファイリング規制。例：プロファイリングに異議を述べる権利（GDPR21 条）。

GDPR は、その 4 条 4 号によれば、「プロファイリング」という用語の広義の理解に基づいている。これは、個人関連データに対する、あらゆる種類の自動処理と解される。この処理は、自然人に関する人格の特定の側面を評価するため、とりわけ、その自然人の仕事能率、経済状況、健康、個人的嗜好、興味関心、信頼性、行動、居所または転居に関する側面を分析あるいは予想するために、そうした個人関連データが利用されることから構成されている。すなわち、プロファイリングとは特別なデータ処理のことである。GDPR は、特に 2 つの規定でこうした種類のデータ処理に言及している。つまり、21 条における異議申立権および 22 条における自動化された決定に対する要求である。

GDPR21 条は、GDPR6 条 1 項 e または f に基づくデータ処理に対する異議申立権を規定している。通常の場合、これにはデータ対象者の特別な状況から生ずる理由があることが前提となる（〔21 条〕1 項 1 文）。ダイレクトマーケティングの場合は、そうした理由がなくても、つまり無条件で、異議申立てが可能である（〔21 条〕2 項）。両項とも、異議申立権がプロファイリングにも適用されることを明示している。もっとも、こうした明示は宣言的な記述にすぎない。というのも、そうした付記がなくてもプロファイリングは GDPR21 条の適用対象になると思われるからである[83]。本来的には余分な記述であるが、これはおそらく、プロファイリングのような、人格権が非常に鋭く反応する事案に異議申立権を拡張することを明確化したものと解されよう[84]。

GDPR22 条はさらに重要である。22 条 1 項でデータ対象者に認められているのは、自動化された処理だけに基づく決定に服さない権利である。こうした決定は、データ対象者に向けた法的効果を発揮するか、または類似の方法でデータ対象者に著しい干渉を及ぼす。その際、この規定では、自動化された決定に至る過程の最も重要な事例[85]として、プロファイリングを明示的に強調している。プロファイリングの例としてよく知られているのは、例えば融資の際に使用されるスコアリング方式である。この規定の目標は、法的に重大な意味のある決定が、自動化された処理プロセスに依拠するだけでなく、人間による個別の

---

[82] これについては、*Kühling/Sauerborn*, ZD 2022, S. 596 f.

[83] 枚挙にいとまがないが、ここでは、*Caspar*, in: Simitis/Hornung/Spiecker, gen. Döhmann (Hrsg.), Datenschutzrecht, 1. Aufl. 2019, Art. 21 Rn. 15 を挙げておく。

[84] *Martini*, in: Paal/Pauly, DSGVO, 3. Aufl. 2021, Art. 21 Rn. 17.

[85] こうした評価を共有するものとして、*Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 1. Aufl. 2019, Art. 22 Rn. 20.

管理段階へと導くことである[86]。すなわち、その結果として、データ対象者が個人データのアルゴリズムに基づく評価の単なる客体になることの阻止を意図している[87]。GDPR がプロファイリングの過程に相当な危険の可能性を想定していることは、データ保護影響評価の義務（GDPR35 条 1 項、3 項 a を参照）によっても裏づけられている。

もっとも、GDPR22 条 1 項による当初の厳格な規律は、GDPR22 条 2 項に定められた様々な例外の要件によって弱体化されている。一部の文献では、そうした〔GDPR22 条 1 項の〕規律が、GDPR22 条の文脈において、もはや個別の場合における自動化された決定の禁止を語りようがないほどに、GDPR22 条 2 項に規定された例外の要件は包括的であるとさえ解されている[88]。

f）データポータビリティの権利または個人データを移行する権利（例、GDPR20 条） また、これらの権利は実際にはどのような状況で行使されるのか？

GDPR20 条はデータポータビリティの権利を規定している。この規定では、データ対象者が管理者に提供した自己にかかわる個人関連データを、構造化され、一般に使用されており、かつ機械で読み取り可能なフォーマットで受領し、そうしたデータを別の管理者に提供する権利が、データ対象者に認められている。その唯一の要件は、〔データの〕処理が GDPR6 条 1 項 a か GDPR9 条 2 項 a に基づく同意、または GDPR6 条 1 項 b に基づく契約に基づくものであり、かつ処理が自動化されたやり方を用いて行われることである。この請求権によって、市場力と情報的自己決定とのバランスを取ろうとしている[89]。〔GDPR の〕考慮理由〔前文〕では、データポータビリティはプロバイダの変更を可能ないし容易にするものとされており、例として、あるソーシャルネットワークから別のソーシャルネットワークへの移行が挙げられている[90]。これに関して、文献では GDPR20 条の適用範囲がさまざまな広さで理解されており、例えば、大規模なデータ量のクラウドストレージプロバイダの変更も GDPR20 条 2 項の適用事例として挙げられている文献もある[91]。 結局のところ、最終的には別のプロバイダに移動することが容易になることを意図しており、つまりこの限りで、この規律には第一に競争政策的目標ないし一般消費者を保護する目標が与えられてしかるべきである[92]。

④ 個人データ保護法を執行する監督機関の組織と権限。制裁および異議申立ての仕組み

a）組織と権限

管理者に指名されたデータ保護受託者による「社内における」内的監査（GDPR37～39 条）に加え、独立した[93]データ保護監督官庁による外的監査がある。これはヘッセンデータ保護法以来のドイツのデータ保護法の伝統であり（公的機関の監督は公的機関自身では実施できなかった）、現在では EU 基本権憲章 8 条 2 項および EU 機能条約 16 条 2 項の両方で定められている。

---

[86] *Scholz*, in: Simitis/Hornung/Spiecker, gen. Döhmann (Hrsg.), Datenschutzrecht, 1. Aufl. 2019, Art. 22 Rn. 3.

[87] *Martini*, in: Paal/Pauly, DSGVO, 3. Aufl. 2021, Art. 22 Rn. 1.

[88] *Franzen*, in: Franzen/Gallner/Oetker, EuArbRK, 4. Aufl. 2022, Art. 22 Rn. 3.

[89] Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder v. 8./9.10.2014, in: BBDI, Dokumente zu Datenschutz und Informationsfreiheit 2014, S. 23 f.

[90] 考慮理由〔前文〕55。

[91] *Schantz*, NJW 2016, 1841 (1845).

[92] *Herbst*, in: Kühling/Buchner, DSGVO, 3. Aufl. 2020, Art. 20 Rn. 4; *Schantz*, NJW 2016, 1841 (1845); *Kühling/Martini*, EuZW 2016, 448 (450).

[93] これについては、EuGH, Urteil vom 9. März 2010, Rs. C-518/07 – Kommission/Deutschland.

欧州レベルでは、(EU の機関を）監督するのは欧州データ保護監察官によって担われており[94]、そのほかに、データ保護監督官庁の欧州行政連携において中心的な役割をもつ欧州データ保護委員会（Europäische Datenschutzausschuss: EDSA）がある（GDPR70 条 1 項 1 文、刑事司法指令 51 条)。しかし、監督については、――それが公的機関に対するものであれ、非公的機関に対するものであれ――まずは加盟国のデータ保護監督官庁が所管する（GDPR51 条を参照)。加盟国の監督官庁は、GDPR52 条に従い、その任務を遂行するにあたって完全な独立性を認められている。そのほかに、GDPR53 条は、監督官庁の構成員に対する手続法的および人的な要求も規定している。

ドイツ連邦共和国が連邦制をとっていることに基づき、行政活動の大部分は、連邦を構成するラント〔＝州〕において、またラントによって遂行されている。このことはデータ保護法にも表れている。連邦データ保護法（Bundesdatenschutzgesetz: BDSG）は、連邦の公的機関に対する監督を、主として「連邦データ保護・情報自由監察官」（Bundesbeauftragten für den Datenschutz und die Informationsfreiheit: BfDI）に割り当てている（連邦データ保護法 8 条以下)。州の公的機関、ならびに非公的機関（つまり企業、団体など）に対する監督については、連邦を構成する各ラントが責任を負う（ラントのデータ保護法と関連する連邦データ保護法 40 条)。裁判所、教会および宗教団体、ならびにメディアについては、分野固有の例外が存在する[95]。

これに応じて、外的な監査の大部分はラント官庁に委ねられている。必然的に、この分類にはある程度の不統一な運用が伴う。そうした運用の不統一性は、各ラントが GDPR や、個々の点に関して連邦法を執行するというだけでなく、ラント法上のデータ保護規律をも執行するという事情によって、増大している。その解毒剤として、(非公式の)「データ保護会議」(Datenschutzkonferenz: DSK）があり、ドイツのデータ保護官庁が、調整のうえで意見や行動勧告などを議決している。

それに比べると、連邦データ保護・情報自由監察官には比較的小さな任務範囲しか残っていない[96]。それにもかかわらず、連邦データ保護・情報自由監察官は欧州データ保護委員会の代表を務めている。これは、国内的な影響力が小さいという背景からすれば少なくとも疑問に思われるが、規律技術的には、また連邦制を背景とすれば、もっともなことである。

官庁の権限は GDPR55 条 1 項から明らかとなる。原則として、各官庁はその加盟国におけるデータ保護を所管する。GDPR の適用範囲と国境を越えた多くの事態にかんがみれば、これはしばしば幾重にも重なる権限をもたらすだろう。管理者は多数のデータ保護官庁に対応しなければならないであろうし、矛盾した決定が下される危険があるだろう。それゆえ、GDPR56 条は「ワンストップショップ」の原則を定めている――つまり、管理者がある加盟国に主たる営業所を持つ場合、その国の監督官庁が所管する権限をもつ。他の官庁の協力は、背景にある欧州行政連携の枠組みにおいて行われるが、必要に応じて、欧州データ保護委員会もいわゆる一貫性の機構（GDPR60 条、63 条以下）の中で関与する。

データ保護監督官庁の権能は、GDPR から直接に生じる（GDPR58 条)。

b）制裁と異議申立ての仕組み

GDPR に対して違反した場合の制裁として、GDPR 自体が制裁金のカタログを規定しており（GDPR83 条 3～6 項)、GDPR84 条では、それとは別の制裁の可能性に関して、加盟国に言及している。これに関して、

---

[94] 欧州データ保護監察官は、従来のデータ保護監察官と同様、まず第一に EU 行政および EU 機関の内部におけるデータ保護の遵守を監視することを所管する。規則（EG）45/2001 の 41 条 2 項を参照。EU 機関への助言（規則（EG）45/2001 の 46 条 d と結びついた 41 条 2 項）または異議申立ての対処（規則（EG）45/2001 の 46 条 a のような、その他の任務のほかに、欧州データ保護監察官は、欧州データ保護委員会の構成員でもある。GDPR68 条 3 項を参照。基本的な点について、v. Lewinski/Rüpke/Eckhardt, DaSR, 2. Aufl. 2022, S. 353 ff.

[95] 詳細は、*v. Lewinski/Rüpke/Eckhardt*, DaSR, 2. Aufl. 2022, S. 357 ff.

[96] この点につき例えば、*Heil*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, § 5.1 Rn. 45 ff.

GDPR83 条の制裁金の要件は、大きく 4 つのカテゴリーに分けられる。すなわち、1．管理者ないし処理者の義務違反〔83 条 4 項 a〕、2．認証および監視機関の義務違反〔83 条 4 項 b、c〕、3．具体的な処理の枠内における違反〔83 条 5 項 a～d〕、および 4．監督官庁〔の命令に対する違反および監督官庁の調査〕に対する妨害〔83 条 5 項 e、6 項〕である[97]。この場合には、2000 万ユーロ以下の制裁金、または企業の場合であれば、直前の会計年度に全世界で収めた年間総売上高の 4%以下の制裁金が科されうる。

前述の制裁には、国内的には連邦データ保護法 43 条の規定が並ぶが、この規定は GDPR84 条の意味における〔加盟国が定める別の制裁に関する〕規定ではないだろう[98]。この〔行政上の〕秩序違反は 5 万ユーロ以下の過料によって罰せられる。すなわち、額の大きさの点でも欧州の規律を下回っている。

この間に、データ保護会議も欧州データ保護委員会も、制裁金の額に関するガイドラインを議決した[99]。

GDPR77 条によれば、すべてのデータ対象者は、他の行政法上または裁判上の法的救済とは別に、監督官庁に異議を申し立てることを求める権利を有する。さらに、GDPR78 条に従い、すべての自然人または法人は、他の行政法的または裁判外の法的救済とは別に、自己に関して監督官庁が下す法的拘束力のある決定に対して、裁判上の実効的な法的救済を求める権利を有する。このことは、監督官庁が管理者または処理者に対して負担をかける措置を講ずる場合にも、監督官庁が GDPR77 条に基づく異議申立てに応じない場合にも妥当する。

⑤ 司法手続または司法救済（当事者適格。集団訴訟。）

GDPR79 条は、監督官庁による措置（GDPR77 条、78 条）を通じた（場合によっては裁判所により要求されることもある）データ対象者の保護を、直接に管理者および処理者に向けた法的救済によって補完するものである。原則として、データ保護法における権利保護ないし裁判権は、そのつど基礎となる法関係に依存する。そのため、例えば、公共の場でのビデオ監視に対する差止訴訟の場合、行政裁判所が管轄権を有する[100]。これに対して、データ対象者が私的な法人または自然人に対して個人データの削除を求める権利を主張する場合は、民事裁判権が管轄権を有する[101]。労働者データ保護の場合、労働裁判所法（ArbGG）2 条 1 項は、労働裁判所への出訴の途を認めており[102]、あるいは、社会データの処理が法的争訟の基礎となっている場合、社会裁判所法(SGG)51 条は社会裁判権へと移送する役割を果たしている[103]。

GDPR80 条 2 項により、加盟国は GDPR80 条 1 項にいう機関、組織または団体に、団体訴権を付与することができる。これは、たとえデータ対象者の関与なしに可能であっても、〔データの〕処理の結果として、データ対象者に生じる GDPR 上の侵害が関連していなければならない。現在のところ、連邦データ保護法の一部として、データ保護の団体訴権はない。ただし、消費者法ないし競争法と関連する差止訴訟法（UklaG）は、特定のデータ保護法上の事態に拡大された[104]。

---

[97] v. Lewinski/Rüpke/Eckhardt, DaSR, 2. Aufl. 2022, § 24 Rn. 25 ff.

[98] v. Lewinski/Rüpke/Eckhardt, DaSR, 2. Aufl. 2022, § 24 Rn. 36.

[99] Guidelines 04/2022 on the calculation of administrative fines under the GDPR (https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-calculation-administrative_en); Bußgeldkonzept der DSK (https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf).

[100] VG Regensburg, ZD 2020, 601.

[101] 例えば、OLG Bamberg, CR 2006, 274 f. を参照。

[102] BAG, CR 1987, 370.

[103] BSGE 130, 132.

[104] *v. Lewinski*, in: Auernhammer, DSGVO, 7. Aufl. 2020, Art. 80 Rn. 23.

〔GDPR〕82 条によれば、GDPR 違反のために、物的または精神的[105]損害を被ったいかなる者も、管理者または処理者に対して損害賠償を請求する権利をもつ。これも、加盟国の裁判所に提訴されなければならない。

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。

GDPR9 条 2 項ｇは、「遺伝データ、自然人を一意に識別することを目的とする生体データ［および］健康に関するデータ」は、「［そのようなデータの］処理が、追求される目的に対して比例的であり、データ保護の権利の本質を尊重し、そして、データ対象者の基本権と利益を保護するための適切かつ特定の措置を規定する EU 法または加盟国法に基づき、重要な公共の利益を理由として必要である」場合に、許可されると規定している。

この規定と研究目的での健康データの利用との関係について質問がある。

研究目的や医薬品開発のために患者の診療記録や生体データを利用する場合、患者の同意は必要となるか？　研究目的で患者の健康データを収集・利用する場合、研究機関は、同意のほかにどのような法的義務を負うのか？

また、欧州保健データスペース（European Health Data Space：EHDP）における最近の進展についても知りたい。

研究目的での健康データの利用に関する質問について、状況は以下の通りである。

まず、GDPR には研究目的のための「特権」が含まれていることに注意すべきである（89 条）。しかし、これは研究目的でのデータ処理が GDPR から免除されることを意味するわけではない。実際には、GDPR89 条 1 項から読み取れるように、GDPR は適用されるが、EU 法または加盟国法に従い、一部の権利が適用されないことがありうる（89 条 2 項）。

GDPR5 条 1 項ｂは、研究目的は他の目的と両立しないわけではないと定めている。この規定は GDPR6 条 4 項と関連しており、それに応じて、目的が〔当初の収集の目的と〕両立しないわけではないならば、当初の目的が修正される可能性がある。後者の規定の解釈については議論がある。すなわち、少数の学者は、目的の変更は他の前提条件なしに可能であると考えるが、管理者は依然として GDPR6 条 1 項に従った法的根拠を必要とするというのが、大多数の見解である。

健康データに関しては、GDPR9 条が適用され、その 1 項では、健康データの処理を（研究目的でのそれも同様に）禁止しているが、GDPR9 条 2 項には多数の例外が定められている。

研究目的や医薬品開発のために診療記録や生体データを利用する一つの方法は、同意であろう（〔9 条 2 項〕a)。私が質問をきちんと理解しているとすれば、あなたが知りたいのは、9 条 2 項の他の〔b～j の〕条項を、研究目的や医薬品開発のために、診療記録や生体データを処理するための根拠として使用できるか、特に〔9 条 2 項〕ｇ〔の条項〕について、同意がない場合にそうした処理の根拠として使用ができるか、ということである。

私の見解では、この点に関して 4 つの規定を考慮する必要がある。

---

[105] これに関する最新のものとして、EuGH, Urt. v. 4.5.2023, Rs. C-300/21 – Österreichische Post, ECLI:EU:C:2023:370.

質問にて言及があったように、GDPR9 条 2 項 g が適用される可能性がある。公共の利益とは、総人口または少なくともその大部分に影響が及ぶ利益を意味すると解される。これには例えば、伝染病の監視など人道的な目的のための処理が含まれる。公共の利益はテーマ的な特定を含むものではなく、コミュニティに奉仕するあらゆるものに及ぶ可能性がある。しかし、GDPR9 条 2 項 g は、それ自体は法的根拠ではなく、EU または加盟国の立法者が公共の利益とデータ保護の必要性との釣り合いをとるための授権である。ドイツでは、連邦データ保護法 22 条 1 項 1 号 d でこの授権を利用している。しかし、公共の利益にあたる場合を特定することなく、GDPR の文言を単にコピーしただけのこの規定が、GDPR に即したものであるかどうかは疑わしく、いずれにせよ、この規定が研究目的の健康データに適用できるとは考えられないであろう。

GDPR9 条 2 項 h は、少なくとも一応は関連しうる（予防医学または産業医学の目的……医学的診断）。これは各国の立法者への授権でもあり、ドイツは BDSG22 条 1 項 1 号 b でこれを利用している。しかし、研究目的では、GDPR9 条 2 項 j が特別法と考えられている。これについては下記を参照。

GDPR9 条 2 項 i が関連する可能性がある（「健康に対する国境を越えた重大な脅威から保護すること、又は健康管理及び医薬品若しくは医療機器について高水準の質と安全性を確保することのような、公衆衛生の分野における公共の利益の理由から必要となる」）。〔GDPR9 条 2 項〕g および h とは対照的に、GDPR9 条 2 項 i は、公衆衛生上の利益にはっきりと言及している。これは通常、データ対象者の同意がまったく得られない事例に関するものである。「公衆衛生」とは、規則（EC）No. 1338/2008 においてと同様に理解される。これによると、公衆衛生には、「病的状態や障害を含む健康状態、その健康状態に影響を及ぼす決定要因、健康管理の必要性、健康管理に割り当てられる資源、健康管理サービスの供給及びそれへのユニバーサルアクセス、並びに対応する支出と資金及び最終的には死亡の原因［……］のような、健康に関連するあらゆる要素」が含まれる。この点に関して、GDPR9 条 2 項 i は、公衆衛生への脅威を予防することを意図している。対照的に、GDPR9 条 2 項 h では、健康管理を考慮することが意図されている。ドイツは、連邦データ保護法 22 条 1 項 1 号 c でこれを利用している。

〔GDPR〕9 条 2 項 j は研究を扱っている。研究とは、前文の 159 に即して広義に理解される。「本規則の意味における科学的な研究目的での個人データの処理は、例えば、技術開発及び実証、基礎研究、応用研究及び民間資金による研究［……］のための処理を含むものと広義に理解されるべきである」。この非常に鷹揚な理解は、研究目的での処理に関する公共の利益の留保がないことによっても強調されている。ただし、〔GDPR〕9 条 2 項 j も、EU 法または加盟国法の規定によって実施される必要がある。

ドイツでは、連邦データ保護法 27 条が適用され、そこでは「規則（EU）2016/679 の 9 条 1 項の特例により、規則（EU）2016/679 の 9 条 1 項の意味における特別な種類の個人データの処理であっても、科学的若しくは歴史的な研究目的又は統計目的で、それらの目的のために処理が必要であり、処理に関する管理者の利益が、処理を実行させないことに関するデータ対象者の利益を著しく上回る場合には、同意がなくとも許可されるものとする。管理者は、〔連邦データ保護法〕22 条 2 項 2 文に従い、データ対象者の利益を保護するための適切かつ特定の措置を講じなければならない。

データ保護法ではよくあることだが、この規定では利益のバランスをとることが要求される。このため、多くの研究は、今でもボランティアに基づいている。

（同意以外の）研究機関の義務については、GDPR89 条がいくつかの指針を示している。一般に、研究

機関は他の管理者と同様に扱われ、GDPR が管理者に課すあらゆる義務を果たす必要がある。さらに、GDPR89 条 1 項に従い、処理は、データ対象者の権利と自由のための適切な保護措置の対象となる。GDPR89 条 1 項および 2 項によれば、これらの保護措置には、データ最小化の原則（GDPR5 条 1 項 c）の尊重を確保するための技術的および組織的措置が含まれていなければならない。これは例えば、収集するデータ量や処理範囲を目的に必要な程度に削減する、保存期間を設定する、そしてデータへのアクセス可能性を規制することによって達成される。データ最小化の要件（GDPR5 条 1 項 c）および保存制限の要件（GDPR5 条 1 項 e）は、GDPR89 条 1 項、3 項および 4 項の匿名化および仮名化に関する規定によって考慮されている。しかし、GDPR25 条 1 項の一般規定にかんがみると、GDPR89 条 1 項で追求されている研究目的でのデータ処理に関する最低基準の引き上げが実際になんらかの価値を付加するかどうかは疑わしい。同じことは連邦データ保護法 27 条 3 項についてもいえる。

最後に、欧州保健データスペース（EHDS）は欧州保健連合の一部であり、特定分野における初の EU 共通データスペースに当たる。目下の発展には、患者の概略記録のみならず、電子処方や電子管理が含まれており、それらは EU 各国で徐々に導入が進んでいる。

【訳者付記】

この翻訳では、原則としてドイツ語の語義に忠実となるよう訳したが、とりわけ GDPR 上の用語について、すでに英語からの定訳があるものについては、それを採用した（例えば、„Verantwortlicher“〔責任者〕には、対応する“controller”の定訳である「管理者」を当てた）。ただし、英語からの定訳がドイツ語と大きく距離を示す場合は、その限りでない（例えば、“data subject”の定訳は「データ主体」であるが、対応するドイツ語の„betroffene Person“ないし„Betroffene“は、あえて直訳すれば「影響を受ける者」「かかわりをもつ者」となる。被影響者、関係者、当事者、対象者、該当者、被害者などと訳しうるが、この翻訳では、さしあたりデータ対象者と訳した）。

翻訳中の〔　〕内は訳者による補足であり、[　] 内は原文の著者による補足である。原文のイタリックによる強調は圏点で示した。

なお、条文番号や文献の出典などに関し、明らかな誤りと思われる箇所について、訳者の判断で修正した箇所がある。

※本研究は、JST［ムーンショット R&D][助成金番号 JPMJMS2293]の支援を受けたものである。

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）
訳：佐藤太樹（慶應義塾大学大学院法学研究科後期博士課程）

1.憲法と個人情報保護法との関係性

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。

プライバシー権は、スイス連邦憲法 13 条１項（以下、「憲法」）により保護されている。同条項は、「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」と規定している。

情報自己決定権（the right to informational self-determination）は、憲法１３条２項により保障されている。憲法に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、「連邦最高裁」）は、この権利を認めている。憲法 13 条２項は、「すべての人は、個人データの濫用から保護される権利を有する」と規定している。そのため、情報自己決定権は、憲法 13 条１項に規定されている広義のプライバシー権の派生物なのである。特筆すべき点として、連邦最高裁によれば、憲法 13 条２項は、個人データの濫用からの保護を定めているだけでなく、情報自己決定権も保障していると広く解釈されていることが挙げられる。連邦最高裁は、憲法上の情報自己決定権は、「原則として、問題となっている情報が実際にどの程度の秘匿性を有しているかにかかわらず、連邦政府機関や民間人による個人データの取扱いに関して、すべての者が、当該データの取扱いの有無およびその利用目的を決定することができなければならない」旨を保障するものであると一貫して判示している（Decision of the FSC 147 I 280, consideration 7.1 を参照。原文の英文は、原文著者による翻訳。）したがって、連邦最高裁は、憲法 13 条２項には情報自己決定権が含まれていると判示すると同時に、同権利を非常に広義に解釈している。ただし、こうした見解は判例法理上、部分的に相対化されている。スイスの連邦機関は、合法性の原則に拘束されているため、個人データを取扱う法的根拠が存在する場合にのみ、当該データを取扱うことができる。連邦機関による個人データの取扱い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取扱いについてデータ主体に同意を要求する必要はない。その結果、データ主体は、連邦機関による個人データの取扱いについて決定する権利を持たない。結局のところ、連邦機関に関して言えば、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取扱いについては状況が異なる。一般に、民間団体は、透明性の原則、利用目的の制限および比例原則といったデータ保護の原則に準拠している場合に限り、個人データの取扱

いが認められている。GDPR とは対照的に、スイスのデータ保護法（DPA）では、個人データの取扱いを一般的に認めつつ、一定の場合につき取扱いを禁止している。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、同意を取得するほか、データの利用を優先すべき正当な利益がある旨を主張すること、またはそのような取扱いを許容する法的根拠を示すことによって、データの取扱い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。そのため、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個人データ保護法の憲法上の意義

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。

スイス連邦データ保護法（The Swiss Federal Act on Data Protection）（以下、「DPA」）は、スイスの連邦機関と私人（すなわち、企業）の双方に適用される。DPA の目的は、「個人データを取扱う際にその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の取扱いに関する具体的な要件が異なる。連邦機関とは異なり、一般的に私人は、基本権に拘束されない。ただし、基本権は、私人に対して第三者効を及ぼすことがある。特にデータ保護法の領域では、立法者は、民間団体の相互関係の中で情報自己決定権を考慮に入れた法律を制定する義務を負う。このことは、連邦機関と民間団体による個人データの取扱いを規制する DPA の各規定において実現されている。

2. 個人情報保護法の現状と課題

①他国における法制度の影響

個人データ保護法を制定するにあたってモデルとした国はあるか。

1992 年に制定された当初のスイス連邦データ保護法の起源を遡ると、同法のモデルとなった特定国への明示的な参照は行われていない。しかし、同法の立案は、ドイツ、フランス、およびオーストリアでのデータ保護法の制定後間もなく始まっていることから、スイスの DPA はこれらの国々の法律によって影響を受けていると考えて差し支えない。なお、スイス連邦最高裁は、ドイツ連邦憲法裁判所（以下、「連邦憲法裁判所」）の「国勢調査判決」を明示的に参照しており、前記判決において、ドイツの連邦憲法裁判所が導き出した情報自己決定権を承認している。

2023 年 9 月 1 日に発効した 2020 年 DPA は、EU 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」）により多大な影響を受けている。2020 年の DPA の改正は、スイスが、GDPR45 条の求める保護水準の十分性を認定された国家として今後も認められるよう、GDPR との調和を目指すものであった。さらに、同改正は、改正議定書の署名および批准を目指すべく、同議定書とスイス法との整合性を確保するものであった。

②「個人データ」の定義と範囲

クッキー情報及びその他のオンライン識別子は個人情報保護法における「個人データ」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」の定義。

スイスの DPA では個人データを GDPR と同様に定義し、「識別された自然人又は識別可能な自然人（「データ主体」）に関する情報」としている（DPA5 条（a））。GDPR の下では、管理者が、入手可能な（その他の）データと組み合わせることによって、特段の努力を要することなく当該個人が識別される場合、その個人は識別可能なものとみなされる。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。また、スイス電気通信法（以下、「TCA」）は、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の取扱いについては、利用者がその取扱いの有無や目的、さらに当該取扱いを拒否する権利について通知されている場合にのみ、当該データの取扱いが認められると規定している（TCA45c 条（b））。当該規定は、クッキーの使用にも適用される。

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

DPA32 条 2 項は、人格権の保護に関する行為は、スイス民法典（以下、「民法」）により規律されると規定している。特に、DPA32 条 2 項（c）は、請求権者が、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手段として設けられているため、データ主体がいつでも主張できる権利として解釈されていない。それゆえ、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保障されており、事案ごとに対抗利益を検討しなければならない。

【追加質問】：民法上の人格権に基づく個人データの削除請求は、如何なる場合に認められるか。

DPA はデータ主体の人格を保護することを目的としていることから、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関係がある。さらに、DPA は、DPA に違反した場合にデータ主体が採りうる救済手段について民法の規定を参照している。

DPA は民法の規定を直接参照しているため、削除請求の可否は民法のもとで定められる。加えて、DPA32 条 2 項（c）は、救済手段の一つとして削除権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）。データ主体に対する違法な人格侵害が発生した場合、民法による救済手段を行使することができる。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することができる（民法 28 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手段も行使できる。削除請求が認められるかどうかは、管轄の民事裁判所の判断による。当該請求は、違法な人格侵害が単に差し迫っているだけではなく現に発生しており、かつ、裁判所が判断する時点で当該侵害が継続している場合にのみ認められる。

b)個人情報保護法における同意の位置づけと意義、（オプトインかオプトアウトか） つまり、個人情報

保護法上、本人の同意が必要とされるのはどのような場合か。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。

GDPR の下では、個人データの取扱いは一般的に禁止されており、一定の場合に限り取扱いが認められている（GDPR6 条 1 項は、「取扱いは、以下の少なくとも一つが適用される場合においてのみ、その範囲内で、適法である」とする。）のに対して、スイスの DPA は、個人データの取扱いを一般的に認めたうえで、一定の場合につきその取扱いを禁止している。DPA30 条 1 項は、「個人データを取扱う者は、データ主体の人格を違法に侵害してはならない」と規定している。私人は、データ保護の原則に準拠している限り、個人データの取扱いが一般に認められる。例えば、個人データの取扱いは誠実に行われ、比例的であり、特定の目的のみに基づき収集されなければならない（利用目的の制限）。これらの原則に違反する形でデータが取扱われる場合、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 項（a））。そして、そのような侵害行為は、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法律により正当化される場合を除き、違法である（DPA31 条 1 項）。データ主体の利益を上回るデータ管理者の利益は、DPA31 条 2 項で例示されている。そのため、事業者は、例えば、契約の締結または履行に直接関連して契約当事者の個人データを処理する際に、対抗する私的利益を援用することができ（DPA31 条 2 項(a)）、その場合にはこれらのデータの取扱いについて同意を得る必要はない。個人データの取扱いが同意によって正当化される場合、それは自由意志に基づくものであって、具体的で、事前に説明を受けたうえでの、明確な同意に基づいて行われなければならない（article 5 (2) of the Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data 参照）。ただし、センシティブな個人データが取扱われる場合（この場合は明示の同意が必要である。DPA6 条 7 項(a)）を除き、一般に黙示の同意でも認められる。この点に関連し、個人データの取扱いに反対する明示的な意思表明が行われた場合、人格権の侵害が発生するとみなされるため(DPA 第 30 条 2 項(b)参照)、当該取扱いを正当化する必要が生ずる。したがって、一般的にオプトアウトの可能性が認められている。企業は、個人データを取得し、これを取扱う場合、データ主体から逐一同意を取得する必要はない。むしろ、他の方法、すなわち対抗する正当な利益を援用して個人データの取扱いを正当化することができる。スイス企業データ保護協会が 2022 年から 2023 年の冬に実施した（非公式な）調査によれば、調査に参加した 45 社による個人データの取扱いのうち、同意に基づくものは約 15%に過ぎなかった。残る 85%は、他の正当化根拠（すなわち対抗利益または法的根拠）に基づくか、データ保護原則に適合しているため一切の正当化を必要としないものであった。

個人データが第三者に提供される場合、同意は必要とされない。ただし、情報開示義務の一端として、データを取得する際に、個人データの受領者またはその一覧を公開しなければならない。

c)通知＝同意モデルの限界とその対策。

DPA の執行は、主に連邦データ保護・情報コミッショナー（以下「連邦データ保護・情報コミッショナー」または「コミッショナー」）によって行われ、同コミッショナーには調査に着手する権限が与えられている（後述）。このように、スイスの DPA は、専従の第三者機関に権限を委ねることで、「プライバシー

の自己管理モデル（privacy self-management model)」の限界に起因する諸課題に部分的に対応している。しかしながら、DPA は、データ主体による合理的選択を前提としている。したがって、DPA は上記の諸課題を十分に解決しているとは言えない。DPA は、同意が「自由意思に基づき、1 つまたは複数の特定のデータの取扱いについて、十分な情報提供を受けたうえで」行われた場合にのみ有効であると規定しているに過ぎない（DPA 第 6 条 6 項)。センシティブな個人データが取扱われる場合、私人によるプロファイリング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する場合、データ主体による明示的な同意が必須となる（DPA 第 6 条 7 項)。

d) 情報銀行や 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。

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。

DPA では、プロファイリングについて、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」であると見なされた場合、明示的な同意が与えられなければならない。（DPA6 条 7 項（b))。ただし、こうした規定は、同意が、対抗利益等による正当化の規律枠組み（上記参照）に関して求められる場合にのみ適用される。高リスクの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リスクを伴うプロファイリングであって、例えば、データの突合により、自然人の人格の根源的な部分を分析することを可能にしてしまうものを指す（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義務付けられている（DPA22 条 1 項)。

また、連邦機関が実施するプロファイリングについては、データ主体による明示的な同意が必要とされる（DPA6 条 7 項（c))。さらに、連邦機関がそのようなプロファイリングを行う場合、その法的根拠となりうる正式な法律が存在しなければならない（DPA34 条 2 項（b))。

f)データ・ポータビリティ権は保障されているか。

データ・ポータビリティ権は、2020 年の DPA 改正に伴い追加された。DPA28 条は GDPR に基づいており、GDPR20 条と軌を一にしている。DPA 第 28 条(1)によれば、個人データが自動化された方法で取扱われ、かつ当該取扱いがデータ主体の同意に基づいているか、またはデータ管理者とデータ主体間の契約の締結または履行に直接関係して個人データが取扱われている場合において、当該データのデータ主体は、その管理者に開示したデータを、標準的な電子形式を用いて無償で開示するよう、当該管理者に請求することができる。GDPR20 条 2 項と同様、DPA においても、一般的な要件が満たされ、かつ移転が過度の負担を伴わない場合、データ主体は、データ管理者に対して、自身の個人データを他の管理者に直接移転するよう請求することができる（DPA28 条 2 項)。

さらにDPA第29条は、所定の要件が満たされた場合、データ・ポータビリティ権が制約されうる旨を規定している。

【追加質問】データ・ポータビリティ権は現状どのように社会実装されているか。

2020年改正のDPAが2023年9月1日に発効したばかりなので、まだその効果を確言できる状況にない。

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）。

連邦データ保護・情報コミッショナーは、DPA上の監督機関である（DPA43条等）。委員長は、スイス議会により4年間の任期で任命されるとともに、他の機関から独立して職権を行使する（DPA43条4項・44条1項）。

コミッショナーは、個人データの取扱いが、データ保護に係る規制に違反している十分な兆候がみられる場合、連邦機関または私人に対して調査を開始することができる（DPA49条1項）。当該連邦機関または私人は、調査に必要な全ての情報を提供し、関連する文書をすべて同コミッショナーに提出する義務を負う（DPA第49条3項）。これに従わない場合、コミッショナーは調査に必要な全ての情報・文書へのアクセス、施設・設備への立入検査、証人尋問、専門家による査定を指示することができる（DPA第50条1項）。

データ保護に係る規制への違反があった場合、FDPICは行政措置として、データの取扱いを全部または一部修正・停止・終了させ、個人データを全部または一部削除・破棄するよう命じることができる（DPA第51条1項）。さらに、国外へのデータ移転に関する規定に違反があった場合、コミッショナーは当該移転を延期または禁止することができる（DPA第51条2項）。

さらにコミッショナーは、連邦機関および私人に対し情報提供・研修・助言を行い、国民の意識向上を図るとともに、権利行使の方法に関して情報提供を行い、また連邦法律の立案際して意見を具申する（DPA第58条1項）。

DPAは、同法の違反行為に対する制裁を、行政処分ではなく刑事犯罪として位置付けている。GDPRとは異なり、制裁の対象は企業そのものではなく、例えば企業の従業員といった個人となる。罰金額はGDPRより低いものの、その影響はより深刻となりうる。というのも、罰金は（大）企業によって償還される余地がないため、従業員は、罰金や刑事手続（場合によっては前科につながる可能性）を回避する強い動機を持つためである。手続法上、DPA上の犯罪行為の起訴や公判は、スイスの一般刑事法に基づき、州の管轄となる。

DPA60条1項は、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、違反者は、最高で25万スイスフラン（約4,200万円）の罰金刑に処せられる旨を規定している。さらに、個人データの収集または自動化された決定についてデータ主体に適切に通知することを故意に怠った場合、またはデータ主体がDPA19条2項に基づく権利を行使するために必要な情報を故意に提供しなかった場合にも、刑事責任が生じる。これらの責任は、苦情の申告があった場合にのみ適用される。

さらに、調査の過程においてコミッショナーに故意に虚偽の情報を提供した場合、または故意に協力を

拒否した場合、その者は、25 万スイスフラン以下の罰金に処せられる（DPA60 条 2 項）。

加えて、DPA61 条は、注意義務に違反した場合について最大 25 万スイスフランの罰金を定めている。具体的には、DPA その他の規定に違反して故意に個人データを国外に漏えいした場合、DPA の関連規定が満たされていることを確認せずに個人データの取扱いをデータ処理者に委託した場合、または最低限のデータセキュリティ要件を遵守しなかった場合、違反者は、苦情の申告に基づき、刑事責任を負う。

さらに、DPA62 条によれば、職業上の守秘義務に故意に違反にした場合、違反者は、苦情の申告に基づき、最大 25 万スイスフランの罰金に処せられる。最後に、DPA63 条は、コミッショナーまたは上訴機関が発した決定（DPA63 条の刑事罰への言及を含む）に故意に従わなかった場合ついて、違反者に対して同額の罰金を科すと規定している。

これらの行為に対する時効は 5 年である（DPA66 条）。

⑤司法的救済の仕組み（訴訟要件、集団訴訟の可能性）

個人データが私人によって取扱われている場合、原則としてデータ主体は、誤ったデータの訂正を請求することができる（DPA 第 32 条 1 項）。データ主体の人格の保護に関係するその他の救済措置については、DPA は民法の関連規定を参照している。特に、請求権者は、特定のデータの取扱いの禁止、第三者に対する個人データの開示の禁止、または個人データの削除・破棄を請求することできる（DPA 第 32 条 2 項参照）。司法上の救済措置は、データ管理者、データ処理者、または補助者など人格権侵害の原因となるあらゆる者を対象とすることができる。

私人間の訴訟手続には、スイス民事訴訟法が適用される。データ主体はデータ管理者に対して訟権を有し、いずれかの当事者の住所または本店所在地の裁判所に提訴することができる。物的管轄権および機能的管轄権は州法によって規定される。

個人データが連邦機関によって取扱われている場合、司法手続は行政手続法（連邦法）の一般規定によって規律される（DPA41 条 6 項参照）。連邦機関に対して、①個人データの違法な取扱いの差止め、②個人データが違法に取扱われている状況の除去、または③個人データの取扱いの違法性の確認を求める者は、当該連邦機関に裁定を求める権利を有する（DPA41 条 1 項参照）。当該裁定は、連邦行政裁判所、最終的には連邦最高裁への上訴により争うことができる。

コミッショナーによる調査も、最終的にはコミッショナーの裁定へと至る。これらは行政裁判所への上訴によって争うこともできる。データ主体は調査の当事者ではないが、コミッショナーから調査結果について通知を受けなければならない（DPA 第 49 条 4 項）。

⑥医薬品開発などの研究目的で診療データ等を利活用する場合に、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？

スイス法において、研究目的または医薬品開発のための患者の医療記録もしくは生体データの利活用は、ほとんどの場合、ヒト研究法（Human Research Act）（以下「HRA」）の規律対象となる。HRA は、人間の疾病や人体の構造・機能に関する全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場合にも適用される（HRA 第 2 条 1 項(e)）。HRA の適用対象となる研究の場合、健

康関連の個人データを（一次）取得する際にはインフォームド・コンセントが必要となる（HRA16 条等）。したがって、当事者は、書面によるインフォームド・コンセントを付与した場合にのみ、研究プロジェクトに参加できる。適切な説明を受けたといえるためには、以下の事項について、理解可能な口頭および書面による情報提供が必要である。すなわち、（i） 研究プロジェクトの性質、目的、期間及び実施手順、（ii）予見可能なリスクおよび負担、（iii）特に本人またはその他の者との慣例で研究プロジェクトによって期待される利益、（iv）収集された個人データを保護するための措置、（v）本人の権利（HRA16 条 2 項）。当事者は、同意の有無を決定する前に、適切な熟慮期間を与えられなければならない（HRA16 条 3 項）。さらに、あらゆる研究プロジェクトは、所定の倫理委員会による認証を得なければならない（HRA45 条 1 項(a)）。

遺伝データ（およびび生体物質）の二次利用には特別なルールが適用される。これらの検体やデータは、当事者のインフォームド・コンセントがある場合、特定の研究プロジェクトに限って、暗号化されていない状態で使用可能である（HRA32 条 1 項）。加えて、これらのデータは、当事者のインフォームド・コンセントがある場合、暗号化（すなわち仮名化）された形で研究目的全般に利用することが可能である（HRA32 条 2 項）。さらに、当事者に事前に通知を行ったうえで、その者が匿名化に異議を唱えていない場合には、生体物質および遺伝データは研究目的のために匿名化することができる。匿名化された生体物質および遺伝データは、HRA および DPA の適用範囲外となる。

遺伝データ以外の健康関連の個人データについても、同様の規律枠組みが存する。これらのデータは、当事者が事前に同意した場合、研究目的全般のために暗号化されていない状態で利用可能である（HRA33 条 1 項）。さらに、当該データが暗号化（すなわち仮名化）されているときには、当事者が異議を唱えていない場合に限り、当該データを別途利用することが認められる（HRA33 条 2 項）。匿名の形でデータを収集したとき、またはデータを匿名加工した場合については、HRA の適用を外れるため（HRA2 条 2 項(c)参照）、当該データの利用は制限なく認められる。

さらに、HRA34 条は例外規定を設けており、同条によると、以下の 3 つの条件を満たす場合、データ主体の同意なしに、生体物質または健康状態に関連した個人データを研究目的で利用することができる。第一の条件は、同意の取得または同意の撤回に関して情報を提供することが不可能、または著しく困難であることである。なお、当事者に不当な負担を課す場合も同様とされる。第二の条件は、書面での利用拒否が示されていないことである。第三の条件は、研究実施に係る利益が、生体物質または健康状態に関連した個人データの二次利用について決定権を有している当事者の利益を上回っていることである。HRA34 条は、例外的な事例のみを念頭に置く規定であるとはいえ、同条は実務上も広範に活用されている。

スイスでは現在、欧州ヘルスデータ・スペース（European Health Data Space）へ参加する予定はない。ただし連邦議会は、医療などの戦略的重要分野におけるデータの二次利用を規律する法律の制定を連邦内閣に要求している。同法案の提出は、2024 年または 2025 年以降の見込みである。

留意事項：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。

***

Ⅲ.スイス

※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（帝京大学法学部助教）

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。

---

[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.

（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 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

[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）

[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：

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

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。

[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］

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、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

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

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）

---

[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）

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）

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）

GDPR１７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. 311-3-1 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

---

[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

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

[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.

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、

---

[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.

IV.フランス

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。

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]（タマサート大学法学部専任講師）

訳・荒川稜子（慶應義塾大学 KGRI 客員所員）

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の憲法上の位置づけ

「プライバシー（privacy)」という用語は、仏暦 2534 年に制定された第 15 版にあたる 1991 年憲法第４７条が制定されるまで、タイ憲法では言及されていなかった[2]（「人の家庭内の権利、名誉、名声あるいはプライバシーは保護される」)。それ以前は、仏暦 2492 年の 1949 年憲法において、通信における秘密の保護（the protection of secrecy in communications）と家族の権利（right to family）について記載されているに過ぎない。

仏暦 2534 年の 1991 年憲法第 47 条と同様の規定は、プライバシーを侵害する著述あるいは映像の公開を禁止する条項を含む、いわゆる「人民の憲法（the people’s constitution)」と呼ばれる仏暦 2540 年の 1997 年憲法において再度規定されている[3]。また、仏暦 2550 年の 2007 年憲法では個人情報の不当な利用に対する保護が追加された[4]。

現行の仏暦 2560 年に制定された 2017 年憲法においても同様の保護は維持されているが、そうした権利に対する制限の対象は個人情報全般へと拡大された。

---

[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）の立憲革命以来のタイでは、暫定的なものを含め 20 編もの憲法が制定されてきた。こうした変化の主な理由は、13 回にもわたる軍事クーデターである。基本権の章は類似の構造を維持し、時間の経過とともに進化している。仏暦 2540 年に制定された 1997 年憲法は、広範な市民参加を伴った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.(リンク先英語)

[3] 1997 年憲法（仏暦 2540 年）第 34 条：

人の家庭内の権利、名誉、名声あるいはプライバシーは保護される。

いかなる方法によるかを問わず、人の家庭内の権利、名誉、名声およびプライバシーを侵害する、あるいは損なう著述あるいは映像の公開は、公共の利益のための場合を除き、これを行うことはできない。

[4] 2007 年憲法（仏暦 2550 年）第 35 条：

人の家庭内の権利、名誉、名声ならびにプライバシーは保護される。

いかなる方法によるかを問わず、人の家庭内の権利、名誉、名声及びプライバシーを侵害する、もしくは損なう著述または映像の公開は、公共の利益のための場合を除き、これをなすことはできない。

人は自己に係る個人情報により不当に利益を追及することから法律の規定に基づき保護を受ける権利を有する。

> *第 32 条　人は、プライバシー、名誉、名声ならびに家庭内の権利を享有する。第一段に規定された人の権利を侵害する、もしくは損なう行為、あるいは個人情報の利用は、公共の利益のために必要な限度においてのみ、当該規定に制定された場合を除き、許されない。*

こうした変更は、映像や著述の範疇を超えた現代における個人データに対する幅広い理解を反映しており、本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。

1991 年憲法 （仏暦 2534 年）	1997 年憲法 （仏暦 2540 年）	2007 年憲法 （仏暦 2550 年）	2017 年憲法 （仏暦 2560 年）
居住の自由から切り離されたプライバシー権に対する簡潔な認識	プライバシー権の認知 + プライバシーを侵害するおそれのある著述または映像の公開の禁止	プライバシー権の認知 + プライバシーを侵害するおそれのある著述または映像の公開の禁止 + データの不当な利用に対する保護	プライバシー権の認知 + 個人情報の不当な処理に対する一般禁止

概して、タイ法下においてプライバシー権は情報自己決定権と異なるという解釈はなされていない。また、居住の自由といった古典的な意味でのプライバシー権に関連する条項も存在する[5]。

憲法上の保護の他に、民商法典[6]と刑法典[7]は常に不法行為責任を規定してきた。これらの規定はプライバシーの侵害を含むと一般的に理解されているが、民商法典と刑法典の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判例第 4893/2558 号であり[9]、これはマスメディアが侵害してはならない 1997 年憲法（仏暦 2540 年）と 2007 年憲法（仏暦 2550 年）の両方で定められているプライバシー権について言及されている。

（2）個人情報保護法の憲法上の意義

個人情報保護法（以下、PDPA）の主な目的は、権利の保護にある。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、これは憲法第 26 条[10]で規定されている基本権を制限するもの

---

[5] 2017 年憲法（仏暦 2560 年）第 33 条：

> 人は居住の自由を有する。人は平穏に住居に居住し、それを占有することを保護される。裁判所の命令もしくは令状がある、もしくは法律の規定に基づくその他の事由がある場合を除き、占有者の同意なしに住居への立入、もしくは家宅捜索をなすことはできない。

[6] 民商法典第 420 条、422 条および 423 条

[7] 刑法典第 326 条および 333 条

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

[9] 最高裁判所判例第 4893/2558 号（2015 年 5 月 11 日）

[10] 2017 年憲法（仏暦 2560 年）第 26 条：

> 人の権利または自由を制限する法の施行は、憲法に基づく条件に依拠してなければならない。憲法がその条件を定めていない場合、当該する法律は法の支配に反したものではなく、また人の権利または自由に不合理な負担を課す、あるいは制限するものではなく、人の名誉に影響を及ぼさず、また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。
> 第一段の法律は一般的に適用されるものであり、特定の事件または人物への適用を意図したものではない。

として説明されている。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 2017 年憲法（仏暦 2560 年）第 32 条を特に参照している。

> *「本法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、これはタイ王国憲法第 26 条、32 条、33 条および 37 条によって許可されたものである。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、個人データ保護権が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、タイ王国憲法第 26 条に規定された基準と一致している。」*

第 26 条への言及は、PDPA の前文が第 33 条の定める居住の自由と第 37 条における財産権に言及していることを反映しており [11]、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を反映している。

一般的に、タイの立法者らは立法時に行われた主要な研究内容を簡潔に想起させるため、法律の末尾に注釈を記載する。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を理由に制定された。また、技術の進歩は、こうした侵害に該当する可能性の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おり、最終的には経済的損害を与えている。したがって、個人データの使用を規制する規則、仕組み、または措置を設けるためにも、個人データ全般を保護する法律が必要である。」*

この注釈は、タイの立法者らの念頭には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が存在していることを反映しており、学術研究においては、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概要

（１）他国の法制度による影響

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を受け、人々が政府の情報にアクセスするための権利を強化することを目的とした情報公開法（Official Information Act）が仏暦 2540 年（西暦 1997 年）に制定された。本法令の第三章には、個人情報の保護に関する規定が含まれており、必要性原則、目的制限、直接的なデータ収集、そして透明性が示されている。その後の仏暦 2546 年（西暦 2003 年）クレジット・データ事業法令（Credit Information Business Act）に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、（EU データ保護指令（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から影響を受けている。ただし、英国データ保護法と米国公正信用報告法という二つのモデルは、特にデータ主体の同意に関して、原則や法律の様式が異なっている [12]。

個人情報保護法（PDPA）

[11] 2017 年憲法（仏暦 2560 年）第 37 条：

人は財産および相続に関する権利を享有する。

その権利の範囲及び制限は法律の規定に従う。

[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）

PDPA の起草と成立の試みは、仏暦 2540 年（西暦 1997 年）に情報公開法が制定された直後から始まった [13]。PDPA 草案の初期版は、EU、英国、豪州、シンガポールを含む異なる国々の法律から影響を受けている。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）によって着手された。

しかし 2014 年のクーデター後、軍事政権はデジタル経済法の改革へと繋がった「タイランド 4.0」政策を宣言している [14]。著作権法、および電子取引・コンピュータ犯罪・電気通信に関する規則の改正を経て、電子取引開発機構（以下、ETDA）とデジタル経済社会省（以下、MDES）の協力の下、サイバーセキュリティ法案と個人情報保護法案が起草された。

2014 年の軍事クーデターから三年後の 2017 年、論争を引き起こした国民投票――これは仏暦 2560 年の 2017 年憲法という新憲法の制定へと至った――を経て、軍事政権は学術コミュニティ、市民社会、および一般国民からの抵抗が強まる中、仏暦 2550 年（西暦 2007 年）に制定されたコンピュータ犯罪法（Computer Crime Act）を改正した。この改正はオンライン上の自由の抑圧を貫き、恣意的な執行を可能にしたことで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ない中で自己検閲を誘発した [15]。当時、サイバーセキュリティ法案は、他国でも類似の法律がそうした手段で使用されているように、政府が人々のプライバシーに侵入するための新たな手段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。本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して非難されている。」* [17]

これらの事情を背景に、サイバーセキュリティ法案は個人情報保護法案と併せて検討されなければならない、という要求が主流となった。したがって、ETDA と MDES は両法の草案を見直すために市民社会の関与を深めることを試みた。GDPR が 2018 年に発効されたことは ETDA、MDES、および法制委員会の起草者らに大きな影響を与え、個人情報保護法案の構造や原則を変更させるに至っている [18]。軍事政権一次内閣下の MDES 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への参加を可能とするために個人情報保護法案の起草過程を加速させる重要な後押しとして言及している [19]。

学術的ガイドラインを通じた GDPR の影響

---

[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/>.

[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>. See also, 'Deputy PM insists cyber security bill still subject to change' (National News Bureau of Thailand, 17 October 2018) <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 .

デジタルや銀行分野の法律事務所や企業と協働で作成されたアカデミア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 1.0（以下、(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 はタイ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企業が GDPR に準拠する際や、タイ国内向けの企業に対して新たな個人情報保護法案への準備を整えるよう支援する際に、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）検討した国民立法議会の委員会[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」に含まれる可能性を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と見なされたため、市民社会もこの GDPR モデルを支持した。

PDPA の最終版は GDPR の重要な原則に従っている。研究や統計の目的は、追加の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、自動化された意思決定に対する介入に関する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ている[22]。

国際的な慣行に従う動きと、適用除外を狙う国内の抵抗の狭間で

PDPA が GDPR やその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 はプライバシー権に対して好意的であるという評判も、MDES がコンピュータ犯罪法改正による反発に対応し、サイバーセキュリティ法への批判を回避することを可能にした。

しかしながら、PDPA 第４条は様々な政府機関に対して広範な適用除外を定めており、こうした利点を薄めうる。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。仏暦 2566 年（西暦 2023 年）のテクノロジー犯罪に対する保護と抑圧への対策に関する勅令（Royal Decree on Measures for Protection and Suppression of Technology Crimes）には、データ処理の目的について 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。PDPA は、当局が法律により規定された公的任務を行う際に、個人情報を処理するための明確な法的根拠を提供しているにも関わらず、こうした新しい適用除外は、タイの官僚が PDPA や情報公開法を含むその他の個人情報保護に関する法を、サイバー犯罪や詐欺の防止といった公共の利益を追求する上での障害と見なす場合、明らかに問題となるといえる。多くの学者や市民社会は、データ処理を監督する手段のないまま、当局が国民の情報をさらに収集することを目的として、こうした一般的な適用除外を乱用する可能性を懸念している。また、この例外には銀行と電気通信という二つのデータ集約型産業による個人データの処理が関与していることから、透明性の原則はこの文脈においてかなり損なわれている。

---

[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]国民立法議会（National Legislative Assembly）は、2014 年クーデターの後に軍事政権によって指名された機関であり、立法府として機能している。

[22] 複数の組織がこの誤解を解こうと試みている。例えば、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/ >.（いずれもタイ語）

[23] テクノロジー犯罪に対する保護と抑圧への対策に関する勅令第 12 条：

> この勅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。

2023年６月、汚職防止関連の要求といった政府の要求に応じることを目的に個人データを提供する場合、さらなる政府機関や民間セクターがデータ保護に関する複数の義務から免除されることを定めた、新たな法令が暫定内閣によって承認された[24]。この新たな法令は、国会による検討を伴わずに執政府（executive branch）による適用除外の拡大を認めるという、解釈の余地があるPDPA第４条（２）の条項に基づいて発行された。

> *「本法の条項の全てもしくは一部は、第一項でデータ管理者に対して規定された同様の方法で、またはいずれかのその他の公共の利益を目的として、いかなる方法、事業者または団体においても、いずれかのデータ管理者に適用される例外は法令の形式で公布されなければならない。」*

こうした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モデルから明らかに脱線させることが予想される。また、これは憲法上のプライバシー権保護の程度を下げる恐れもある。しかし、そのような適用除外の合憲性について、憲法裁判所で争うような戦略的訴訟が生じるとは考えにくい。これは2017年憲法（仏暦2560年）32条は、このような適用除外は「公共の利益」に該当すると説明される可能性が高いという解釈を許容しうるためである。多くの市民社会は、そうした決定が下された場合、政府機関がさらなる適用除外の拡大を行う前例となることを恐れている。

（２）「個人データ（個人情報）」の定義と範囲

「個人情報」の範囲は、PDPA第６条にて以下のように定義されている：

> *「『個人情報』とは、自然人に関する情報で、当該個人を直接的または間接的に識別できるものであるが、故人に関する情報は含まれない。」*

情報公開法では、以下のように定義されている：

> *「『個人情報』とは、個人の名がある、もしくはその者を示す数字、番号のある教育、財務状況、病歴、犯罪歴もしくは職歴といった個人固有の情報、指紋、音声レコード、写真といったその者を特定できるその他の形態の指示物を意味する。このとき死亡者の個人情報も含める。」*

PDPAの定義は、情報公開法と比較して広範だが、故人に関する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。こうした広範囲の定義には、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の個人情報保護措置の下、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]。

（３）データ主体の権利と個人データ処理者（data processor）の義務

PDPAにおけるデータ主体の権利は、特に委員会が非常に限られた執行力しか持たない情報公開法におけ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

[24] Royal Thai Government, Press Release 11 July 2023, at https://www.thaigov.go.th/news/contents/details/70221
[25] Piyabutr Boonaramruang et al, Thailand Data Protection Guideline 3.0 (Chulalongkorn University Press, 2020), p 85.（タイ語）

権利[26]、アクセス権[27]、訂正権[28]、消去権[29]、制限権[30]、およびデータポータビリティ権[31]である。これらの権利の一覧はGDPRと類似しているが、データ主体はPDPAに基づきプロファイリングを含む自動化された意思決定の対象とならない権利がない点で異なる。

a）個人情報の消去権あるいは利用停止請求権

個人情報の削除、破棄、および匿名化する権利はPDPA第33条に含まれている。この権利は（1）必要な目的が失われた場合、（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法的根拠がなかったという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適用される。PDPAは、データが開示された場合、データ管理者が一定の措置を講じること、および関連する他のデータ管理者にも通知することを義務付けている。

個人情報の利用を制限する権利は PDPA第34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が想定されている。

b）個人情報保護法における同意の位置付け

タイのPDPA第24条は必要性原則を統合し、正当な目的のための適法かつ公平な処理（fair processing）[33]に関する七つの根拠（同意、歴史的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（legitimate interest）[35]、およびデータ管理者の法的義務）を規定している。

のちにデータ保護委員会によって新たに発表された規則が適用される「歴史的アーカイブおよび研究・統計」の根拠を除き、その他の六つの根拠はGDPRとほぼ同一である。GDPRと異なり、同意は現在のデジタル環境を鑑みるに唯一の主たる根拠とすることはできず、またすべきでもないと起草委員会が

---

[26] PDPA第25条および第27条

[27] PDPA第30条

[28] PDPA第35条

[29] PDPA第33条

[30] PDPA第34条

[31] PDPA第31条

[32] PDPA第34条：

データ主体は、以下に該当する場合、データ管理者に対し個人情報の使用の制限を要求する権利を有する。

(1) データ管理者が第36条に基づき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情報であるが、データ主体が当該個人情報の利用制限を要求している場合；

(3) 当該する収集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（3）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。データ管理者が第一段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うした措置を講じるよう命令するために専門家委員会に異議を申し立てる権利を有する。委員会は、第一段に従って利用停止に関する規則を制定し、公表できる。

[33] 第24条で用いている用語は「収集（collection）」である。しかし、第24条にて示されている根拠と関連するその他の規定を考慮し、本規定は、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べきである。

[34] しかしながら、仏暦2550年（西暦2007年）の国民健康法（National Health Act）9条は、医療サービス受給者を医療実験の対象として使用することに関する同意取得を義務付けている。PDPA第3条（1）と併せると、同意は医療実験の法的根拠であり続けている。他セクターの規制者も、PDPAに追加して類似の条件を設定している可能性がある。

[35] タイ語で使用されている用語は「法的利益（lawful interest）」であるが、PDPCやその他の専門家による準備作業やその後の説明にて、当該用語は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。

認めているにもかかわらず、同意の根拠は一般原則とされ、その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起草の既定の方法であった。この規定により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。

明らかに同意をデータ処理の主な根拠として定めていないその他の関連する規定と、起草の経緯と併せて考慮すると[36]、同意は主な根拠に依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「公的任務または職務権限」、および両文脈における「法的義務」である。GDPR と同様に、同意はデータ管理者にとって最良の依拠する根拠ではない。これは第 19 条がデータ主体の自律性と、データ主体が自身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ためである。オプトインへの同意が必要であり、また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サービスなどには適しているが、通常の業務では依拠すべきではない。しかしながら、多くのデータ管理者はほとんどの状況において「同意」が求められているものと未だに混同している。この迷信は、データ保護に直接関係する法[37]と関係しない法[38]の両者を含む、これまでの法律に同意が言及されていたこと、また 2022 年 6 月に PDPA を発効した際の関係者によって誤った伝達がなされたことなど、様々な複数の理由によってもたらされている。

第三者への個人データの開示に関して、かかる開示が処理目的という当初の範囲内で必要である場合、同意は必要ではない。第 23 条と第 25 条は適切な通知を義務付けており、第 27 条と第 39 条ではそうした開示に関する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 条における有効な同意の要件は、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を部分的に指摘している。同条は GDPR に従い、以下の事柄を要求している。

> *「この同意の要求は、別の事項と明確に区別でき、理解しやすく容易にアクセスできる方法で、明確かつ平易な文言を用いて、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なく表示されなければならない。」*

また、第 19 条は、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は個人情報保護委員会（以下、PDPC）にあると規定している。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義務的な標準書式を参照している[39]。また、データ管理者に対して、各業界が定めた既存の自主的な標準書式に従うこと、さら

---

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

[37] 例えば、仏暦 2550 年（西暦 2007 年）クレジット・データ法令（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への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保護者の同意。

[39] PDPA 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、事業、または事業体において、個人データの保護を規定するセクター固有の法律が存在 する場合は、当該法の規定が適用される。これは、以下のいずれかの場合には適用されない

(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、上記の特定の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；

(2) 異議に関する規定、専門委員会にデータ主体保護のために発令する権限を付与する規定、および関連する罰則を含む監督官庁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：

(a)当該法が異議に関する規定を定めていない場合

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（European Data Protection Board）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類似の提案を行っている。2022 年 9 月 7 日に発表された通知に関するその他の PDPC ガイドラインも、GDPR や ICO による勧告に従っている[41]。これらのガイドラインに法的拘束力はないものの、専門委員会と裁判所はこれらを考慮した法解釈を行う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

PDPA 第 24 条は、歴史的アーカイブおよび研究・統計における、一般的な個人データ（センシティブではないデータ）の処理に関して異なる法的根拠を規定している[42]。解釈の方向性が不明瞭なため、この法的根拠が依拠されることは少ない。保護措置に関する具体的なガイドラインは、未だに PDPC より発表されていない。

診療記録や生体認証データを含むセンシティブデータを司る第 26 条も、厳格な同意条件に関する例外を設けており、これは多くの場合、医療従事者やヘルスケアならびに福祉的措置に関するものである。GDPR 第 9 条（2）（i）と同様に、第 26 条（5）（b）[43]も、法律で定められた公衆衛生の利益を目的とした診療データの使用は、正当な目的であるとする。これは、特定の法律に基づいて行われる研究プロジェクトでは患者の同意が不要であることを意味する。また、PDPC の委員会メンバーは、民間研究所が政府機関と協働していない場合、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 によって直接求められているわけではないものの、医療や研究に関するその他の職業倫理や規制により求められる可能性がある。

(b) 当該法の規定が、その当該法に基づき異議を検討する権限のある監督官庁にデータ主体保護のために発令する権限を与えているが、その権限が本法に基づく専門委員会の権限と同等ではない場合。及び、当該法に基づき権限を有する監督官庁が専門委員会に要求した場合、あるいはデータ主体が本法に基づき専門委員会に異議を申し立てるかのいずれかの場合。

[40] 次の URL より閲覧可能（リンク先タイ語）
<https://www.mdes.go.th/uploads/tinymce/source/*สคส/แนวทางการดำเนินการในการขอความยินยอมฯ*.pdf>.

[41] 次の URL より閲覧可能（リンク先タイ語）
<https://www.mdes.go.th/uploads/tinymce/source/*สคส/แนวทางการดำเนินการในการแจ้งวัตถุประสงค์ฯ*.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 条は、実験の対象として医療サービス受給者を利用することについて、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、同意は医療実験の法的根拠であり続けている。PDPA に加え、他のセクターの規制も同様の条件を設定している可能性がある。

[43] PDPA 第 26 条：

人種的若しくは民族的な出自、政治的な意見、カルト、宗教上若しくは思想上の信条、性生活、犯罪歴、健康に関するデータ、障害、労働組合情報、遺伝子データ、生体認証データ、並びに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、データ主体からの明確な同意がない限り禁止される。これは、以下のいずれかの場合には適用されない。

（5）以下の目的を達成するために法律の遵守が必要である場合；

（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、国境を越える重大な伝染病または伝染性もしくは疫病性の伝染病に対する保護、または医薬品、医療用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の分野における公共の利益

第 26 条（５）(e) も、法律で定義された公共の利益をもう一つの同意の例外として規定 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」を提供する義務は、個人データの処理によって得られるうる公共の利益と、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) 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

PDS といった個人データに対する本人の controllability の補助の利活用を目的とした機器や仕組みに関する具体的な条項は存在せず、そうした活用は禁止されていない。

これに関して、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、 PDPA 第 24 条に基づく法的根拠において「契約」または「正当な利益」とみなされる可能性がある。そうした PDS の運営者は、データ管理者と見なされなくてはならない。センシティブデータの処理は、PDPA 第 26 条に基づき、より厳格な条件の対象となる。

e) プロファイリングに対する規制

GDPR 第 21 条で示されているような、プロファイリングに異議を述べる権利を規定する具体的な条項はない。ただし、本件に関しては過去にも PDPA 制定後にも議論されており、例えば、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に関するガイドラインなどでそうした議論が行われている[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（good fait）を証明するために影響評価を記録しなければならない。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行使することで、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) GDPR 第 20 条のようにデータ・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？

第 31 条は、データ管理者から自身の個人データをアクセス、および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 PDPA 第 31 条（２）に含まれており、以下の通りである。

(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という形式で個人データを直接取得する要求

国家立法議会の委員会は、草案の検討過程において本規定について詳細に議論している。公共セクターからの多くの代表者が、本権利を他国で見做されているような市場の競争を促すものよりも、開かれた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こうした意図とは対照的に、PDPA はオープンデータ構想への主な障壁として何度も言及されている。

本権利の実施は、まだ実務では見られてない。本権利は、データ管理者がその権利の存在を容易に証明できるという技術的な状況を条件としていることから、本規定に基づいた異議の申し立てが認められる見込みは薄いと言える。

（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）

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

組織構造と政府との関係性

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。PDPC の現メンバーは法律の他に医療業界、証券取引、法執行、および軍事など関連する分野の専門家 10 名である。MDES 事務次官、首相府事務次官、法制委員会事務局長、消費者保護委員会事務局長、権利自由擁護局局長、PDPC 事務所の司法長官および事務局長が、その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 の委員を犯罪行為（actus reus）により解任することができる[46]。

タイ公法の下、PDPC は「独立行政組織」の地位にある。PDPC は通常の政府機関とは異なる規則によって管理される中立した政府機関であり、政治的な介入を受けてはならない[47]。PDPA 第 46 条は、政府がシード資金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、および様々な規定、規範、下位規則などの発行も担当する。さらに、PDPC は国家デジタル経済社会開発委員会（National Committee for Digital Development for Economy and Society）が策定した方針に従い個人情報保護に関する規制に対しても責任を負い、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に関する規制の権限を有する他の政府機関に、助言や協力をする義務も負う。

制裁や告訴の仕組み

PDPC は、適切と判断した場合、異議の検討やコンプライアンスの違反を調査、そして紛争を解決するための専門委員会を任命することができる[49]。現在、PDPC は二つの専門委員会を任命しており、一つは財務・経済関連の異議、もう一つはデジタル技術関連の異議に特化している。

PDPA 第 71 条から 76 条は、データ主体を対象とした異議を申し立てるための仕組みを規定している。異議は PDPC に直接、または電子メールにて提出できる。異議申し立てのテンプレートは、その対象が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、またはその他の政府機関）である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、異なる意義申し立ての仕組みも考慮することを専門委員会に義務付けている第 73 条第２段と一貫している。

---

[45] PDPA 第 12 条

[46] PDPA 第 13 条

[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（Office of the Public Sector Development Commission）の原則と慣行に従っており、これらの原則と実践は以下の URL より閲覧可能 <https://webdev.excise.go.th/act2560/images/files/*กฎหมายอนๆ/_แก้ไข_เพมเตม*.pdf>（リンク先タイ語）。最新版の各カテゴリのリストは以下のリンクより閲覧可能<https://po.opdc.go.th/>（リンク先タイ語）

[48] PDPA 第 16 条（１）

[49] PDPA 第 72 条

[50] 詳細に関しては https://www.mdes.go.th/mission/detail/6408-*ประกาศและคำสั่งของสำนักงาน* を参照（リンク先タイ語）

「異議の申出、受理拒否、却下、審議、および審議期間は、他の法令に基づき審議権限があった場合の異議の受理拒否また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。」

こうした第 73 条の解釈は、異なる法律の下で重複している課題について規定する第３条と併せて、銀行、保険、電気通信といった特定のセクターにおけるプライバシー関連の問題を規制する他の政府機関と PDPC との間で、管轄権の問題を引き起こす恐れがある。

異議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行為の禁止、または損害を停止させるための行為の履行を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]と行政罰[53]を与えることができる。行政処分には通知、召喚、調査、押収、および没収が含まれ、行政刑罰は最大 5,000,000 タイバーツ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できる[55]。

加えて、PDPA 第 79 条から第 81 条は、最高１年の刑事罰を規定しており、さらに第 78 条は実際の損害の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裁判所）が PDPA 関連の紛争を判断する可能性を示唆している。

（５）司法的救済の仕組み

PDPC の権限下での主な執行措置である行政制裁の他に、PDPA 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異議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した場合に有益である。

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おらず、タイの訴訟手続法の一般原則が適用される[58]。データ漏洩に対する集団訴訟は、タイ民事訴訟法典 222/8 条で提起が認められる対象事件に該当する可能性がある[59]。しかしながら、司法裁判所の裁判官の知識が PDPA 関連の紛争に関す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、全体的に疑問が残る。

※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ある。

---

[51] PDPA 第 74 条（３）

[52] PDPA 第 74 条（４）

[53] PDPA 第 90 条

[54] PDPA 第 85 条および第 87 条

[55] タイの行政裁判所の仕組みに関する詳細は以下を参照
https://www.admincourt.go.th/admincourt/en/structure.php（リンク先英語）

[56] PDPA 第 77 条から第 78 条

[57] PDPA 第 79 条から第 81 条

[58] タイにおける集団訴訟手続きの詳細に関しては、以下を参照
Tanaporn Farungsang, ‘Summary of Class Action under the Civil Procedure Code’ (SEC, 2019)
<https://www.sec.or.th/EN/Documents/LawsandRegulations/ClassAction-appendix-EN.pdf.>（リンク先英語）

[59] 民事訴訟法典 222/8 条

以下の訴訟において、構成員が多数存在する場合、その構成員である原告は集団訴訟を申し立てることができる：

(1) 不法行為に基づく訴訟

(2) 契約違反に基づく訴訟

(3) 環境、消費者保護、労働、証券及び証券取引所、取引競争（独占禁止）等の法律に基づく権利の主張に関する訴訟

VI. 台湾

台湾の個人情報保護法制

Chien-Liang Lee（中央研究院法律学研究所教授・同所長）
訳・門谷春輝（慶應義塾大学大学院法学研究科前期博士課程）

1. 憲法と個人情報保護法制との関係性

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付け

(1) 台湾において、プライバシー権及び情報自己決定権は、権利として憲法上保障されている。
＜編集上の都合により削除＞
[訳者による要約：プライバシー権は、中華民國憲法第 22 条（「およそ人民のその他の自由及び権利は、社会秩序及び公共の利益を妨げない限り、 均しく憲法の保障を受ける。」）に基づき保障される基本権として、台湾の憲法裁判所に当たる司法院大法官会議の複数の解釈において認められている。]

(2) プライバシー権ないし情報自己決定権
＜編集上の都合により削除＞
[訳者による要約：司法院大法官会議は主に「情報プライバシーの権利」という用語を用いてきたが、2005 年の司法院大法官第 603 號解釈は、自由、民主主義、そして立憲主義に基づく法制度の中核的価値は、人間の尊厳を守り、人格の自由な発展を確保することであるという考えからプライバシーの権利が導出されていると解釈した。そのため、プライバシー権は、私生活に対する干渉のほか、情報自己決定を保護するものであると考えられている。]

②個人情報保護法制の憲法上の意義

現行規定である個人データ保護法（中国語では「個人資料保護法」）は、1995 年から施行されていたコンピュータ処理個人データ保護法（中国語では「電腦處理個人資料保護法」。以下、「旧法」という。）を 2010 年にその題名を含めて改正し、2012 年 10 月 1 日に施行された（直近の改正は、2025 年 11 月 11 日に公布された)。個人データ保護法及び旧法は、プライバシー権や情報自己決定権には言及していない。立法者による改正法の説明には、「プライバシー」という用語が多くみられるが、これは、個人データに対するプライバシー保護が、個人データ保護法の制定に当たって立法者の主な関心事であったことを示している。

人格権の保障は、個人データ保護法の目的の一つである。個人データ保護法に情報プライバシーや情報自己決定が包含されていると考えた場合、人格権の保障がさらに強化されていると解釈することができる。旧法の下で、本人同意は、政府機関又は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った。また、個人データの利用は、原則として収集された際の目的に限定されていた。このように、旧法は、個人データの自律性を形成したものとして位置付けられる。他方で、個人データ保護法は、インフォームド・コンセントに重点を置いており、データ主体によるコントロールに関する権利を保障している。この背景には、情報自己決定権を個人データ保護法の原理の一つとして位置付ける立法者の意図がある。

2. 個人情報保護法制の現状と課題

①外国法の影響

旧法は、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ついてのガイドライン」（Guidelines on the Protection of Privacy and Transborder Flows of Personal Data）が示した 8 つの原則を参照している。これは、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、責任の原則の 8 つから成る。

個人データ保護法による旧法の改正段階では、EU の GDPR の前身であり、個人データの処理や移転を規制していたデータ保護指令（Directive 95/46/EC）の要件が言及されている。この要件は、データの品質、データ処理の適法性、センシティブデータの処理、当事者への通知、当事者の権利、当事者の異議、自動化された個人の意思決定、データの機密性・セキュリティ、登録、データ処理に関連する公開、越境データ移転等から成る。

②「個人データ」の定義と射程

一般的に言えば、個人データ保護法における個人データの定義は、GDPR と類似している。

その基準となるのは、自然人を直接的又は間接的に識別可能か否かである。死者の個人データは除外される。暗号化[1]又は非識別化[2]されたデータが個人データに該当するか否かは、データを比較、照合、又は結合した後に自然人を識別できるかによる。クッキーが個人データに該当するか否かは、特定の場面において収集されたデータにより自然人を直接的又は間接的に識別できるかによる。以下の表は、「個人データ」の定義と射程について、GDPR と個人データ保護法を比較したものである。

[1]「暗号化されたデータは、それ自体から特定の個人を直接識別することはできないが、比較、照合、又は結合によって個人を識別できるのであれば、それらは個人データ保護法の下での個人データとなる。」（國家發展委員會發法字第 1090004500 號）を参照。

[2]「電気・電子製品の試験・認証機関である電子検験中心により非識別化を受けたデータに個人データ保護法が適用されるか否かは、その非識別化されたデータが特定の個人を直接的または間接的に識別するために使用できるかどうかに依存する。これに関する紛争については、司法判断に委ねられる。」（國家發展委員會發法字第 1080081030 號）を参照。

GDPR	個人データ保護法
第 4 条 （1）「個人データ」 とは、 識別された自然人又は識別可能な自然人（「データ主体」）に関する情報を意味する。識別可能な自然人とは、特に、氏名、識別番号、位置データ、オンライン識別子のような識別子を参照することによって、又は、当該自然人の身体的、生理的、遺伝的、精神的、経済的、文化的又は社会的な同一性を示す一つ又は複数の要素を参照することによって、直接的又は間接的に、識別されうる者をいう。	第 2 条 （1）「個人データ」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、家族の情報、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、連絡先の情報、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又は間接的に識別するために使用される可能性のある情報を指す。 ・個人データ保護法施行規則第 3 条 個人データ保護法第 2 条（1）の「間接的に識別」されたデータ主体とは、政府機関又は非政府機関が、データを比較、照合、又は結合しない限りデータ主体を直接的に識別できない状況のことをいう。
・GDPR は、死者に対しては適用されない（前文（27））。	・個人データとは、存命中の自然人のデータのことを言う。死者のデータは、個人データ保護法による保護の対象外である（國家發展委員會發法字第 1090021610 號）。

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

個人データ保護法第 3 条によると、データ主体は自身の個人データについて、次の権利を行使することができる。1. 自身の個人データを照会し、その内容を確認する権利、2. 自身の個人データの複製を求める権利、3. 自身の個人データを補足又は訂正する権利、4. 自身の個人データの収集、処理、又は利用の停止を求める権利、5. 自身の個人データを消去する権利。なお、これらの権利は契約により放棄又は制限されてはならない。すなわち、個人データ保護法の下では、データ主体は少なくとも以下の権利を有していると理解することができる。

1. 照会又はアクセスを求める権利
2. 複製を求める権利
3. 補足又は訂正を求める権利
4. 収集、処理、又は利用の停止を求める権利
5. 削除を求める権利

個人データ保護法の規定に基づく、各権利の具体的な内容は次のとおりである。

1. 照会又はアクセスを求メル権利：データ主体は、政府機関又は非政府機関に対し、照会に応じるとともに、収集された個人データを確認することを求めることができる（第 10 条）。
2. 複製を求める権利：データ主体は、政府機関又は非政府機関に対し、収集された個人データの複製を提供するよう求めることができる（第 10 条）。

3. 補足又は訂正を求める権利：データ主体は、政府機関又は非政府機関に対し、彼らの個人データの正確性を担保するとともに、個人データの訂正又は補足を行うよう求めることができる（第 11 条（1））。
4. 収集、処理、又は利用の停止を求める権利、及び 5. 削除を求める権利：
（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、政府機関又は非政府機関に対し、個人データの処理又は利用を停止するよう求めることができる（第 11 条（2））。
（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、又は該当する期間が満了した場合、データ主体は、政府機関又は非政府機関に対し、個人データの削除、又はその処理や利用の停止を求めることができる（第 11 条（3））。
（3）個人データの収集、処理、又は利用が個人データ保護法に違反する場合、データ主体は、政府機関又は非政府機関に対し、個人データの削除、又はその処理や利用の停止を求めることができる（第 11 条（4））。

GDPR とは対照的に、個人データ保護法には、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、又は（GDPR 第 17 条の忘れられる権利と同様の）個人データが収集又は処理された目的に関連して不要になった個人データの削除を請求する権利の規範がない。

B. 政府機関の義務

個人データ保護法第 6 条（1）に規定されている個人データ（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）を除き、政府機関による個人データの収集又は処理は、明白な目的の下、以下のいずれかの根拠に基づいて行われなければならない。
1. 法律により定められた義務を履行するために必要な範囲内にあること
2. データ主体による本人同意[3]が存在すること、又は
3. データ主体の権利や利益が侵害されていないこと（第 15 条）。

個人データ保護法第 6 条（1）に規定されている個人データ（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）は、原則として収集、処理、又は利用が認められていない。ただし、以下の場合を除く。
1. 法律により明示的に定められている場合。
2. 政府機関が法律により定められた義務を履行するため、又は非政府機関が法律により定められた義務を履行するために必要な範囲内で、かつ、その前後において適切な安全対策が講じられている場合。
3. 個人が自発的に開示した個人データ、又は他の場所で合法的に開示された個人データ。
4. 政府機関又は学術研究機関が、医療、保健、犯罪防止、統計、又は学術研究の目的で必要とする場合で、かつ、提供者による処理または開示方法によって、特定の個人を特定できないデータである場合。
5. 政府機関が法律により定められた職務を遂行する、または非政府機関が法律により定められた義務を履行するために必要な範囲内で、かつ、その前後において適切な安全対策が講じられている場合。
6. 個人から書面による同意を得た場合。ただし、特定の目的のために必要な範囲を超えて情報が収集、処理、又は利用される場合、又はその他の法的制約により、当事者の書面による同意のみに基づく収集、処理、又は利用が禁じられている場合、あるいは、そのような同意が当事者の意思に反する場合は、この限りではない。

[3] ここでいう「同意」とは、個人データ保護法に基づく情報の通知の後、データ主体によって与えられる合意の意思表示を指す（第 7 条（1））。また、政府機関又は非政府機関が情報を通知した際、データ主体が反対の意思を示さず、かつ積極的に自身の個人データを提供した場合、データ主体の同意は与えられたものとみなすことができる（第 7 条（3））。

政府機関は、個人データ保護法第 15 条又は第 19 条に従い、個人データを収集する場合にデータ主体に対し、以下の情報を明示的に通知すること。
1. 政府機関又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種類
4. 個人データを利用する期間、領域、受領者、及びその方法
5. 個人データ保護法第 3 条に基づくデータ主体の権利、及びその権利を行使する方法
6. 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））

政府機関又は非政府機関は、データ主体により[自発的に]提供されていない個人データの処理又は利用に先立って、個人データ保護法第 15 条又は第 19 条に従い、データ主体に対し、データの収集源及び個人データ保護法第 8 条（1）1～5 で規定されたその他の情報を通知すること（第 9 条（1））。
政府機関は、以下の情報をオンライン上で公開するか、又は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。これは、以下の情報にいかなる変更があった場合にも、適用される。
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その目的
4. 個人データの種類（第 17 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、又は公開を予防することを目的として、セキュリティ対策やメンテナンスを実施するための専門の人員を割り当てること（第 18 条）。

C. 非政府機関の義務
個人データ保護法第 6 条（1）に規定されている個人データ（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）を除き、非政府機関による個人データの収集又は処理は、明白な目的の下、以下のいずれかの根拠に基づいて行われなければならない。
1. 法律により明示的に要求されていること
2. 非政府機関とデータ主体の間に契約関係又は準契約関係があり、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公開されている、又は適法に公開されている場合
4. データ提供者により処理された、又はデータ収集者により公開された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として、学術機関による公益目的の統計又は研究に必要であること
5. データ主体による同意[4]
6. 公益のために必要であること
7. 個人データが一般に公開されている情報源から取得されていること（ただし、個人データの処理又は利用を禁止するのに値する最も重要な法益をデータ主体が有しているときは除く）
8. データ主体の権利や利益が侵害されていないこと（第 19 条（1））。

非政府機関は、個人データ保護法第 15 条又は第 19 条に基づいて個人データを収集するとき、データ主体に以下の情報を明示的に通知すること。
1. 政府機関又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、受領者及び方法

[4] ここでいう「同意」の定義は、前掲注 3 と同一である。

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））

非政府機関は、データ主体により[自発的に]提供されていない個人データの処理又は利用に先立って、個人データ保護法第 15 条又は第 19 条に従い、データ主体に対し、データの収集源及び個人データ保護法第 8 条（1）1～5 で規定されたその他の情報を通知すること（第 9 条（1））。

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、又は公開を予防することを目的として、適切なセキュリティ対策を実施すること（第 27 条（1））。

④ 個人データ保護法を執行する監督機関の組織と権限

台湾には、個人情報保護を所轄する単一の機関が未だ存在しない。これは、個人情報保護が分権型であることを意味している。各行政庁は、それぞれの所管する事務に関してデータ保護の責任を負う。台湾の最高行政機関である行政院は、個人データ保護に関して非政府機関の監督を行う中央当局の一覧を定めている[5]。

憲法裁判所に当たる司法院憲法法廷は、2022 年の判決（111 年憲判字第 13 號）において、個人データ保護法について、個人データ保護のための独立した監督機構が存在しないことにより情報プライバシーの保護が不十分となっているため、違憲の可能性があるほか、監督機構に関連する枠組みが 3 年以内に創設されるべきであると判示した。

これを受けて行政院は、2023 年 4 月 13 日、個人データ保護法を所轄する機関として個人データ保護委員会（中国語では「個人資料保護委員會」）を設置するため、個人データ保護法に第 1-1 条を設ける同法の改正案を提出した。2023 年 5 月 31 日、この改正案は立法院により可決されたが、まだ発効には至っていない。この施行日を指定する権限は、行政院に委ねられている[訳注：本改正案は、2025 年 11 月 11 日に大統領により公布されたが、施行日は未定である（2026 年 4 月 1 日時点）]。

⑤ 司法的救済の仕組み（訴訟要件、集団訴訟の可能性）

個人情報保護に関して、救済の問題は前述のデータ主体の権利と密接に関係しており、相互依存的な関係にある。台湾の救済制度では、被告が政府機関である場合は行政訴訟手続、そして被告が非政府機関である場合は民事訴訟手続を通じ、救済が図られる。これらの救済は、個人データ保護法には規定されていない。しかし、これらの手続は、行政不服審査法、行政事件訴訟法、及び民事訴訟法の規定に従い、それぞれの違反の性質に応じて進められる。加えて、個人データ保護法には、次のとおり、損害賠償について具体的な規定が設けられている。

A. 請求の根拠と責任の原則
1. 政府機関
（1）政府機関は、天災、非常事態又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データ保護法違反に起因する個人データの不法な収集、処理、利用、又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（第 28 条（1））。
→政府機関は、ほぼ無過失責任を負うといえる。
（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による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求めることができる（第 28 条（2））。
2. 非政府機関

[5] <https://www.moj.gov.tw/media/16809/542114375377.pdf?mediaDL=true>

（1）非政府機関は、個人情報の違法な収集、処理、利用、又はその他のデータ主体の権利侵害について、それらが故意又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、生じた損害について責任を負うものとする（第 29 条（1））。
→ 立証責任は非政府機関にある。
（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による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求めることができる（第 29 条（2）にて前述の第 28 条（2）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又は不可能である場合、被害者は裁判所に対し、損害の重大性に応じて、一つの事案につき 500 圓以上 2 万圓以下の賠償を請求することができる（第 28 条（3））。
（2）同一の事案において、複数のデータ主体の権利が侵害された場合、データ主体に対する損害賠償の総額は 2 億圓を超えないものとする。ただし、当該事案に関連する利益が 2 億圓を超える場合、損害賠償は当該利益の価額を上限とする（第 28 条（4））。
2. 非政府機関についても、上記と同様である（第 29 条（2））。
3. 個人データ保護法以外の損害賠償の法的根拠（第 31 条）：
（1）政府機関には、国家賠償法が適用される。
（2）非政府機関には、民法典が適用される。
4. 集団訴訟（第 32 条～第 40 条）
（1）同一の事案において、複数のデータ主体の権利が侵害された場合、財団法人又は公益法人は、少なくとも 20 人のデータ主体から訴権の委任状を取得した後、自身の名で裁判所に訴訟を提起することができる（第 34 条（1））。
（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。

以下の表は、救済に関して GDPR と個人データ保護法を比較したものである。

GDPR	個人データ保護法
・第 77 条 （1）他の行政上の救済又は司法上の救済を妨げることなく、全てのデータ主体は、そのデータ主体が、自己と関係する個人データの処理が本規則に違反すると判断するときは、特に、データ主体の居住地の加盟国、就業場所の加盟国又は違反行為があると主張する場所の加盟国において、 監督機関に異議を申立てる権利を有する。	・第 28 条 （1）政府機関は、天災、非常事態又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データ保護法違反に起因する個人データの不法な収集、処理、利用、又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。 →政府機関が免責されるのは、天災等の場合に限られる。これは GDPR よりも厳格である。
・第 79 条 （1）第 77 条により監督機関に異議を申立てる権利を含め、利用可能な行政上の救済又は裁判外の救済を妨げることなく、個々のデータ主体は、自ら、本規則を遵守せずに自己の個人データの処理がなされた結果として本規則に基づく自己の権利が侵害されたと判断するときは、効果的な司法救済の権利を有する。	・第 29 条 （1）非政府機関は、個人情報の違法な収集、処理、利用、又はその他のデータ主体の権利侵害について、それらが故意又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、生じた損害について責任を負うものとする。 →非政府機関は、証明責任を果たした場合に免責される。これは GDPR と同様である。
・第 82 条 （1）本規則の違反行為の結果として財産的な損害又は非財産的な損害を被った者は、管理者又は処理者から、 その被った損害の賠償を受ける権利を有する。 （2）処理に関与した管理者は、本規則に違反する処理によって発生した損害に関し、法的責任を負う。処理者は、処理者に対して特に課される本規則上の義務をその処理者が遵守しなかった場合、又は、管理者の適法な指示の範囲外で処理者が行動した場合、若しくは、その指示に反して行動した場合においてのみ、処理によって発生した損害に関し、法的責任を負う。 （3）管理者又は処理者は、 その損害を生じさせた出来事に関し、 いかなる意味においても責任を負わないことを証明したときは、同条（2）に基づく法的責任を免れる。	・第 34 条 （1）同一の事案において、複数のデータ主体の権利が侵害された場合、財団法人又は公益法人は、少なくとも 20 人のデータ主体から訴権の委任状を取得した後、自身の名で裁判所に訴訟を提起することができる。
・第 80 条 （1）データ主体は、 加盟国の国内法に従って適正に組織され、 公共の利益に属する制定法上の目的をもち、 かつ、データ主体の個人データの保護と関連するデータ主体の権	

利及び自由の保護の分野において活動する非営利 の組織、団体又は協会に対し、自身の代わりに異議を申立てること、自身の代わりに第 77 条、第 78 条及び第 79 条に規定する権利を行使すること、並びに、加盟国の国内法が定めている場合、自身の代わりに第 82 条に規定する賠償金を受ける権利の行使を委任する権利を有する。	

⑥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。

個人データ保護法第 6 条（1）4 の但書によると、自然人の医療記録、ヘルスケアデータ、及び遺伝子データは、データ提供者が処理した、又はデータ管理者が開示したデータが特定のデータ主体の識別に至るものでない限り、政府機関によるヘルスケア、公衆衛生、又は防犯を目的とする場合、及び学術機関による統計又は研究を目的する必要な場合に、収集、処理、及び利用することができる。言い換えれば、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、又は利用できるのである。

ここで、司法院憲法法廷が 2022 年に下した判決（111 年憲判字第 13 號）を改めて紹介する。

本判決の概要は、次のとおりである。

医事サービス機構（醫事服務機構）は、全民健康保険法第 80 条に基づき、衛生福利部中央健康保険署（以下、「健康保険署」という。）に対し、保険医療費の請求のために、被保険者の診療記録や薬の処方データ等を提供している。健康保険署は、健康保険に関する膨大な個人データを長年にわたって収集してきた。国家衛生研究院は、健康保険署から健康保険に関する個人データの提供を受けた上で、「国民健康保険研究データベース」（全民健康保險研究資料庫）を作成・公開した。また、国家衛生研究院は、公開された健康保険情報を衛生福利データ科学センター（衛生福利資料科學中心）に送信した。原告は、プライバシー権によって憲法上保障を受ける健康保険データが目的外使用されたことを理由に、これらの行為が違法であるとして、健康保険署が全民健康保険法上定められた目的を超えて健康保険データを外部提供すべきではないと主張した。健康保険署はこの主張を受け入れなかったため、原告は行政訴訟を提起した。行政訴訟の確定終局判決によって敗訴した原告は、個人データ保護法第 6 条（1）4 の但書、全民健康保険法第 79 条及び第 80 条の規定が違憲であるとして、司法院憲法法廷に対して憲法異議を申し立てた。

憲法法廷の判示は、次のとおりである。

全民健康保険法第 79 条及び第 80 条の各規定について、健康保険に関するデータの保存、処理、及び外部送信に関する規律に加え、全民健康保険局により外部へ提供されるデータの対象、目的、法的要素、範囲、及び措置に関する明示的な規律が欠けている。

また、全民健康保険局から他の政府機関又は学術機関へ送信された、元の収集目的の範疇を超える個人の健康保険データの利用に関して、当時の法体系で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存在しないため、中華民國憲法第 22 条により保障される情報プライバシー権に反する。

さらに、健康保険データを所管する官庁は、オプトアウトの対象、根拠、手続き、及び法的効果を規定する、又はオプトアウトを拒否する法律を 3 年以内に制定しなければならない。この期限が過ぎた場合、データ主体はデータの目的外利用を停止するよう要求することができる。

批判すべき点：

VI. 台湾

1. 本判決は、個人データ保護法第 6 条（1）4 の但書が、政府機関による国民健康保険研究データベースの設立の法的根拠となりえるか、という問いを明確にしていない。
2. 本判決は、データ主体のオプトアウトの権利に関する立法を求める一方で、本人同意を伴わないデータの強制的な収集、処理、又は利用を可能にする個人データ保護法第 6 条（1）4 の但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。利用停止を求める権利、又はオプトアウトの権利は、影響を受ける者からの事前の同意を前提としている（オプトインの権利とは対照的である)。法律に基づき、政府機関が影響を受ける者からの同意なしに個人データを強制的に収集、処理、又は利用できるのであれば、影響を受ける者はどのようにして利用停止を求める権利を行使できるのだろうか？それと反対に、影響を受ける者が個人データの利用停止を求める権利を既に行使した場合、政府機関はどのように個人データを強制的に収集、処理、又は利用できるのだろうか？このような矛盾が生じないよう、本判決のオプトアウトの権利に関する判示は、ヘルスケアデータ等の機微なデータの二次的利用にのみ応用されるべきである。また、政府機関が二次的利用を強制することのできる範囲は、限定されるべきである。

謝辞：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

尚知永（慶應義塾大学訪問研究員、韓国弁護士）

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]。

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

[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

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。

[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。

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

[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。

[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。

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[12]）。さらに、

---

[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。

[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] 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

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

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。

[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。

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。

[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。

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
      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。

[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。

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

[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。

[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）。

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。

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（被告）の

[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

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]）。

（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。

[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。

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。

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、

[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。

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

[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。
[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。

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）
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-klage）[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

[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。

[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。

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
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

[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）。

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。

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

[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。

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。 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。

---

[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）。

[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。

[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。
[42] 注４０を参照。

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)。

※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。

---

[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)

Ⅷ. 中国

中国の個人情報保護法制に関する調査

松田侑奈（慶應義塾大学 KGRI 客員所員）

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。

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

[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。

Ⅷ.中国

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）。

[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。

Ⅷ.中国

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
個人信息権 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。

[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。

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。

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

---

[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。

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。

（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：〇〇省インターネット情報弁公室、〇〇市工商行政局等)。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)。

---

[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。

(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

---

[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

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。

「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。

---

[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

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。

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。

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’個人信息保护特别義務設置研究”、 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。

[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。

Ⅷ.中国

⑬趙万一、“从民法與憲法关系的視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田婭娟、「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。

Ⅷ.中国

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（北九州市立大学法学部准教授）

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（*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。

---

[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――憲法と立法過程・深層からみるプライバシーのゆくえ』（弘文堂、 2024 年）202 頁以下〔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。

IX.カナダ

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

[3] *R. v. Spencer*, [2014] 2 S.C.R. 212

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 Act*, 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

[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.
[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.

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。

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

[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。
[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.

「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

[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。
[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).

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。

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

[30] *See,* OPC, "The Privacy Act in brief" (August 2019)
[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).

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、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、

[33] Innovation, Science and Economic Development Canada, “The Artificial Intelligence and Data Act (AIDA) – Companion document” (March 2023).

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。

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

[34] OPC, "Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)" (May 2018).
[35] OPC, *ibid.*
[36] *See*, OPC, "Organizational Structure" (August 2023).

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

[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

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。

---

[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.

[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）。

IX.カナダ

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

アメリカ連邦プライバシー法・カリフォルニア州プライバシー権法概説

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）
訳・門谷春輝（慶應義塾大学大学院法学研究科前期博士課程）

アメリカのプライバシー法の理論及び実務は、各国の中でも最も複雑なものの一つである。このような複雑性を生む要因となっているのは、(EU の一般データ保護規則（GDPR）のように）データの収集と処理に関するほぼ全ての側面を規制しようとする法体系ではなく、むしろその逆である。アメリカの消費者プライバシー法には、包括的な法令が存在せず、それらは極めて断片的である。この調査報告書では、アメリカの連邦プライバシー法、並びに本稿執筆時点[2023 年]において全米で最も包括的な消費者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（California Consumer Privacy Act: CCPA)、及びカリフォルニア州プライバシー権法（California Privacy Rights Act: CPRA）について概説する。

以下、第 1 章では、アメリカの連邦レベルと州レベルのプライバシー法の概要を紹介した上で、自主規制モデル（self-regulatory models）の実務上の意義、そして本人同意に関連する課題について述べる。また、第 2 章では、執行に関する課題を取り上げる。

1.1 アメリカ合衆国憲法

情報プライバシー（information privacy）とは直接関係しない一部の例外を除くと、アメリカ合衆国憲法（以下、「憲法」という。）は、主に政府権力を羈束するものであり、私的権力はその対象とはならない。一般的には、アメリカ人（国民・永住権保持者）に「憲法上の権利」があると言う場合、政府による何らかの行為に対抗する権利、あるいは政府が支持した私的な行為に対する権利を意味している[1]。 また、「プライバシー」（privacy）という単語も、憲法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、憲法修正第 1 条、修正第 4 条、修正第 5 条、そして判例法上確立された実体的デュープロセス（substantive due process）の法理から導出されると考えられている。表現の自由を保障する憲法修正第 1 条について、連邦最高裁判所は、同条が匿名表現の自由に対する保障を含むと判示している[2]。これは情報プライバシーの一形態であると言えるが、表現活動を行う団体に対し、政府がある匿名の構成員を開示するよう強制しようとする場合をはじめとして、限られた状況にしか適用されない。憲法修正第 5 条は、刑事被告人の権利を保障し、私有財産に対する保障を与えるものであるが、研究者らによれば、これもプライバシーの権利の一つとして位置づけられている。加えて、実体的デュープロセスの法理は、個 人の自律を保障するプライバシーの権利の一つとして捉えられている。異人種間婚や（ごく最近までは）中絶の権利も、実体的デュープロセスの法理により保障されていた。

情報プライバシーに最も直接関係する憲法条文は、憲法修正第 4 条である。憲法修正第 4 条は、政府による不合理な捜索及び押収等から個人を守る規定であり、刑事訴追の文脈においてよく援用されるが、他の政府関係者にも広く適用される。憲法修正第 4 条の条文は、その保障対象を「身体、家屋、書類、及び所有物」と定めているが、同条は、政府による電子データへのアクセスにも適用される。例えば、連邦最高裁判所は、政府による携帯電話の通話履歴等に対する捜索[3]、そして携帯電話の位置情報

[1] *See* Shelley v. Kraemer, 334 U.S. 1 (1948).

[2] NAACP v. Alabama ex. Rel. Patterson, 357 U.S. 449 (1958).

[3] Riley v. California 573 U.S. 373 (2014).

に対する捜索[4]に関して、これらの捜索を行う前に令状を取得しなくてはならないと判示している。この点については、以下、詳述することとする。すなわち、憲法によるプライバシーの権利の保障は、主に政府による何らかの行為に関連する場合に限定されるといえる。もっとも、州レベルでは、州憲法においてプライバシー権の権利を明示的に定める州がいくつか存在する。しかし、連邦レベルと州レベルの双方において、[訳注：ドイツの]情報自己決定権のように、強力なプライバシーの権利の保障はみられない。

1.2 連邦レベルのプライバシー法

連邦レベルでは、包括的な消費者プライバシー法やデータ保護法は存在しないが、特定の領域を対象とする数多くの法令によりプライバシー法が構成される（セクター別アプローチ（sectoral approach））。代表的な法令として、ヘルスケア領域では、医療保険の携行性と責任に関する法律（Health Insurance Portability and Accountability Act: HIPAA)、そして金融領域では、グラム・リーチ・ブライリー法（Gramm-Leach-Bliley Act: GLBA）及び公正信用報告法（Fair Credit Reporting Act）等が挙げられる。これらの法令の適用範囲は、特定の組織等に制限されていることが一般的である。HIPAA を例に挙げると、その適用範囲は、対象事業者及び業務提携者により処理される特定のデータに限定される。なお、保健福祉省（Department of Health and Human Services）は、HIPAA の条文を明確化するため、プライバシー規則を制定している。他方で、児童オンラインプライバシー保護法（Children’s Online Privacy Protection Act: COPPA）は、特定の領域に限定されず、13歳未満のすべての児童のデータに適用される。もっとも、その適用範囲は必ずしも無制限ではなく、児童から個人情報を収集又は保持していることについて「現実の認識」（actual knowledge）を有している事業者等に限定されている。

連邦政府において、プライバシー規制を主に所管しているのは、連邦取引委員会（Federal Trade Commission: FTC）である。FTC は、「通知・選択」（notice and choice）アプローチを採用している[5]。また、FTC が「不公正あるいは欺瞞的な行為、実務を用いることを禁止することができる」と定めた FTC 法第 5 条により、FTC にはプライバシー規制に関する法的権限が与えられている。プライバシーに関して、FTC は欺瞞的な行為の疑いのある企業に対し調査を実施し、「同意判決」（consent decree）と呼ばれる企業が罰金を支払い、当該行動を変更することに合意するという交渉による合意を行う（これは、事実上有罪を認めるようなものである)。同意判決書は公開され、連邦レベルのプライバシーに関して、限定的なコモン・ローを形成する。ここでは検討しないが、FTC のプライバシーに関する同意判決については、数多くの文献調査が行われている。政治的過去に関係する複雑な理由により、FTC は通常、FTC 法第 5 条による権限に基づいて規則を発行することがない。しかし、COPPA 等の別の法令により議会から権限が与えられている場合には、FTC が規則を公表することがある。

これらは、厳格な規制を受けているヘルスケアや金融をはじめとする領域以外の企業にとって、連邦政府のプライバシー法を遵守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るプライバシー・ポリシーを公表するべきであり、そのポリシーに記載した条件を守らなければならない。一般的には、そのポリシーは「ベストプラクティス」に基づいており、企業に自由を与えるような書き方がなされる。これらのポリシーが曖昧、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・ポリシーという形で「通知」し、そのポリシー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保障されていないのと同様に、連邦レベルのデータ保護法も存在しないため、連

[4] Carpenter v. United States, 138 S. Ct. 2206 (2018).

[5] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers (March 2012), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>

X.アメリカ

邦レベルのプライバシー規制においては、企業による個人データの収集・処理・移転に極めて寛容な姿勢が示されている。

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する中、最も強い影響力を持ち、最も高い水準のプライバシー保護を行っている法令は、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）というプライバシー法を改正したものであり、これらはアメリカの消費者プライバシー法における大きな転換点であると考えられている。CPRA は、カリフォルニア州で事業を運営し、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、アメリカ内の州の中で最大の人口・経済規模を誇るため、CPRA は連邦法ではないものの、その影響は極めて大きい。

CPRA は、特定の消費者の権利、すなわち、①アクセス権、②訂正請求権、③削除請求権、④情報が販売または共有される方法を知る権利、及び⑤データの第三者への移転を制限する権利を保障している。また、CPRA の下で、消費者は、企業が消費者に提供している財・サービスを提供するために必要である場合にも、当該企業が「センシティブな個人情報」を利用・開示することを制限する権利も有している。他のいかなる方法で個人情報を利用する際にも、企業は必ず同意を取得しなければならない[7]。なお、GDPR で規定されているようなデータの処理、プロファイリング、または移転に対し異議を申し立てる具体的な権利は規定されていない。

CPRA の定めるところによると、企業は、個人データの収集・利用・保持・共有について、その目的を必要かつ比例的な程度に制限しなければならない[8]。また、データ主体の合意に基づき、個人データを取得する第三者もこれらの権利や制約を尊重しなくてはならない。

[6] California Civil Code 1798.140 (d).

[7] California Civil Code 1798.121.

[8] California Civil Code 1798.100 (c).

X.アメリカ

CPRA における個人情報の定義は、次のとおりである。

「個人情報」とは、特定の消費者又は世帯を、識別し、関連し、叙述し、合理的に関連付けることができ、又は直接的に若しくは間接的に合理的にリンクさせることのできる情報を意味する。個人情報には､以下に限定されるわけではないが、特定の消費者又は世帯を識別し、関連し、叙述し、合理的に関連付けることができ、又は直接的に若しくは間接的に合理的にリンクさせることのできるものであれば、以下が含まれる。

(A) 識別子。例えば、実名、別名、郵便住所、一意個人識別子、オンライン識別子であるインターネット･プロトコル･アドレス、電子メール･アドレス、アカウント･ネーム、社会保険番号、運転免許証番号、旅券番号、又はその他の類似の識別子。
(B) 第 1798.80 条第（e）項 4 で述べる個人情報の類型。
(C) カリフォルニア州法又は連邦法のもとでの保護された分類の特性。
(D) 商業的情報。個人の財産の記録、購入、取得又は検討した製品又はサービスの記録、又は、その他の購入又は消費の履歴又は傾向についての記録を含む。
(E) 生体情報。
(F) インターネット又はその他の電子的なネットワーク活動の情報。閲覧履歴、検索履歴、及び、インターネット･ウェブサイト、アプリケーション又は広告との消費者のやりとりの情報を含むが、これに限られない。
(G) 地理位置データ。
(H) 音声、電子、視覚、温度、嗅覚、又は類似の情報。
(I) 職業又は雇用に関する情報。
(J) 公に利用可能な、家族教育権とプライバシー法（合衆国法典（「United States Code」）20、第 1232g 条； 連邦規則集（「Code of Federal Regulations」）34、パート 99）に定義されている個人識別情報ではない情報として定義される教育情報。
(K) 消費者についての選好、性格、心理的傾向、性質、行動、態度、インテリジェンス、能力及び素質を反映する消費者のプロファイルを作成するために本項で識別された情報から引き出された、推定。
(L) センシティブな個人情報。

CPRA では、一般に公開されている情報、公共の関心事、また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、アメリカのプライバシー法における最も詳細で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、他の情報から導か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。センシティブな個人情報は、GDPR の「特別な種類の個人データ」に分類されるデータに類似しているが、同時に「地理位置データ」も含んでいる[10]。

また、CPRA 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公表することを目的として、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、変更する際には同意を取得しなければならない。CPRA は、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、消費者の所在地により区別することは難しいため、多くの企業が CPRA に準拠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 からある程度示唆を得ているようであり、EU の法体系から借用した用語である「必要かつ比例的」という文言にこのことが窺える。消費者のデータを保護する義務は、データを保管する者が代わる場合にも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」（controllers）及び「処理者」（processors）といった文言は用いられていない[11]。これらの法令は、GDPR ほど包括的な規制を目指しておらず、AI 等台頭しつつある分野を明示的に規制していない（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

各国において（特にアメリカのように包括的なプライバシー法が制定されていない国や地域では）、業界の定める基準や自主規制がプライバシー保護の重要な要素となっている。そのうち、最も一般的な基準は、公正情報取扱原則（Fair Information Practices: FIPs、あるいは FIPPs とも呼ばれる）である。経済協力開発機構（OECD）が 1980 年代に公表したものが、最も頻繁に引用される[12]。なお、FTC も同様の内容の原則を公表している[13]。FIPs は、良いプライバシー（good privacy）を構成する要素に関する広範な原則あるいはガイドラインである。その原則は次の 8 つから成る。

[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>

1. 収集制限の原則。個人データの収集には制限を設けるべきであり、いかなる個人データも、適法かつ公正な手段によって、かつ適当な場合には、データ主体者（本人）に知らしめ又は同意を得た上で、収集されるべきである。
2. データ内容の原則。個人データは、その利用目的に沿ったものであるべきであり、かつ利用目的に必要な範囲内で正確、完全であり最新なものに保たれなければならない。
3. 目的明確化の原則。個人データの収集目的は、収集時よりも遅くない時点において明確化されなければならず、その後のデータの利用は、当該収集目的の達成又は当該収集目的に矛盾しないでかつ、目的の変更毎に明確化された他の目的の達成に限定されるべきである。
4. 使用制限の原則。(a) データ主体者（本人）の同意がある場合、または (b) 法律の規定による場合を除き、目的明確化の原則により明確化された目的以外の目的のために、開示・利用その他の使用に供されるべきではない。
5. 安全保護の原則。個人データは、データの紛失や不正なアクセス、破壊、使用、改ざん、開示などのリスクに対して、合理的なセキュリティ保護の措置によって保護されるべきである。
6. 公開の原則。個人データに係わる開発、運用及び政策については、一般的な公開の政策が取られなければならない。個人データの存在、性質及びその主要な利用目的とともにデータ管理者の識別、通常の住所をはっきりさせるための手段が容易に利用できなければならない。
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、合理的な期間内に、過度にならない費用で、合理的な方法で、自己に分かりやすい形で、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、その理由が与えら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。かつ
    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、修正、完全化、補正させること。
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。

研究者の間では、FIPs の有用性については議論がある[14]。しかし、多くの企業のプライバシー・ポリシーが、FIPs が示した諸原則に言及する形で作成されている。

1.5 同意とダークパターン

前述のとおり、アメリカのプライバシー法は主に「通知・選択」、あるいは本人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・インターフェースの設計において、プライバシーに関して企業の利益に有利な選択肢へと消費者を微妙に誘導する選択アーキテクチャ、あるいは行動心理学的手法が普及していることから、近年の研究においては、本人同意を効果的に行使 する上での消費者の[認知的]能力の限界に注目が集まっている[15]。このような手法は「ダークパターン」（dark patterns）として知られており、この手法は未だ広く普及していないものの、[訳注：仮にダークパターンに対応したプライバシー保護の規制が実施された場合、それは]アメリカ版の情報自己決定権となるのではないかと思われる。

[14] Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 Md. L. Rev. 952 (2017).

[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).

2010 年代やそれ以前にも、FTC は、消費者の[訳注：プライバシー・ポリシー等に対する]理解不足がインフォームド・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 の同意判決のように、FTC は FTC 法第 5 条による権限に基づき、隠れた手数料を請求したり、データ収集を行うことを明示したりしない、欺瞞的な行為を行う企業に対する執行を行ってきたしてきた[17]。しかし、FTC が正式にダークパターンに対する規制を強化することを発表したのは 2021 年のことである[18]。このような動向は歓迎すべきであるが、[訳注：ダークパターンに類似する欺瞞的な行為による]同意モデルに対する侵食は、過去 20 年以上にわたり発生してきたものであり、法的権限の不在が大きな要因となり FTC はそれを抑止できていない。

CPRA は、より強固な本人同意の要件を課すことで、ダークパターンに対処しようとしている。カリフォルニア州プライバシー保護局が提案している規則によると、本人同意は「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」でなくてはならないとされ、ダークパターンを利用してはならないことが明記されている[19]。また、本人同意を取得する際のダークパターンの利用に対処するため、追加の規制も容認している[20]。規則の草案では、本人同意が、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実行する（execute）ことが容易であること、を義務付けるとされている[21]。これに沿わないその他すべての本人同意の仕組みは、ダークパターンと見なされ得る。

FTC や CPRA による規制とは別の取組ではあるが、ある程度関係しているものとして、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なされている。忠実義務とは、企業が利用者のデータの収集・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求めるという講学上の概念である[22]。例えば、利用者情報を収集するウェブサイトは、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移転をはじめとする一部の行為もそれ自体が忠実ではないとされる。忠実義務は、新たな理論であるが、いくつかの法案に既に採用されており、同意に基づいた規制モデルの失敗を是正する試みである[23]。

2.1 執行

前述のとおり、FTC は一般的な消費者プライバシーの執行機関であり、セクター別のプライバシー法については各領域の機関がその所管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る。同意判決とは、FTC が一定期間にわたり企業の商慣行に様々な条件を課すものである（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差し控える等）。企業は一般的にこれら

---

[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] これらの事例については、以下のリンクを参照。<https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3202-effen-ads-llc-icloudworx> ;< 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-trickor -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).

[23] *See* the Data Care Act of 2021. <https://www.congress.gov/bill/117th-congress/senate-bill/919> なお、マサチューセッツ州では、忠実義務の考え方を取り入れたプライバシー法案が提出されている。<https://malegislature.gov/Bills/192/HD2664>

の合意において罪あるい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、さらには同意判決の期間を延長することもできる。FTC は、同意判決の前に非公式の調査を実施し、違法行為の証拠が十分にある場合には訴訟を提起することもある。もっとも、それらほとんどは和解され、同意判決という結果に至っている[24]。

州レベルでは、CPPA による規制の執行が 2023 年 7 月 1 日に開始されたが、近時の判決がそれを 2024 年 3 月 29 日まで延期している。しかし、州司法長官事務所は、既に発効している CCPA や CPRA の古い規定を執行している[25]。同事務所による執行は、FTC と同様の方法で運用されており、ほとんどが和解に至っている。一部の市や自治体では、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]、ここではそれらの取り組みは取り上げない。

2.2 司法手続き

前述のとおり、政府によるプライバシー法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訴も珍しいが、稀にみられる。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、これらは私訴を容認していない[27]。私訴を容認している法令の場合でも、本稿では取り上げきれないほどの様々な個別の課題があるため[28]、本稿では一般的な課題に言及する。この種の訴訟における主要な障害の一つが、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仲裁を優先し、訴訟を禁止している点である。これは個別の訴訟だけでなく、集団訴訟も禁じている。さらに、プライバシー関連の訴訟における損害は、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、各州が独自の民事訴訟手続規則やコモン・ローの法体系を有しているため、さらに複雑である。さらに、本稿執筆時点[訳注：2023 年]では、9 の州が独自の包括的な消費者プライバシー法を制定しているが、それぞれ私訴の取扱いは異なっている。ウォレンとブランダイスが 1890 年に示したコモン・ローにおけるプライバシー侵害[29]は、州法上広く認められているが、この法的構成により勝訴することは困難であり、一般的には、デジタル時代のプライバシー保護のための効果的な手段ではないと考えられている。CCPA や CPRA は、データセキュリティに関する事案に対し、損害賠償や私訴権を規定しているが、他の条項についてはこれらの規定はない。その執行は、州司法長官事務所に委ねられている。なお、カリフォルニア州の他のプライバシー法、例えば州の医療記録プライバシー法等は、私訴を容認している[30]。

謝辞：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。

[24] Daniel J. Solove, Woodrow Hartog, The FTC and the New Common Law of Privacy, 114 Colum. L. Rev. 583, 610 (2014).

[25] 州司法長官事務所は、CCPA の執行事例のリスト (https://oag.ca.gov/privacy/ccpa/enforcement) 、及びプライバシー全般に関する執行事例の リスト (https://oag.ca.gov/privacy/privacy-enforcement-actions)を公表している。

[26] Ira Rubinstein, *Privacy Localism*, 93 Wash. L. Rev. 1961 (2018).

[27] 連邦のプライバシー法の中で最も「強力」である HIPAA は、私訴を容認していない。

[28] 一例を挙げると、連邦政府に対するスパイ行為やデータへのアクセスについて、盗聴法（Wiretap Act）及び電子通信の保存に関する法律（Stored Communications Act）に基づき、請求権を容認する連邦レベルの訴訟も存在する。

[29] Samuel D. Warren, Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

[30] California Civil Code 1798.150.