



Title	個人情報の刑法的保護の可能性と限界について
Author(s)	佐藤, 結美
Degree Grantor	北海道大学
Degree Name	博士(法学)
Dissertation Number	甲第11183号
Issue Date	2014-03-25
DOI	https://doi.org/10.14943/doctoral.k11183
Doc URL	https://hdl.handle.net/2115/55424
Type	doctoral thesis
File Information	Yumi_Sato.pdf



平成25年度 北海道大学大学院法学研究科

博士学位請求論文

「個人情報の刑法的保護の

可能性と限界について」

佐藤結美

目次

第1章 はじめに

第1節 問題の所在

第2節 研究方法

第2章 日本法における個人情報保護の現状

第1節 秘密漏示罪

第2節 信書開封罪

第3節 支払用カード電磁的記録不正作出準備罪

第4節 不正指令電磁的記録に関する罪

第5節 不正アクセス禁止法

第6節 個人情報保護法

第1項 成立過程と概要

第2項 罰則の方式に関する議論

第1款 個人情報保護検討部会の議論

第2款 個人情報保護法制化専門委員会の議論

第7節 小括

第3章 イギリス法における個人情報保護

第1節 1998年データ保護法の概要

第1項 基本事項について

第2項 データ保護原則 (Data Protection Principle) について

第3項 罰則について

第1款 データ保護原則の違反

第2款 個人データの不法取得等の罪

第2節 個人データの不法な取得等に対する直接罰規定について

第1項 1998年データ保護法55条の成立まで

第2項 55条違反の犯罪の主観的要素

第3節 情報コミッショナーによる個人情報保護の現状について

第1項 報告書「プライバシーの価値とは何か? (What price privacy?)」

第2項 第2報告書「続・プライバシーの価値とは何か? (What price privacy now?)」

第3項 制裁金について

第4節 センシティブな個人データ (sensitive personal data) に関する法的規制

第1項 センシティブな個人データに含まれるデータについて

第2項 データの取り扱いの条件

第5節 小括

第4章 フランス法における個人情報保護

第1節 1978年情報処理・情報ファイル及び諸自由に関する法律の概要

第1項 基本事項について

第2項 情報処理・全国自由委員会（CNIL）

第3項 刑法典における処罰規定

第2節 刑事罰について

第1項 詐欺的・不誠実・不正な手段による情報収集の罪（刑法226-18条）

第2項 市場調査等のための情報処理の罪（刑法226-18-1条）

第3項 センシティブ情報の入力・保存の罪（刑法226-19条）

第1款 刑法226-19条・1978年法8条の成立過程と憲法院判決について

第2款 226-19条の罪の成立要素について

第4項 本人への敬意・私生活の内奥を侵害する情報漏洩の罪（刑法226-22条）

第3節 CNILによる制裁について

第1項 CNILによる制裁の実態

第2項 CNILの制裁と刑事罰

第4節 小括

第5章 ドイツ法における個人情報保護

第1節 連邦データ保護法の概要

第1項 基本事項について

第2項 個人データの収集・処理・利用の適法化要件

第3項 連邦個人データ・情報自由保護観察官（連邦監察官）

第4項 監督官庁

第5項 過料と刑事罰

第2節 データ保護法における過料と刑事罰について

第1項 過料

第1款 客観的な成立要件

第2款 主観的な成立要件

第2項 刑罰

第3節 監督官庁による規制の実態

第1項 監督官庁の位置づけ

第2項 監督官庁による過料・刑罰

第1款 シュレースヴィヒ=ホルシュタイン州

第2款 ザールラント州

第3款 過料・刑罰に対する監督官庁の姿勢

第4節 小括

第6章 保護法益としての個人情報と規制方法

第1節 個人情報の法益性

第1項 現行法における他の保護法益への不可包含性

第2項 憲法上の価値から導出される保護法益としての個人情報

第2節 個人情報の侵害に対する妥当な規制のあり方

第1項 第三者機関による監視の可能性

第1款 共通番号法成立前の第三者機関に関する議論

第2款 特定個人情報保護委員会

第3款 第三者機関による金銭制裁の可能性

第2項 刑事規制の可能性

第1款 イギリス・フランス・ドイツの刑罰規定の特徴

第2款 イギリス・フランス・ドイツにおける第三者機関の実務の特徴

第3款 妥当な刑罰規定の在り方、金銭制裁と刑罰の役割分担

第3節 小括

第7章 おわりに

第1章 はじめに

第1節 問題の所在

本論文では、個人情報そのものを刑法における保護法益として捉えることが可能であるか、そして、個人情報保護法益たり得るとすれば、どのような保護が妥当であるかということについて検討する¹。「個人情報保護」の重要性は誰もが賛同するものであるが、個人情報保護の妥当な在り方については明確な方針が定まっていらないようである。氏名や住所などの個人情報が漏洩する事件が繰り返し発生している一方で、「個人情報保護」を理由とした過度の情報の秘匿などといった「過剰反応」も見られる。このように、個人情報を取り巻く状況は二極化している。日本の個人情報保護法制において、どのような情報がどのように保護されるべきなのか、情報の取り扱いがどのように規制されるべきなのかということについての議論が曖昧で不十分だからではないだろうか。

では、日本の現行法において個人情報はどの範囲で保護されているのか。例えば、刑法134条の秘密漏示罪は、「医師、薬剤師、医薬品販売業者、助産師、弁護士、弁護人、公証人又はこれらの職にあった者」と「宗教、祈祷若しくは祭祀の職にある者又はこれらの職にあった者」が「正当な理由」なく「その業務上取り扱ったことについて知り得た人の秘密を漏らした」場合に処罰するという方法により、限定された状況下での個人情報の保護を行っている。刑法134条の秘密漏示罪以外にも、特別法によって様々な職業の者についての刑罰を伴う守秘義務が規定されており、個人の「秘密」は広く保護されているように見える。しかし、何らかの方法によって守秘義務者から秘密を知った第三者がそれを他人に漏らし、その結果個人に不利益がもたらされたとしても、刑法134条等に規定されている主体ではない以上、処罰することはできない。

続いて、2003年に制定された個人情報保護のための一連の法律は公的部門と私的部門に分けられ、後者の個人情報取扱事業者については個人情報に関する義務違反行為を直

¹従来の先行研究では、財産的な性質を有する情報の保護について議論が行われてきた。そのような情報の一例として、営業秘密の刑罰的保護という問題も興味深いテーマではあるが、本論文で扱う対象は個人情報に限定する。

営業秘密の刑罰的保護についての代表的な研究としては、加藤佐千夫「刑事罰による営業秘密の保護と不正競争防止法の変遷」中京法学44巻3・4号（2010年）263～289頁、「企業秘密の刑罰的保護（1）（2）」名古屋大学法政論集116号（1987年）207～242頁、117号（1987年）283～316頁、「企業秘密の刑罰的保護・再論—財産犯的構成の批判的検討を通して」名古屋大学法政論集127号（1989年）107～131頁、山口厚「営業秘密の侵害と刑事罰」ジュリスト962号（1990年）45～51頁、「営業秘密の刑事罰による保護」NBL820号（2005年）12～18頁、佐久間修『刑法における無形の財産の保護—企業秘密、コンピュータ・データを中心として—』（成文堂・1991年）、一原亜貴子「不正競争防止法による営業秘密の刑事法的保護」商学討究56巻2=3号（2005年）279～301頁、「営業秘密侵害罪の保護法益」商学討究59巻4号（2009年）165～197頁、「営業秘密侵害罪に係る不正競争防止法の平成二一年改正について」岡山大学法学会雑誌60巻3号（2011年）477～494頁などがある。

接的に処罰するという方法ではなく、主務大臣の命令に違反して初めて処罰されるという間接罰方式を採っている。

個人情報保護法における「個人情報」の定義は幅広く、様々な情報を含んでいることから、個人情報に関する義務違反行為を一律に直接的に処罰する方式を採らなかったことは、その限りでは了解可能な帰結であると思われる。しかし、「個人情報」と一口に言っても、氏名・住所・電話番号・生年月日といった基本的な情報から、職業・年収・信用情報・学歴・趣味嗜好といった、個人の人格に関わるような情報まで多岐にわたっているのも、そのような情報の性質によって保護の在り方が異なると考えられる。また、個人情報保護法における個人情報取扱事業者の義務も多岐にわたっており、情報の利用目的の明確化や情報の不正取得の禁止、情報管理や従業員の監督といった様々なものがある。このように、個人情報保護法が間接罰の対象とする「個人情報保護における義務違反についての主務大臣の命令に対する違反」という行為の範囲も幅広いものになっていることから、重要性の低い情報に対する比較的軽微な侵害も、重要性の高い情報に対する重大な侵害も一律に、主務大臣の命令とその違反に対する罰則という扱いを受け得ることになり、均衡を失するのではないかと考えられる。

以上のように、日本の現行法は個人情報を重要なものとして保護する姿勢を採りつつも、保護の仕方が断片的であり、個人情報そのものを保護法益とするという考え方には至っていないと思われる。一般法であるはずの個人情報保護法も、情報の性質や重要性、情報侵害の行為態様に着目することなく、「個人情報保護における義務違反」「主務大臣の命令に対する違反」という抽象的な概念によって情報侵害を規制しようとしているので、個人情報の漏洩や売買といった問題に対して効果的に対処することが困難になっている。

昨今では、企業による個人情報の大規模な流出事件が多発しており、個人情報の流出・漏洩自体による直接的な被害の他、漏洩した情報が他の犯罪に利用されるといった二次被害の発生も否定できない。情報漏洩について、企業が損害賠償責任を負うケースも見られるが、損害賠償を課され得るという可能性が、どの程度の抑止力になっているのかという疑問がある²。

このように、日本の現行法には情報の漏洩や窃盗などを直接的に処罰する規定は存在しないが、情報の売買や窃盗といった不正な取り扱いを処罰するための試みとして、情報の不正収集を財産犯によってカバーするという考え方が判例によって提唱されている。

まず、大日本印刷事件³は、被告人が稟議決裁一覧表の原本を社内で借りて、これを会社

²今井猛嘉「刑法における情報の保護」『刑法の争点（新・法律学の争点シリーズ2）』（2007年）163頁も、個人情報が刑法典における保護の対象となっていないという立法の在り方は、①個人情報やプライバシーの価値が十分に議論されていなかったこと、②個人情報に対する重大な侵害が想定できなかったことに由来しているものの、現在ではインターネット等を通して、民事的制裁では対応しきれない重大な侵害が容易になされ得るので、新たな検討が必要であると述べている。

³東京地判昭和40年6月26日判時419号14頁。

のコピー用紙に複写して、そのコピー用紙を持ち出した行為が、窃盗罪に問われた事案である。東京地裁は、「当初からの意図のとおり大日本印刷内で、ほしいままに、同社の機密書類を同社所有のコピー用紙に同社の複写機を使って複写し、これを社外に持ち出したものであるから、全体的にみて、単なるコピー用紙の窃取ではなく、同社所有の複写した右稟議決裁一覧表を窃取したものと認めるのが相当である」として、コピー用紙について財物性を認めている。コピー用紙それ自体の財物としての価値は低いので、コピー用紙の窃盗であれば可罰的違法性が否定されるはずであるが、情報を入手するという被告人の意図が重視されている。

続いて、新薬産業スパイ事件⁴は、製薬会社の幹部が他の会社の新薬開発研究の成果を不正に入手するために、別の製薬会社の代表取締役社長と顧問が、それぞれ国立予防衛生所の厚生技官に、秘密資料を持ち出させてコピーを採らせ、もとの場所に戻させたというものである。東京地裁は、「情報の化体された媒体の財物性は、情報の切り離された媒体の素材だけについてではなく、情報と媒体が合体したものの全体について判断すべきであり、ただその財物としての価値が、主として媒体に化体された情報の価値に負うもの」であるとして、コピー用紙に財物性を認めている。

このように、判例は「情報窃盗」といえる行為を処罰するために、情報の化体された媒体に財物性を認めて、これに対する窃盗を認めているが、学説はこのような判断に対して、可罰的違法性の理論でいえば単なる紙の窃盗は不可罰となることと矛盾する、と批判⁵している。情報は他の財物や財産上の利益と異なり、移転しないということと、他人に情報を入手されたとしても、情報の持ち主がその情報を失うわけではないという特殊性⁶があることから、財産犯の枠組みで保護するのは困難であると考えられている。

判例は窃盗罪以外にも、横領罪・背任罪の枠組で情報をカヴァーすることを試みている。まず、横領罪の成否が問題となった事件に、新潟鉄工事件がある⁷。この事件は、新潟鉄工の社員が、会社内において自分で保管していた秘密資料を、退職後に新しい会社で利用するためにコピーを作成しようと考え、社外に持ち出してコピーをした後、元に戻しておい

⁴東京地判昭和59年6月28日判時1126号6頁。

⁵藤木英雄「産業スパイと刑事責任」ジュリスト428号（1969年）34～35頁。

⁶西田典之「財産的情報の刑法的保護—共同研究の基本的視点とまとめ—」刑法雑誌30巻1号（1989年）6頁。また、キャッシュカードの暗証番号を脅迫により聞き出す行為につき2項強盗罪の成否が争われた事件の原審さいたま地川越支判平成20年6月1日（公刊物未搭載）においても、刑法236条2項の「財産上不法の利益」は移転性のある利益に限られるが、被告人がキャッシュカードの暗証番号を聞き出したとしても、暗証番号に関する情報が被告人と被害者との間で共有されるだけで、被害者から失われるわけではないと判断され、このような情報の非移転性と非喪失性を根拠に、236条2項における利益性が否定される結果となった（なお、2審の東京高判平成21年11月16日判タ1337号280頁では、情報の非移転性と非喪失性という性質そのものについては特段の言及をせず、被告人はキャッシュカードと暗証番号を併せ持つことによって預貯金を引き出し得る地位を得たとして、2項強盗罪の成立が肯定された）。

⁷東京地判昭和60年2月13日刑事裁判月報17巻1＝2号22頁。

たというものである。

この事案につき裁判所は、「内容自体に経済的価値があり、所有者以外の者が許可なくコピーすることの許されない機密資料をコピー目的で許可なく持ち出す行為には、その間の所有者を排除して資料を自己の所有物と同様にその経済的用法に従って利用する意思が認められ、使用後返還する意思があったとしても、不法領得の意思が認められる」として横領罪の成立を認めた。このような判断には、伝統的な判例・学説はいわゆる「使用窃盗」につき不法領得の意思が欠けるので窃盗罪は成立しないと解してきたのであるから、会社の機密資料を持ち出して別の会社に売るなどの行為をせず、コピーしてすぐに戻した事案には不法領得の意思を認めることができず、窃盗罪や横領罪は成立しないのではないかという批判⁸がある。

そして、背任罪の成否が問題となったものとして総合コンピュータ事件⁹がある。この事案は、コンピュータ・ソフトウェアの開発販売等の会社に勤務する被告人が、会社が新聞販売店用に開発した購読者管理システムのプログラムを同社の顧客である新聞販売店に設置されるコンピュータに入力して、その使用方法について技術指導するなどの業務を行っていたが、会社は無断で、ある新聞販売店と契約し、そのコンピュータにプログラムを入力して、プログラム代金を受け取ったというものである。この事案は資料の持ち出しの場合とは異なり、会社のプログラムを入力しただけであるので、窃盗罪も横領罪も成立し得ない。そこで、裁判所は被告人の行為につき、「プログラムの入力使用等に当たっては、同社が業務として同社の顧客方に設置するオフィスコンピューターに対してのみ、右フロッピーシートを使用するなど、同社のために忠実にその業務を遂行すべき任務があった」として、任務違背行為により背任罪が成立すると判断した。このような判断には、当該情報の管理を業務としていない一般社員であった被告人は今回の事案における背任罪の主体にはなり得ないという批判¹⁰がある。

これらの判例は、学説からの批判はあるものの、情報が紙やフロッピーといった有体物に化体されているケースの解決としては、一定程度の意義を有している。しかし、有体物に化体されていない情報を不正に収集等する行為についてはカバーすることができないという点で限界がある。以上のことから、従来の刑法の解釈によって個人情報それ自体の窃盗や漏洩などの処罰可能性を捕捉するのは困難である。そして、当該個人情報の重要性和侵害態様の強度によっては、主務大臣の命令に反して初めて刑罰を科されるという間接罰方式ではなく、直接罰方式による処罰の必要性があると思われる。したがって、本論文では、個人情報を保護する刑事罰の可能性と限界について議論を進めることによって、個人情報の侵害に対する妥当な規制方法について検討する。

⁸佐伯仁志「刑法による情報の保護」宇賀克也・長谷部恭男（編）『改訂版 法システムⅢ—情報法—』（放送大学教育振興会・2006年）202頁。

⁹東京地判昭和60年3月6日判時1147号162頁。

¹⁰佐伯・前掲注（8）204頁。

第2節 研究方法

本論文では、刑事罰を視野に入れつつ、個人情報の侵害に対する妥当な規制方法について検討するために、個人情報（データ）の不正な取り扱いを直接的に処罰する規定と、その他の規制方法（第三者機関による規制）を有する外国法の議論を参照する。まず第2章では、日本の現行法における個人情報保護の現状について概観することによって、現行法において個人情報の保護が不十分な領域を確認する。

続いて、第3章では、イギリスの1998年データ保護法について扱う。イギリスのデータ保護法には、個人データの漏洩・窃盗などを直接処罰する規定が存在し、不正な取り扱いをした者が処罰の対象となる。第4章では、フランス刑法における個人情報保護の規定と、情報処理・情報ファイルおよび諸自由に関する1978年の法律について扱う。フランス刑法には個人情報の様々な侵害行為が設けられており、1978年法において、第三者機関が個人情報の不正な取り扱いを規制することが定められている。

第5章では、ドイツ連邦データ保護法について扱う。ドイツ連邦データ保護法は、個人データを扱う機関が、違法または不当なデータの収集・処理・利用によって本人に損害を与えた時に、損害賠償の責任を負うことを規定している。この他に、故意または過失による個人データの様々な侵害行為は過料の対象になり、対価を得て、又は図利他害目的で個人データ侵害行為をした場合には、刑事罰の対象になることが規定されている。

第3章から第5章までは、比較対象としてイギリス・フランス・ドイツの法律を扱うが、この三国は個人情報（データ）の保護のために、直接の刑事罰以外にも第三者機関による監視といった刑罰以外の規制手段が講じられている点で共通している。そして、個人情報（データ）の中でも特に機密性の高い「センシティブ情報」という概念を別個に設けて、「センシティブ情報」の取り扱いを他の一般的な情報と区別している点も共通している。日本の個人情報保護法が「個人情報」の重要性によって情報の取り扱いを区別せず、個人情報の侵害行為につき直接罰ではなく間接罰で臨んでいることに比して、この三国では個人情報の多様な保護の方法が採られているが、これらの外国法の規定をそのまま日本法に導入することが妥当ではないことは論を俟たない。そこで、第3章から第5章において、英仏独の個人情報保護法制における処罰規定についての判例・学説・第三者機関による報告について触れ、各国において刑罰や第三者機関による規制がどの程度功を奏しているのかを検討する。

そして第6章では英仏独の議論を参照しつつ、（1）保護法益としての「個人情報」の定義と範囲、（2）英仏独における「センシティブ情報」のような法概念を取り入れるべきか否か、取り入れるとすればどのように定義するかということ、（3）個人情報の侵害の行為態様はどのようなものかということ、（4）個人情報の不正収集・利用等を直接処罰する必要性と、その条件という観点から、個人情報の侵害に対する妥当な規制方法を検討する。

第2章 日本法における個人情報保護の現状

第2章では、日本の現行法の枠組みにおいて、個人情報や秘密がどの程度保護されているかということについて整理する。

第1節 秘密漏示罪

まず本節では、刑法134条の秘密漏示罪について扱う。

前述の通り、医師や弁護士などの、限定された職業の者が業務上知り得た人の秘密を正当な理由なく漏らす行為は秘密漏示罪にあたるものとして処罰される。その事実の内容を広く知られていないことと、本人が当該事実を秘匿する意思を有していること、それを秘匿する利益¹¹が本人にある場合に、当該事実が秘密であると判断される。秘密の内容がどれほど重要なものであるとしても、134条所定の身分の者が漏示した場合でなければ処罰の対象とはならない。また、刑法134条に規定されていなくとも、国家公務員や看護師などの特定の職業の者が有する守秘義務についても、各々の職業に関する法律において規定されている¹²。

このように、個人の秘密や情報を取り扱う機会のある職業の多くは、刑法や他の関連法規によって刑罰を伴う守秘義務を付与されているので、日常生活の様々な局面において、個人の秘密や情報は幅広く保護されているように見える。その一方で、秘密漏示罪に関連して、守秘義務の身分を持たない者による個人情報・秘密の公表が問題になり得るケースとして、最決平成24年2月13日刑集66巻4号405頁がある。

この事案は、精神科医である被告人が、現住建造物等放火・殺人等の少年Aの保護事件につき、家庭裁判所から少年の精神鑑定を命じられてその作業を進める中、ジャーナリストCから取材を受け、その要求に応じて少年事件記録の写しや鑑定書等を閲覧させるなどしたことについて、刑法134条の秘密漏示罪が成立すると判断されたものである。本件においては、Cが被告人から入手した情報を基にして書籍を出版したことから、少年の事件やAと実父Bとの関係といった家庭環境がさらに広く知られるところとなった。

まず、被告人の行為についての争点と裁判所の判示について見て行くこととする。本件において、被告人と弁護人は、被告人がCに情報を提供したという外形的事実を認めたものの、①少年の鑑定人であった被告人は本罪にいう「医師」にあらず、医師である鑑定人が行う場合でも、鑑定は本罪にいう「業務」に当たらない、②被告人は少年の利益を図るため、Cの行う取材に対する協力としてCに供述調書等を閲覧させたのであるから、その目的は正当であり、手段も相当であるから、被告人の行為には「正当な理由」があり、違法性が阻却される等と主張した。

¹¹山口厚『刑法各論（第2版）』（有斐閣・2010年）132頁など。

¹²国家公務員法100条には、「職員は、職務上知ることのできた秘密を漏らしてはならない。その職を退いた後といえども同様とする」と規定されており、保健師助産師看護師法42条の2、地方公務員法34条1項などにも同様の規定がある。

第1審（奈良地判平成21年4月15日刑集66巻4号440頁参照）は以下のように判示して、被告人につき懲役4月執行猶予3年の有罪判決を下した。

①「刑法134条1項が秘密漏示の主体として掲げる『医師』とは、医師国家試験に合格し、厚生労働大臣の免許を受けた者（医師法2条）をいうものと解されるところ、被告人がこの『医師』に当たることは……明らかである。……本罪の主体として掲げられている者は、弁護人が指摘するように、秘密の主体である相手方との信頼関係に基づき、相手方が自ら打ち明けたことによってその秘密を知るのが通常だといえるが、業務上取り扱ったことについて人の秘密を知り得たのであれば、相手方に意思能力がない場合や業務上必要な調査を行う過程で取得した内容がその相手方の秘密に当たる場合等、相手方の意思、相手方との信頼関係の有無や程度等にかかわらず、正当な理由がない限りその秘密を漏らすことは違法である」として、被告人が刑法134条1項にいう「医師」であることを肯定した。

続いて、被告人が行った精神鑑定の業務性については、「その免許を前提に、専門的知見及び経験に基づき継続的に行う事務に関して人の秘密を取り扱えば、『その業務上取り扱った』ものと解することができる……そうすると、被告人がAについて行った精神鑑定は、本罪における医師の『業務』に当たる」と判断した。

さらに、被告人が閲覧させた供述調書等の秘密性については、以下のように判断する。

②「本罪が個人の私生活上の秘密を保護法益とするものであることからすれば、本罪における『秘密』とは、一般に知られていない非公知の事実であって、これを他人に知られないことが本人の利益と認められるものをいう」という一般論を提示した上で、本件について、「本件保護事件は、少年事件として審判手続が進められているさなかにあり、Aに対する審判結果も出されていなかったこと……からすれば……本件……各書面……については、その存在及び内容が一般には知られていなかったものと認められる」として、事実の非公知性を肯定する。その上で、「各書面は、A、Bの家庭内に関する諸事情、Aの生育歴や学校の成績、Aの精神状態を判断するために行われた各種心理検査の結果やその所見、精神鑑定の内容となるAの家族歴、本人歴や症状、診断等いずれもAやBのプライバシーに極めて深くかかわる個人的な事項を内容とするものであるから、これらは、一般的にみて何人も他人に知られることを欲しない事項といえ、他人に知られないことがA及びBにとって利益である」として、供述書類等が本罪にいう「秘密」にあたることを認めた。

そして、被告人がCに書類を閲覧させたことに「正当な理由」があったか否かについては以下のように判示している。

「被告人は、AやBに関する報道内容に疑問を持っており、Aに殺意がないことを対外的に明らかにしたいとの思いを抱いていたことは認められる。しかし、被告人は……自らが抱く問題意識や考え方を明確に示した上で、Cにその報道を求めたり、記事に関する提案を行ったりすることはなく、Cが自分の意図を理解し、誤った報道を正してくれると思っていたにすぎないのであり……被告人が抱く前記のような思いは、主観的なものにとどまって

いた」と述べている。また、「被告人は、A の鑑定人としての立場にありながら……本件事件記録を、自ら立ち会わず、対象も何ら限定なしに C らに自由に閲覧させ、さらには、解説書面や心理検査の結果等の書面を閲覧謄写させたり、鑑定書と同等の写しを交付したりしたのであって、被告人が抱いていた……思いは、その立場と相いれず……A の利益にかなうものとはいえないばかりか……A 及び B のプライバシー等の秘密に対する配慮を欠いた、非常に軽率な行為」であるとして、手段の相当性も否定する。

本判決は、被告人に係る「正当な理由」の有無について、「取材に応じ、あるいはこれに協力する者の行為が秘密漏示罪に該当するか否かの判断に当たっては、取材協力であることから直ちにその違法性が阻却されると考えるべきではなく、取材行為の目的、手段及び方法に係る正当性、取材協力行為を行った者の立場、目的、同行為の態様等と、漏示対象となる秘密の内容や秘密の主体が受ける不利益を具体的に考慮」すべきであると判示した上で、前述のように、A の利益を図りたいという被告人の思いが主観的なものとどまっていることと、C に書類を閲覧させる手段の相当性を欠いていることから、被告人の行為には「正当な理由」がないと判断した。

第1審の有罪判決に対して、被告人は控訴したが、第2審（大阪高判平成21年12月17日刑集66巻4号471頁参照）も被告人の主張を斥けて控訴を棄却したので、最高裁に上告した。

最高裁は、被告人がA及びBから鑑定を委託されていないことから、被告人の精神鑑定はあくまでも「鑑定人の業務」であって、本罪において規定される「医師の業務」にあたらないとする被告人側の主張に対して、「医師が、医師としての知識、経験に基づく、診断を含む医学的判断を内容とする鑑定を命じられた場合には、その鑑定の実施は、医師がその業務として行うものといえるから、医師が当該鑑定を行う過程で知り得た人の秘密を正当な理由なく漏らす行為は、医師がその業務上取り扱ったことについて知り得た人の秘密を漏示するものとして、刑法134条1項の秘密漏示罪に該当する」と判示し、被告人の上告を棄却した。

本件では、刑法134条1項の主体のひとつである「医師」に、精神鑑定人としての医師が含まれるか、秘密の主体から委託を受けていない精神鑑定は本罪にいう「業務」といえるか、被告人の行為には「正当な理由」があったか否かが争われた。本罪の保護法益を（団体、法人等も含む）個人の秘密とする観点から、法益侵害が認められるためには個人の秘密が134条所定の主体によって漏示されれば足り、秘密の主体と漏示の主体との間に特別の依頼関係や信頼関係は不要であるとして、第1審につき、被告人は134条所定の「医師」であり、精神鑑定が本罪の「業務」にあたると判断した点を肯定する見解がある¹³。改正刑法草案317条は、秘密漏示罪の主体を「依頼者との信頼関係に基づいて人の

¹³松宮孝明「判批」立命館法学337号（2011年）1694頁。豊田兼彦「判批」新・判例解説 Watch 刑法 No.71も同旨。柑本美和「精神医療の実行における守秘義務と情報共有—『僕はパパを殺すことに決めた』事件を題材に—」町野朔・岩瀬徹・日高義博・安

秘密を知ることとなる業務に従事する者」と規定していたが、信頼関係の有無について明言せず、医師や弁護士といった特定の職業の者を主体として限定列举する現行134条の条文に照らすと、特段の信頼関係や委託関係がないからといって、本件被告人を134条の主体にあたらず、精神鑑定は本罪の「業務」にあたらないと判断する理由はないだろう。

次に、本判決は被告人の手段の相当性が欠如しており、それによってAやBの利益が侵害されたことを根拠に「正当な理由」を否定している。この点については、少年審判の制度趣旨という観点から、違法性阻却は困難であるとする見解が多い¹⁴。

医師などの守秘義務の身分を有する者による秘密漏示行為については、判例では「正当な理由」の有無について目的・手段の相当性や利益衡量の観点から検討がなされ、妥当な解決が図られているように思われる。しかし、その一方で本件事案では、守秘義務の身分を持たないジャーナリストであるCによる個人情報・秘密の公開という問題が残されている。秘密漏示罪は、秘密を漏示される相手方の存在を必要とする必要的共犯（片面的対向犯）であるので、相手方が処罰されることはない。この点につき、本罪は人の秘密を扱う職業の者に漏示禁止義務を課すことで秘密を保護するものであるという理由から、たとえ相手方が積極的に漏示をそそのかしたとしても相手方は処罰されないとする見解がある¹⁵。他方、相手方が犯罪の成立に欠くことのできない関与行為をした場合は処罰されないということから、秘密を知っただけでは秘密漏示罪の成立に欠くことのできない関与行為に留まるので処罰されないが、自己に漏示するように教唆した場合には、秘密漏示罪の教唆または幫助として処罰されるという見解も主張されている¹⁶。本件のCも「身分なき共犯」として告訴されたが、嫌疑不十分で不起訴処分となっていることから、Cのように守秘義務保持者に積極的に漏示を働きかけたり要求したりする者は共犯として処罰される可能性もあると思われる。しかし、Cは被告人に対し秘密漏示を要求するのみならず、被告人から得た供述調書等をもとに書籍を出版することによって、AやBの秘密や個人情報を広く公表していることから、書籍出版行為は新たな法益侵害といってもよい。書籍出版によって秘密を漏らす行為は名誉毀損罪でカバーすることも可能であろう。しかし、広く秘密を公表するという行為にまで至らなくとも、秘密漏示罪が相手方の不特定多数であることを要求していないことに鑑みれば、守秘義務者から秘密を得たCのような立場の者が、例えば少数の相手方であっても他の者に秘密を漏示すれば、そのような行為も新たな法益侵害と

部哲夫・山本輝之・渡邊一弘（編）『刑法・刑事政策と福祉 岩井宜子先生古稀祝賀記念論文集』（尚学社・2011年）174～175頁も、秘密提供者と医師との信頼関係に基づいてやり取りされた秘密のみを本罪の保護の対象とすることは、診察以外にも医師の業務の範囲が拡張されている現状に鑑みると、人の秘密の保護としては不十分であると述べている。

¹⁴ 澁谷洋平「判批」年報医事法学25号（2009年）158頁、松宮・前掲注（13）1699頁、田坂晶「判批」刑事法ジャーナル33号（2012年）134～135頁、澁谷洋平「判批」判例セレクト2012〔I〕（法学教室389号別冊）37頁。

¹⁵ 松宮・前掲注（13）1703頁。

¹⁶ 平野龍一『刑法総論Ⅱ』（有斐閣・1975年）379頁。

なると考えられる。このように、現行の秘密漏示罪には、法定された守秘義務者ではない相手方がさらなる漏示行為を行った場合をカバーできないという点で、解釈では埋めることのできない処罰の間隙がある。

第2節 信書開封罪

刑法133条では、封をしてある信書を正当な理由なく開ける行為が処罰される。信書を「開ける」というのは、封を破棄して信書の内容を知り得る状態を作り出すことであり、信書を実際に読んだり、信書の内容を探知したりすることまでは要しないと解されている¹⁷。本罪の法的性質については、①個人の秘密に対する抽象的危険犯であるとする見解¹⁸に対して、②「封をしてある信書」という秘密の形式、または「信書が勝手に開かれない利益」に対する侵害犯であるとする見解¹⁹も主張されている。後者の立場を採れば、信書の内容が秘密である必要はなく、信書の内容が単なる事務的な連絡事項であったとしても、信書の封を開けた時点で既遂に達することになる。

続いて、信書開封罪における「信書」は個人のものに限るか否かが争われている。本罪が個人的法益犯罪であるという見地から、国・地方公共団体相互間の信書を除外すべきとする見解²⁰がある一方で、信書の内容を秘匿する利益は個人のみならず、法人や国・地方公共団体も享受し得るとする見解²¹もある。いずれの見解を採ったとしても、国・地方公共団体と個人との間でやり取りされた信書であれば、その内容は個人情報を含むものといえると考えられるので、本罪は信書であるという条件のもとで個人情報を保護する犯罪類型であるといえる²²。さらに、本罪は信書を開封することによって成立する犯罪であることから、秘密漏示罪とは異なり、信書の内容については、信書の関係者にとって秘密にしておくことに利益のある内容であることといった制限がない。その意味において、信書という範囲内において、個人の秘密や情報が幅広く保護され得るが、本罪がカバーするのは信書の

¹⁷西田典之『刑法各論（第6版）』（弘文堂・2012年）106頁。

¹⁸大塚仁『刑法概説（各論）（第3版増補）』（有斐閣・2005年）127頁、大谷實『刑法講義各論（新版第3版）』（成文堂・2009年）149頁、曾根威彦『刑法各論（第5版）』（弘文堂・2012年）83頁など。

¹⁹松宮孝明『刑法各論（第3版）』（成文堂・2012年）139頁、山口・前掲注（11）137頁。

²⁰大谷・前掲注（18）148頁、西田・前掲注（17）105頁。

²¹山口・前掲注（11）130頁。

²²時武英男「刑法におけるプライバシーの保護」中山研一・西原春夫（編）『現代刑法講座第4巻 刑法各論の諸問題』（成文堂・1982年）138～139頁も、本罪をプライバシー保護の規定であることを前提として、「信書の内容がたとえ国・地方公共団体の秘密であろうと、また発信人・受信人のいずれかが国などであろうとそれは必ずしも問うところではない……なぜなら、本罪が保護しようとするのは私人のプライバシーであるからその可罰性の根拠は、信書の内容もしくは開披行為にではなく、信書の開披によって他人に知られたくない内容・事柄つまりプライバシーが侵害されたという点にある」と述べている。

秘密を探知する行為までであり、その内容を他者に公表する行為等については本罪によって評価されるものではない。

第3節 支払用カード電磁的記録不正作出準備罪

刑法163条の4第1項は、人の財産上の事務処理を誤らせる目的で、その事務処理の用に供する電磁的記録であってクレジットカードその他の代金又は料金の支払い用カードを構成するものを不正に作出する犯罪行為（163条の2第1項前段）や、預貯金の引出用のカードを構成する電磁的記録を不正に作出する犯罪行為（163条の2第1項後段）の用に供する目的で、①電磁的記録の情報を取得する行為と、②情を知ってその情報を提供する行為を処罰対象とする。不正に取得された電磁的記録の情報を同様の目的で保管する行為（163条の4第2項）と、器械又は原料を準備する行為（163条の4第3項）も処罰される。

163条の4は情報窃盜的な性質を有する犯罪類型であると同時に、163条の2の予備罪的な位置づけとなっている。これらの支払用カード電磁的記録に関する罪は、カードの電磁的記録をスキミングによって不正に取得してカードを偽造し、偽造カードを利用して商品の購入等が行われるようになったので、このような事態への対処方法として新設されたものである²³。対象となる電磁的記録の情報は、支払用カードによって支払いを行うためのシステムにおいて、情報処理の対象となるひとまとまりの情報であるとされており、情報の「取得」は、スキミングによって不正に取得する行為や、記録媒体に記録されたカード情報を記録媒体ごと取得する行為など、自己の支配下に情報を移す行為をいう²⁴。このように、個人のカード情報を窃取する行為が処罰対象となっているものの、支払用カード電磁的記録に関する一連の犯罪は「支払用カードを構成する電磁的記録の真正さ、ひいては支払用カードを用いた支払決済システムに対する社会的信頼」を保護法益としている²⁵ので、個人のカード情報は反射的に保護されるにすぎない。

第4節 不正指令電磁的記録に関する罪

近年増加しているコンピュータ・ウイルスによるコンピュータへの攻撃や、コンピュータ・ウイルス等を悪用した犯罪を防止するために、「犯罪の国際化および組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案」が2004年2月20日国会に提出され、2011年の刑法改正で「不正指令電磁的記録に関する罪」が設けられた。これによって、刑法168条の2の「不正指令電磁的記録作成等罪」では、正当な理由なくコンピュータ・ウイルス等を作成、提供する行為が処罰され、168条の3の「不

²³山口・前掲注（11）486頁。

²⁴山口・前掲注（11）494頁、高橋則夫『刑法各論』（成文堂・2011年）537頁など。

²⁵山口・前掲示（11）487頁、高橋・前掲（24）532頁。

正指令電磁的記録取得等罪」では正当な理由なくコンピュータ・ウイルスを取得、保管する行為が処罰される。これらの犯罪類型は、コンピュータ・ウイルスによる情報流出を防ぐために創設されたといわれているが、情報という個人的法益を保護するというよりも、コンピュータ・プログラムの安全性・健全性に対する公共の信用という社会的法益に対する抽象的危険犯として規定されている²⁶。したがって、本罪においては、コンピュータ・ウイルスによって個人情報漏洩されない利益が反射的に保護されているといい得るが、コンピュータ・ウイルスの作成・提供等の行為によって実際に個人情報の漏洩が発生したか否かということは本罪における法的評価の対象外である。

第5節 不正アクセス禁止法

不正アクセス禁止法3条1項では「何人も不正アクセス行為をしてはならない」と規定されており、3条2項は不正アクセスの定義について以下のように規定している。

①アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするものを除く。）

②アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能による特定利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを除く。次号において同じ。）

③電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為

これらの行為のなかで、いずれか一つに該当するものが「不正アクセス行為」である。

続いて、4条は「何人も、アクセス制御機能に係る他人の識別符号を、その識別符号がどの特定電子計算機の特定利用に係るものであるかを明らかにして、又はこれを知っている者の求めに応じて、当該アクセス制御機能に係るアクセス管理者及び当該識別符号に係る利用権者以外の者に提供してはならない。ただし、当該アクセス管理者がする場合又は当該アクセス管理者若しくは当該利用権者の承諾を得てする場合は、この限りでない」と規定することで、不正アクセス行為を助長する行為も禁止している。

²⁶山中敬一『刑法各論（第2版）』（成文堂・2009年）627頁、曾根・前掲注（18）268頁、伊東研祐『刑法講義各論』（日本評論社・2011年）427頁、山口厚「サイバー犯罪に対する実体法的対応」ジュリスト1257号（2003年）18頁。

このように、不正アクセス禁止法では、他人のコンピュータに直接あるいはネットワークを通じて、他人の ID やパスワードを利用して他人になりすまして、あるいは、コンピュータの弱点（セキュリティホール）を突いて不正にアクセスし、他人のコンピュータを利用できる状態にする行為と（不正アクセス罪）、他人の識別符号（ID とパスワード）を提供する行為などの不正アクセス行為を助長する行為（不正アクセス助長罪）が禁止されている。

不正アクセス行為とそれを助長する行為を処罰することによって、コンピュータにおける情報の不正入手を防止することが可能になるだろう。しかし、この法律の目的は「電気通信に関する秩序の維持を図り、もって高度情報通信社会の健全な発展に寄与すること」とされている。そして、この法律ではネットワークに接続され、かつネットワークの利用権者を ID とパスワード等の識別符号によって識別し、その識別符号が入力された場合にのみコンピュータの利用を認めるというアクセス制御がなされているコンピュータのみを保護の対象としており、不正アクセスによる情報の取得が不正アクセス罪の成立要件とされていない。不正アクセス後に個人情報の不正取得が行われたとしても、そのような行為は不正アクセス罪の範囲で法的に評価されるものではないのである。このことから、不正アクセス禁止法の保護法益は、「ID およびパスワードなどによる認証システムによって担保されているアクセス制御に対する社会的な信頼、すなわち正当な利用権者がアクセス制御機能によって正しく識別されていることに対する信頼」²⁷であり、不正アクセス罪は社会的法益に対する犯罪であるとされている²⁸。

このように、個人情報保護の側面のある規定には様々なものがあるが、情報を個人との関係において保護する規定・法律は、秘密漏示罪と信書開封罪と、後述する個人情報保護法であるといえる。

第6節 個人情報保護法

第1項 成立過程と概要

個人情報の漏洩や悪用を防ぎ、個人情報の取り扱いを規制する一般法として、2003年に「個人情報の保護に関する法律（個人情報保護法）」が成立した²⁹。ここでは、個人情

²⁷園田寿「不正アクセス禁止法における『不正アクセス』の概念について」甲南法務研究1号（2004年）109頁。

²⁸成瀬幸典「不正アクセス罪についての一考察」『阿部純二先生古稀祝賀論文集』（第一法規株式会社・2004年）365～368頁では、「アクセス制御機能に対する社会的な信頼」の実質的な意義について議論が展開されている。論者によると、コンピュータの利用につきアクセス制限を付加するいくつかの目的には社会的な意義・性格が付与されていることから、その目的の達成手段であるアクセス制御機能も原則的に社会的信頼の対象となる。社会的な意義を有するアクセス制限の目的として、①情報またはシステムの「不正操作の防止」、②情報の「機密性の保持」、③情報等の「真正性の保証」が挙げられている。

²⁹宇賀克也『個人情報保護法の逐条解説（第4版）』（有斐閣・2013年）1頁以下、宇賀克也『個人情報保護の理論と実務』（有斐閣・2009年）3頁以下、51頁以下。

報保護法の成立過程と、法律の概要について述べる。

日本の行政機関においては、1959年3月から電子計算機が使用されるようになり、行政効率の向上という利益が称揚されると共に、コンピュータによる個人のプライバシー侵害が懸念され始めた。そのような背景を受けて、1975年に行政監理委員会は「行政機関等における電子計算機利用に伴うプライバシー保護に関する制度の在り方についての中間報告」を提出した。その後、1980年には「プライバシー保護と個人データの国際処理についてのガイドラインに関するOECD理事会勧告」が出され、その勧告付属文書にOECD8原則³⁰という個人情報保護の基本原則が示されている。これは、個人情報保護の法制化を行っていた米独仏等の法律を参照して、個人情報の自由な流通の必要性に配慮しつつ個人情報保護を図るためのもので、個人情報保護の国際的な基本原則となっている。このOECD理事会勧告が、加盟国に対して各々の国内法の中でOECD8原則に配慮することを要求したことにより、日本も個人情報保護法制についてさらなる検討を迫られた。

OECD8原則後の日本は、行政部門における個人情報保護法制の整備を優先させるようになった。その契機となったのは、1983年の第2次臨時行政調査会答申であり、この答申において「法的措置も含め個人データに係る制度的方策について積極的に対応することが提言されたことである。このような動きを受けて、1988年に「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」が制定された。このように、行政部門における個人情報保護法制については早くから議論がなされていた一方で、民間部門における個人情報保護の一般法制定に関する議論は後退していた。

しかし、1995年にEUが「個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令（以下、EU個人情報保護指令）」というを出し、その25条において、個人データの第三国への移転は、当該第三国が十分なレベルの情報保護措置を確保している場合に限って行うことができると規定されている。これに加えて日本の民間部門における個人情報漏洩事件が相次いだことから、1998年の高度情報通信社会推進本部の「高度情報通信社会推進に向けた基本方針」において、「民間による自主的取り組みを推進するとともに、法律による規制も視野に入れた検討を行っていく必要がある」と規定されるに至った。

このような背景を受けて、1999年6月の参議院本会議において内閣総理大臣が、個人情報保護のために必要な措置について、「民間部門をも対象とした個人情報保護に関する法整備を含めたシステムを速やかに整えることなどを示すもの」であると認識しており、行政部門のみならず民間部門も含めた個人情報保護法制が政府において行われることになった。1999年11月19日には、政府機関である高度情報通信社会推進本部の下に置

³⁰OECD8原則は以下の通りである。①収集制限の原則、②データ内容の原則、③目的明確化の原則、④利用制限の原則、⑤安全保護の原則、⑥公開の原則、⑦個人参加の原則、⑧責任の原則の8つから成る。

かれていた個人情報保護検討部会によって「我が国における個人情報保護システムの在り方について（中間報告）」が出され、2000年10月には高度情報通信社会推進本部の個人情報保護法制化専門委員会による「個人情報保護基本法制に関する大綱」が、「中間報告」を踏まえた上で出されている。

そして、前述の「大綱」を基にして、2003年3月国会に「行政機関の保有する個人情報の保護に関する法律案」、「独立行政法人等の保有する個人情報の保護に関する法律案」、「情報公開・個人情報保護審査会設置法案」、「行政機関の保有する個人情報の保護に関する法律等の施行に伴う関係法律の整備等に関する法律案」「個人情報の保護に関する法律案」の個人情報保護関係5法案が提出され、可決成立した。

以上のように、日本の個人情報保護のための一般法は、まず行政部門において整備され、その後の国際情勢や日本国内における世論の要求によって、民間部門における個人情報保護法制が整備されるに至った。個人情報保護関係5法の制定により、日本の個人情報保護法制の体系は次の通りになる。「個人情報の保護に関する法律」は、1章から3章までの基本法にあたる部分と、4章から6章までの、民間部門の個人情報保護の一般法にあたる部分から成る。そこで、民間部門には個人情報保護法の1章から6章までが適用され、国および実質的に政府の一部をなす法人には、個人情報保護法の1章から3章までに加え、行政機関個人情報保護法と独立行政法人等個人情報保護法が適用される。そして地方公共団体には、個人情報保護法の1章から3章までと、各地域の個人情報保護条例が適用される。つまり、個人情報保護法の1章から3章までは、様々な機関が保有する個人情報を包括的に保護する基本法として位置づけられている。

ここからは、個人情報保護法の規定内容について述べる。

個人情報保護法では、個人情報は次のように定義される。まず、生存する個人に関する情報であり、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるものである。他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものも個人情報に含まれる（2条1項）。加えて、「個人データ」は個人情報のうち、「個人情報データベース等を構成する個人情報」であるとされている（2条4項）。この法律において個人情報と個人データを区別した理由は、開示請求等の対象となるのは、体系的に整理され、容易に検索できる個人情報に限定することにある³¹。また、死者の個人情報が対象外となっているのは、情報の開示請求等の自己情報コントロール権を有するのは生存者であり、死者に関する個人情報が同時に遺族の個人情報ともいえる場合には、それを生存者である遺族等の個人情報として保護すれば足りるからであると理解されている³²。

個人情報保護についての義務規定である本法4章が適用されるのは、「個人情報取扱事業者」である。個人情報取扱事業者は、「個人情報データベース等を事業の用に供している者

³¹平松毅『個人情報保護—理論と運用』（有信堂・2009年）73頁。

³²宇賀・前掲注（29）『理論と実務』57～58頁。

であるが、国の機関、地方公共団体、独立行政法人等、その取り扱う個人情報の量および利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定める者を除く」とされている（２条３項）。「政令で定める者」については、個人情報保護法施行令によって、「その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去６か月以内のいずれの日においても５０００を超えない者」とされている。つまり、「個人情報取扱事業者」は５０００人以上の個人情報を扱う民間事業者であり、日本国内の多くの企業等がこれに該当する。

このように主体を限定した上で、個人情報保護法４章は個人情報取扱事業者が遵守すべき義務について規定している。本法では個人情報の利用目的の特定（１５条）、利用目的による制限（１６条）、個人情報の適正な取得（１７条）、取得に際しての利用目的の通知等（１８条）のほか、個人データの内容の正確性の確保（１９条）、安全管理措置（２０条）、従業員の監督（２１条）、データの委託先の監督（２２条）、第三者提供の制限（２３条）、個人情報の取り扱いに関する苦情の適切かつ迅速な処理（３１条）などが義務として定められている。これらの義務は、前述のＯＥＣＤ８原則の考え方を具現化したものであると考えられている³³。

本法の特色には、個人情報取扱事業者による個人情報の不当な取り扱いにつき、多様な救済システムを採用していることが挙げられる。個人情報取扱事業者自身（３１条）、認定個人情報保護団体（４２条）、地方公共団体（１３条）、そして国（９条）などが苦情処理にあたることが定められている。しかし、このような苦情処理システムによって解決を図ることができない場合につき、個人情報取扱事業者の事業を所管する主務大臣は報告徴収（３２条）、助言（３３条）、勧告（３４条１項）、違反行為の中止その他違反を是正するために必要な措置をとるべきとする命令（３４条２・３項）をすることができる。そして、実効性担保の手段として、違反行為につき直接刑罰を科するという方式ではなく、個人情報取扱事業者が命令に従わない場合に初めて刑罰（６か月以下の懲役または３０万円以下の罰金）を科するという間接罰方式を採っている（５６条）。

第２項 罰則の方式に関する議論

第１項で見てきたように、個人情報保護法では間接罰方式が採られている。個人情報には様々な内容のものが含まれており、個人情報取扱事業者の義務内容も多岐にわたっていることから、違反行為に対して一律に直接刑罰を科するという方法を採用しなかったことは、その限りでは了解可能である。しかし、主務大臣の命令に違反して初めて刑罰を科するという方法は、企業等による個人情報の大量漏洩のような重大な情報侵害に対応できるのだろうか。この点を検討するため、第２項では個人情報保護法における罰則として、直罰ではなく間接罰方式が採用されるに至った経緯について、（１）個人情報保護検討部会³⁴と（２）

³³園田寿「個人情報保護法の成立」現代刑事法５５号（２００３年）８１頁。

³⁴個人情報保護検討部会の議事録は、<http://www.kantei.go.jp/jp/it/privacy/index.html> を参

個人情報保護法制化専門委員会³⁵の議論を通して概観する。

第1款 個人情報保護検討部会の議論

まず、第1回個人情報保護検討部会（1999年7月23日）において、「罰則の在り方とその適用範囲」について、安富潔委員は「刑事罰の関係で最も考えなければいけないのは、保護すべき個人情報の範囲」であり、「法規制によって自由な情報の流通というものが阻害されてはならない。他方で、情報保護のために刑事罰が必要になってくることもある」が、情報保護のために刑罰を用いる根拠は何かということが問題となると述べている。そこで、安富委員は従来の刑法の財産犯の枠組で情報を捕捉することができるのかということも含め、保護すべき個人情報の範囲について議論が必要であると述べている。

保護法益としての個人情報という問題は、第2回以降の検討部会でも議論されている。第2回（1999年8月6日）において、安富委員は「刑事罰ということになりますと、伝統的な刑法の枠組みの中で考えることになりますから、どういう保護法益ととらえるかという非常に難しい議論になってまいりますし、少なくとも今の日本の刑法では、現実の空間といえますか、そういう場で物理的に存在する物の保護という発想から保護法益を理解していく考え方から抜け切っておりませんから、バーチャルというか、電子空間のようなものとそうでない現実の空間との境がなくなってきたという発想は、なかなか刑事法の中ではとりにくいということがあります」と述べている。第1回検討部会における前述の発言と同様に、情報という異質なものを、存在が明確な財物と同様に扱うことの困難性に言及している。

続いて、第5回検討部会（1999年9月21日）では、日弁連が1998年に発表した「個人情報大綱」を題材に議論が展開された。日弁連の大綱は、プライバシーを始めとする個人情報の保護を主目的とする法律を制定すべきだと主張するものであり、最小限の罰則が必要であるという立場によるものである。

これに対して安富委員は、「財産権的な考え方でこの個人情報というのをとらえての罰則規定の御趣旨なのでしょうか。あるいは……もし民間部門の方で刑罰規定を設けるとするならば、いかなる保護法益に対する侵害行為に対して処罰を設けるという構想なのか」と質問したところ、大綱について報告した弁護士は、プライバシーを保護法益としつつ、様々なルール違反行為の中でも「罰則によって規制しようというのはもうちょっと実質的な侵害につながるようなものに限定」して、情報を不正入手する行為と、情報を渡す行為を中心に構成すると述べている。質問者の安富委員が要約するところによると、「個人情報というもの、それに一定の価値があるとして、それを侵害するから罰するというのではなくて、行為態様について、不正な活動というか、それに実質的な違法があると見るとい

照した。

³⁵個人情報保護法制化専門委員会の議事録は

<http://www.kantei.go.jp/jp/it/privacy/houseika/index.html> を参照した。

う理解」であり、「情報そのものの種類だとか、価値とか、そういうところに着目をするとなかなか罰則を設けることはできない」ので、行為態様から捕捉するのがこの大綱の手法となっている。大綱には、「保護法益としての個人情報」の範囲よりも処罰に値する行為態様を検討の方が刑罰の明確性に資するという問題意識があったように思われる。

これまでの検討部会における議論や各種専門機関からのヒアリングを踏まえて、検討部会の座長であった堀部政男は「座長私案」を作成し、第7回検討部会（1999年10月20日）において報告した。座長私案では、「そもそも罰則の創設には謙抑的であるべきであり、他の手段によって実効性担保が全く期待できない場合に限り、その創設を検討することが適切と考えられる」という一般論が提示され、「分野を問わず一律に罰則等の規制措置を設けることについては、構成要件の明確化の観点から、前提として全分野を通じた登録制度や届出制度の創設が必要となる可能性が高い」ことが指摘されている。

このように、座長私案は罰則を設けることに対して慎重な姿勢を採っているが、鈴木文雄委員は「不当な収集」、換言すれば「情報窃盗」についての刑法の手当というものを考える必要があるのではないかと問題提起する。これに対して、安富委員は「情報というのは財産だけに純化できるものではありません。そういう意味で言いますと、情報窃盗というものを果たして現行の刑法の枠組みの中で、果たして処罰できるようにつくり上げられるかということ、恐らくこれは非常に難しいだろうと思います」と述べている。

一方、安富委員は保護法益よりも行為態様に着目をして、これに何らかの規制をかけて罰則をつくることが可能かどうかという問題提起も行っている。ここでは、個人情報の収集権限のあるところに何らかの形で登録されている情報を不正な行為によって盗む、漏洩するという行為態様なら罰則を設けることが可能だと思われるが、およそ広く一般的に不正な入手ということを処罰するのは、現行刑法の枠組みからいって困難であることが指摘されている。これに対して、情報の侵害について苦情処理や相談窓口はあるものの、社会的な抑止力になっているとはいえないという意見が出された。そして、情報には財物とは異なる性質があるものの、売買の対象となっており、悪意による情報の詐取等に刑事罰を与えることができるような法的整備が必要であるとの意見もあった。このように、個人情報の漏洩などに有効に対処すべきであるという社会的な問題意識と、「個人情報窃盗」を構成要件化することの困難性との矛盾が顕在化している。

第8回検討部会（1999年11月9日）では、悪意による情報の詐取については刑罰で臨むべきなのか、それとも情報窃盗罪の創設には慎重になるべきかという議論がなされ、第9回検討部会（1999年11月19日）では「我が国における個人情報保護システムの在り方について（中間報告）」が出された。この中間報告では、罰則について「刑事法の一般理論として、罰則の創設には謙抑的であるべきであり、他の手段によっては実効性担保が期待できない場合に限り、その創設を検討することが適切である」「分野を問わず一律に罰則等を設けることについては、各分野における個人情報の利用の形態等が様々であるので、構成要件の明確化の観点から問題が多い」「広く薄い罰則であっても、あらゆる分野

の一般多数の事業者にとっては、自由な事業活動の阻害要因となるなど、他の保護されるべき権利、利益が損なわれるおそれがある」といった理由から、「あらゆる分野を通じた一般多数の事業者を対象とする基本法において、罰則等を創設することについては、慎重に考えるべきである」という結論に至った。

第2款 個人情報保護法制化専門委員会の議論

個人情報保護検討部会では、一定以上の情報侵害行為につき罰則を設けることが議論されたが、情報を従来の刑法の保護法益においてどのように位置づけるのかといった構成要件化につき困難があったことから、中間報告において何らかの罰則を提示するには至らなかった。続いて、個人情報保護法制化専門委員会の議論について概観する。

個人情報保護法制化専門委員会においても、個人情報保護検討部会と同様に、外国法の参照、日本の現行法の分析、関係省庁のヒアリング等を通して、保護されるべき「個人情報」とは何かということが議論されている。その中で、第13回委員会（2000年4月28日）において、高橋和之委員から「苦情処理などを行政機関が勧告し、勧告を聞かなかった場合にはサンクションを与えるというようなこともあり得るのではないか」と問題提起した。これは、個人情報保護検討部会の中間報告が直接的に刑罰を用いることに対して消極的な姿勢を採っていることと、民事責任は必ずしもサンクションとして有効な方法とはいえないのではないかという疑問による。そこで、行政に勧告権を与え、勧告を無視するような場合には罰則の対象とすることを射程に入れてもよいというのである。このような考え方は、現行個人情報保護法における間接罰方式の原型となっている。

第24回委員会（2000年9月8日）において、上谷清委員から「非常に悪質な個人情報の処理をする者については何らかの罰則は是非設けてほしい。当面、私が考えているのは、第三者提供にまつわるような不正な情報の処理です」という提案があった。

そこで上谷委員は、処罰範囲は①情報の内容面と②手段の悪質性の観点から限定することができるとした上で、個人情報取扱事業者に限らず一般の個人であっても、個人の秘密に関わるようなものを第三者に提供したり、何らかの形で個人情報を盗み出して第三者に提供したりする場合は罰則の対象となり得ると述べる。

ここで小早川光郎委員長代理は、このような二重の絞りによる処罰範囲の検討方法につき、産業界は従業員が職務上の横領背任のような形で、必ずしも秘密ではなくとも集積すれば経済的価値があるものを、自己の利益のために使うような行為につき処罰を要求していると述べた。これに対して上谷委員は、そのように幅の広い保護法益で重い罰則を科すことは困難であり、個人情報が集積して経済的価値を帯びるということを構成要件化することも困難であると述べている。

続いて第25回委員会（2000年9月14日）では、第24回委員会で罰則につき意見を述べた上谷委員が出したA案と、委員会事務局が作成したB案が議論の題材となった。

まず、A案では（ア）「正当な理由なく、人の秘密に属する個人情報を第三者に提供した

者及びその提供を受けた者について罰則を設ける」、(イ)「情報を管理する者の同意を得ないで、人の秘密に属する個人情報を取得した者について罰則を設ける」とされている。いずれも主体を限定していないが、名誉毀損罪や侮辱罪等の個々の既存の刑事罰の対象にならないような個人の秘密についてうわさ話をするだけで罰則の対象になることにつながるのではないか、情報を受動的に得た受領者も罰則の対象になるのかという疑問が司会者から出されている。

一方、B案では(ア)「法令で定められた守秘義務規定に違反して提供される個人情報であることを知りながら、それを取得した者について罰則を設ける」(イ)「(ア)に違反して取得された個人情報であることを知りながら、それを第三者に提供した者について罰則を設ける」とされている。そしてB案は、この委員会で一貫して問題となっている「悪質な第三者提供」について、主務大臣は個人情報取扱事業者に対して単なる改善指示を行うよりも、行政処分としての改善または中止命令をできることとして、その違反について罰則を設けるという考え方が提示されている。

このように、A案では「人の秘密に属する個人情報」の範囲が広がっているが、現代社会では大量に集積された情報の流通によって問題が生じているという観点から保護客体を限定する必要があるという意見が出された。

そして、第27回委員会(2000年9月29日)では、「大綱」の完成に向けて間接罰についての議論が展開されている。高橋和之委員は第13回委員会において、「苦情処理などを行政機関が勧告し、勧告を聞かなかった場合にはサンクションを与えるというようなこともあり得るのではないかと提案したが、第27回では「行政官庁から命令を出しておいてそれに違反の場合というワンクッションを入れる罰則のつくり方というのは……罰則の規定の仕方というのは基本は法律で定めることであるわけで、法律で罰すべきことを定めなくて抽象的に定めて行政機関が具体化するというようなやり方」に対しては、行政機関の裁量の拡大という観点からの批判もあることを述べている。

間接罰方式について、個人情報保護検討部会の座長である堀部政男は、従業員が個人情報を漏らしたり悪用したりしているケースには対応できないのではないかと主張しているが、藤井昭夫内閣審議官は、事業者の監督責任が問われる可能性があり、情報を漏らす等の行為をした従業員には解雇の可能性あることを指摘する。

このような議論を受けて、個人情報保護法制化専門委員会は大綱を出している。罰則についての大綱は以下のとおりである。

『個人情報』、『個人情報の取扱い』には様々なものがあるが、本基本法制においては、これらを広く捉えるとともに、個人の権利利益の侵害を事前に防止する仕組みとしていることとの関係で、これと並べて個人情報の『質』と『侵害の態様』を重視する刑事罰の規定を設けることになじまない面がある……また、本基本法制において、個人情報の第三者提供等を行政上の観点から規律するということになれば、その行政上の規律を確実に守らせるための仕組みが必要との考え方もあるところである。

そこで、本基本法制においては、個人情報の第三者提供等について、一定の要件の下に主務大臣が改善・中止命令を発し、それが守られない場合に罰則が適用される仕組みを設けることが適当である。

一方、政府は……個人情報の取扱いに関連する既存の各法律の守秘義務規定を中心に、個人情報の『質』と『侵害の態様』に応じた個人情報保護の観点から、早期に見直して罰則規定の整備を図るとともに、今後、本基本法制の趣旨に沿って各関係の法律を整備するに当たっても、同様の観点から罰則規定の整備を検討することが求められる」。

このように、大綱では間接罰方式を採用することを明言しており、それが法律に受け継がれている。個人の権利侵害を事前に防止する法的性格との関係で、個人情報の「質」と「侵害の態様」に基づく刑事罰とはなじまないとされているが、刑事罰には事後的な解決の他に予防という側面もあることから疑問が残る。検討部会の中間報告とは異なり、専門委員会では早い段階から、罰則を視野に入れた議論が行われていたが、処罰範囲の不当な拡大とならないように慎重な検討が行われていたことは両者に共通する点である。間接罰方式について、「個人情報にはさまざまな種類の情報が含まれており、個人情報取扱事業者にもさまざまな種類の事業者が含まれているから、一律に違反行為に対する直罰方式を採用しなかった法律の態度は妥当なものだと思われる。個人情報の中でも特に保護の必要性が高いいわゆるセンシティブ情報、たとえば個人の医療情報や金融・信用情報などに関しては、直罰方式を含めたより厚い刑法的保護を特別法で導入することを検討すべきであろう」とする学説³⁶の他、「主務大臣の命令を必要以上に強力なものとし、政府が個人事業者の日常的な業務にまで広範に介入する可能性を開くものである」「情報の『質』を度外視して主務大臣の命令違反といういわば行為無価値的側面からの一般的な処罰規定を置くことについては原則的な問題がある」という批判³⁷もある。

個人情報を「質」や内容、侵害の行為態様によって区別すべきとする考え方は委員会でも挙げられていたが、大綱および法律には反映されていない。検討部会も専門委員会も、刑罰の謙抑性の原則が極めて重視されていたという点では共通するが、第13回専門委員会の議論に見られるように民事責任のサンクションとしての有効性が疑問視されていたことから、検討部会の議論に比して罰則を設けることに抵抗感は少なかったようである。だが、その後の専門委員会の議論を見ると、個人情報の「質」と「侵害の態様」に着目した規定を設けるには、その構成要件化が困難であるという論調であったことも併せると、間接罰方式を提示する「大綱」は、刑罰の行き過ぎた回避と濫用のいずれにも偏ることがないようにという問題意識による暫定的な結論であったと思われる。しかし、様々な程度・内容のものを含む「主務大臣の命令違反」につき一律に罰則を科すことによって、広く薄い罰則を設けることとなってしまった。このような方法のもとでは、企業による個人情報の大量漏洩という重大な違反も、個人情報の取得後にその利用目的を本人に通知するのが

³⁶佐伯・前掲注（8）205頁。

³⁷園田・前掲注（33）82頁。

多少遅延したという比較的軽微な違反もすべて同様に扱われ得ることになり、罪刑の均衡を欠くものである。したがって、構成要件化が困難であるという指摘はあるものの、比較法的考察などを通して、個人情報とその重要性和侵害の行為態様という観点から分類した上で、妥当な保護のあり方を検討することが求められる。

第7節 小括

本章では、日本の現行法において個人情報や個人の秘密がどの程度保護されているのかということについて検討してきた。

まず、刑法134条の秘密漏示罪をはじめとする様々な職業についての秘密漏洩の罪によって、個人の秘密は様々な局面で厚く保護されているように見える。たしかに、個人情報の漏洩などの不正な取り扱いは、個人情報や秘密を知る機会のある職業の者によることが多い。しかし、法律で定められた守秘義務者以外の個人による個人情報・秘密の漏洩が行われる危険性もある。刑事事件を起こした少年の精神鑑定を行った医師の秘密漏示罪が問題となった最決平成24年2月13日刑集66巻4号405頁では、ジャーナリストCが被告人の精神科医に対して情報提供を積極的に要求して、被告人から得た情報をもとに少年についての書籍を出版したが、秘密漏示罪の教唆や幫助等で処罰されることはなかった。秘密漏示罪は特定の職業の者が個人の秘密を漏らすことを処罰する規定であるがゆえに、何らかの方法で個人の秘密を知った非守秘義務者が秘密を漏らし、それによって秘密の主体の利益が侵害されたとしても、処罰することはできない。秘密漏示罪、そして各種の秘密漏洩の罪にはこのような処罰の間隙がある。

続いて、信書開封罪は、個人の秘密に対する抽象的危険犯なのか、信書の秘密の形式や信書を勝手に開けられない利益に対する侵害犯なのかという点で争われている。そして、信書が個人のものに限定されるか否かという点でも争われているが、信書の内容が個人に関するものであれば、それを開封されたことによって個人情報や秘密を探知され得る。したがって、本罪は信書という範囲内で個人情報や秘密を保護しているといえる。

秘密漏示罪と信書開封罪は個人的法益犯罪であり、個人との関係で情報や秘密を保護している。その一方で、不正アクセス禁止法や不正指令電磁的記録に関する罪は、それぞれコンピュータ・プログラムの安全性・健全性に対する社会の信頼、アクセス制御に対する社会的な信頼が保護法益であるとされていて、個人情報はその反射効として保護されているにすぎない。したがって、不正アクセスやコンピュータ・ウイルスによって個人情報が侵害されたか否かは法的評価の対象外である。また、支払用カード電磁的記録に関する罪では、電磁的記録の情報を窃取する行為が処罰の対象となるが、本罪の保護法益は電磁的記録の真正性と支払決済システムへの社会的信頼であって、個人のカード情報そのものではない。このように、現行刑法典では、個人情報は断片的に保護されているにすぎない。

個人情報保護の一般法としての法的性質を有するのが、個人情報保護法である。本法では、個人を識別する情報が幅広く保護されており、個人情報取扱事業者は個人情報保護の

ために様々な義務を有する。義務違反に対して直ちに刑罰が発動されるのではなく、主務大臣の命令に違反した場合にはじめて罰則の対象となる。

個人情報保護法の法制化につき、個人情報保護検討部会と個人情報保護法制化専門委員会が議論を行い、それぞれ「中間報告」「大綱」を提示している。個人情報の侵害に刑罰を設けることには、両者ともに刑罰の謙抑性という観点を重視していたが、専門委員会の方が民事責任の有効性に懐疑的であり、刑罰に対する抵抗感が少なかったように見受けられる。検討部会の中間報告には罰則について具体的な提案がなかったが、専門委員会の大綱には主務大臣の命令違反に対して罰則を設ける旨が記載されている。専門委員会の議論の段階においては、個人情報の「質」と「行為態様」に応じた罰則の在り方が提案されていたにもかかわらず、実際の大綱には間接罰という広く薄い刑罰方式が提示され、それが現行法のもととなった。個人情報の「質」と「行為態様」に応じた構成要件化が困難であることも議論の中で指摘されていたが、このような罰則方式では重要な個人情報に対する重大な侵害も、軽微な個人情報の侵害も同様に扱われることとなり、罪刑の均衡を欠く。したがって、広く薄い刑罰を一律に科すのではなく、個別具体的な状況に応じた構成要件化のための議論が必要である。

第3章 イギリス法における個人情報保護

本章では、イギリスにおける1998年データ保護法（Data Protection Act 1998）について扱う³⁸。後述するように、1998年データ保護法は、不正に個人データを取得等した者を直接的に処罰する規定を設けており、データ保護についての第三者機関である情報コミッショナーが情報保護のための厳罰化に積極的な姿勢を採っている。個人情報の侵害を処罰する規定を日本法に設けることを検討するにあたり、イギリス法における直接罰規定の意義と、情報コミッショナーの役割と実務について分析する。

まず、1998年データ保護法が成立するまでの過程について述べる。コンピュータの普及に伴うデータ保護立法の必要性和、データの取り扱いによる個人のプライバシーへの脅威に関する議論が起こり、1998年データ保護法の前身である1984年データ保護法（Data Protection Act 1984）が制定された。1984年データ保護法制定前の法律は、各種機関によって保有される多くの個人情報の取り扱いに対する規制としては不十分であったことから、1970年代初頭に、Younger のプライバシー委員会（Committee on Privacy）は個人データを処理するコンピュータの使用にあたって次のような10の指針を発表した。

(a) 情報は、特定の目的のために保有するとみなされるべきであり、適切な許可なく他の目的のために使用されてはならない。

(b) 情報へのアクセスは、情報を提供した目的のために許可された者に限定するべきである。

³⁸以下、イングランド及びウェールズを「イギリス」とする。

(c) 収集または保有される情報の量は、特定の目的を達成するために必要最小限にすべきである。

(d) 統計目的のために情報を処理するコンピュータシステムにおいて、識別データと残りのデータを分離するための設計及びプログラムにおいて、適切な対策をすべきである。

(e) 主体が自らについて保有される情報について知らされる手段を準備すべきである。

(f) システムによって達成されるべき安全のレベルは、事前に利用者が特定すべきであり、情報の意図的な濫用や誤用に対する予防策も含むべきである。

(g) 監視システムは、セキュリティーシステムの違反の探知を容易にするために提供されるべきである。

(h) 情報システムの設計において、情報保有期間の限界を定めるべきである。

(i) 保有されるデータは正確でなければならない。不正確な情報を是正し、最新化するための機構が必要である。

(j) 価値判断の規約化に注意を払うべきである。

Younger 委員会は、個人や各種機関によるプライバシーの侵害に対して更なる保護を与えるための立法が必要か否かを検討していたので、委員会はデータの保護よりもプライバシーの保護の方により関心を持っていた。Younger 委員会の提案は制定法化されなかったが、委員会の報告を受けたイギリス政府は、将来的にデータ保護機関を設けるための詳細な知見を得るために、Lindop 委員会を設立した。政府は委員会の委員長に Younger を指名していたが、Younger が死亡したことにより Lindop が委員長に就任することとなった。

Lindop 委員会は以下の内容の報告書を発表している。

「Younger 委員会はプライバシーについて扱っているが、我々はデータ保護について扱う。実際、この2つの領域は一部重なっており、重なる部分は『情報プライバシー』または『データプライバシー』と呼ばれる。これは重要な領域であり……データプライバシーの概念と意義、その結果を検討することは有意義なことである。この目的のために、データプライバシーという用語を、自分に関するデータの伝達に対するコントロールを個人が要求することという意味で用いる」。

Lindop 報告書は、データ保護のための機関を設立し、ビジネス界によるデータの取り扱いに対する特別な法典を制定するべきであると提言する。Younger 報告書がプライバシーの全分野の検討をすすめていたのに対して、Lindop 報告書はデータ保護を検討対象とした上で、プライバシー権を「ひとりで放っておいてもらう権利」ではなく「自己情報コントロール権」として解すべきことを明らかにした。当時の政権交代により、結果的に Lindop 報告書も制定法化されなかったが、その内容は1984年データ保護法に受け継がれることになった。

このように、個人データの濫用や誤用によるプライバシー侵害に対する保護の必要性という観点から1984年データ保護法が制定されたが、1995年10月14日の EU データ保護指令 (EU Directive on Data Protection) に基づく法改正が行われた。EU 指令

が出された場合、加盟国は指令の内容に沿った国内法を制定することを義務付けられるので、多くの加盟国が法律の制定や改正を行った。データ保護指令は、加盟国間の情報流通を容易化するために、加盟国間における個人データ保護のレベルの格差をなくすことを目的としている。指令の7条は、個人データが取り扱われる前に満たさなければならない多くの条件を定めている。そこでは、データの取り扱いが法的義務の履行に必要な場合や、データ主体の生命にかかわる場合などの例外的な場合を除いて、データの取り扱いにはデータ主体の同意が必要であるとされることに加えて、個人の人種・民族的出自、政治的信条、宗教的・哲学的信条といった特別なカテゴリーの情報の取り扱いにあたり、一定の厳格な条件を満たすことが必要であり、その中の1つがデータ主体の明確な同意であることが規定されている。続いてデータ保護指令は、データ主体の権利やデータの安全等についても規定している。

このようなデータ保護指令に従って1998年データ保護法が制定され、2000年3月1日に施行された。1984年法との主な相違点は以下の通りである。まず、1998年法では、自動処理されたデータのみならずマニュアルデータにまで保護の対象が拡大されている。続いて、指令の内容を受けて、一般的な個人データとは別に、より厳格な保護を要する「センシティブな個人データ」という概念が設けられた³⁹。そして、EU加盟国間の適切な情報流通という趣旨を有するデータ保護指令を受けて、情報の取り扱いについて一定の条件を満たしていない限り、欧州経済領域（European Economic Area）に加盟していない国にデータを流通することが禁止されるようになった。データ主体の権利も強化され、データの不正な取り扱いによって被った損害や苦痛に対する損害賠償が認められるようになった。以上のように、1998年法は個人データの保護と監督をさらに強化するものとして成立した⁴⁰。

第1節 1998年データ保護法の概要

本節では、1998年データ保護法の概要について述べる。

第1項 基本事項

この法律では、「個人データ (personal data)」が保護の対象になる。個人データとは、「(a) データによって特定される生存中の個人に関する当該データ、および (b) データ管理者が

³⁹ 1984年データ保護法にも類似の規定は存在したが「センシティブな個人データ」という文言は用いられていない。1984年法2条3項は、「国務大臣は、次に掲げる事項に関する情報からなる個人データに関し、追加的保護措置を講ずるため、命令により、データ保護原則を修正し、または補足することができる。(a) データ主体の人種、(b) データ主体の政治的意見または宗教的その他の信条、(c) データ主体の肉体的もしくは精神的健康状態またはその性生活、(d) データ主体の犯罪歴」と定めている。他の一般的な個人データよりも厳重な保護をし得ることが定められつつも、実際にどれほど保護を厚くするかということは国務大臣の裁量に委ねられていたという点で、1998年法と異なっている。

⁴⁰ 1998年データ保護法成立までの過程については、Peter Carey, *Data Protection: a practical guide to UK and EU law*, 2d ed, Oxford University Press, 2004, 1-9 を参照した。

保有するか保有する可能性があり、かつ個人に関する意見（**opinion**）の表明及び個人に関するデータ管理者若しくは他の者の意向（**intention**）の表示を含む、データ及び他の情報によって特定できる生存中の個人に関するデータ」⁴¹と定義されている（1条（1）項）。たとえば、特定の人が「怠け者である」というのは「当該個人に関する意見の表明」であり、「怠け者であるから、解雇する」というのは「意図の表示」とされている⁴²。したがって、日本の個人情報保護法における「個人情報」より範囲が広いと言える。また、この法律では一般的な個人データよりも厳格な取り扱いを要する「センシティブな個人データ（**sensitive personal data**）」という概念がある。

この法律では、データ主体（**data subject**）である生存する個人には、6つの権利が認められている。それは、①個人データへのアクセス権、②個人に損害や不利益をもたらし得る取り扱いを止めさせる権利、③ダイレクトマーケティングを目的としたデータの取り扱いを止めさせる権利、④自動的な決定（**automated decision-taking**）に関する権利、⑤損害賠償を請求する権利、⑥不正確な個人データを修正・封鎖・抹消・破棄する権利である。

この法律において、データの処理に関わるのは「データ管理者（**data controller**）」である。データ管理者は、「個人データが処理され、または処理されるべき目的および方法を決定する者」と定義されていて、個人・法人・団体の如何を問わないとされている。この法律ではデータの取り扱い（**processing**）が規制されているが、「取り扱い」は「情報やデータの取得、記録または保有、何らかの操作や一連の操作をすることを意味する。以下のものを含む。(a)情報やデータの編成、修正、変更、(b)情報やデータの検索、参照、利用、(c)伝送、頒布その他の方法によって情報やデータを提供すること、(d)情報やデータの配列、結合、封鎖、抹消、破棄」と定義されている。

データ管理者には、①情報コミッショナー（**Information Commissioner**）に通知する義務と、②データ保護8原則（後述）を遵守する義務がある。情報コミッショナーは、単独法人（**corporation sole**）であり、国王から独立してデータの取り扱いを監督する機関である。データ保護法違反のおそれのある事業所等を調査したり、参考人に対する事情聴取といった行政的な措置を採ったりしている。そして、データ管理者は情報コミッショナーへの通知義務に基づいて、個人データを取り扱うにあたって、データに関する項目と、第7データ保護原則（情報の安全性の確保）を遵守するための措置を通知しなければならない。

第2項 データ保護原則（Data Protection Principles）について

ここでは、データ管理者が遵守すべきとされるデータ保護原則について述べる。1998年データ保護法の附則（**schedule**）1には、データ保護原則が8つ規定されており、デ

⁴¹イギリスのデータ保護法の邦訳は、木村光江・星周一郎「海外の個人情報保護法における刑事規制（1）イギリスのデータ保護法の概要とその運用状況—刑事規制を中心に」クレジット研究27号（2002年）258～268頁と、石井夏生利『個人情報保護法の理念と現代的課題』（勁草書房・2008年）を参照した。

⁴²堀部政男「個人情報の法的保護」法とコンピュータ20号（2002年）70頁。

ータの取り扱いにおける重要な指針となっている。

まず、第1原則は、「個人データは公正に、合法的に処理されなければならない (Personal data shall be processed fairly and lawfully)」と規定した上で、「センシティブな個人データ (sensitive personal data)」といわれる重要な情報（後述）については、後述する附則3の条件のうち少なくとも1つを遵守する必要がある、その他の個人データ一般については後述する附則2の条件のうち、少なくとも1つの遵守が必要であるとされている。附則2の規定する条件には、①データ主体がデータ処理に同意していること、②データ主体が当事者となる契約を実行するためにデータ処理が必要であること、③データ主体の利益をはかるためにデータ処理が必要であることといったものがある。

第2原則は、「個人データは1つまたは2つ以上の特定の適法な目的のためにのみ取得されなければならない。そして、その目的またはそれらの目的と適合しない方法でさらに処理されてはならない」として、限定された目的のためのデータ処理を指示している。第3原則は、「個人データは処理される目的に応じて適切で、関連するものでなければならず、過度であってはならない」として、データ処理の目的適合性を規定する。第4原則は、個人データは正確 (accurate) で、必要に応じて最新のもの (where necessary, kept up to date.) でなければならないと規定する。第5原則は、個人データは処理目的のために必要な期間よりも長く保管されてはならないと規定する。第6原則は、個人データはこの法律におけるデータ主体の権利に従って処理されなければならないと規定する。第7原則は、無権限による、または不法な個人データの取り扱い、または個人データの偶発的な損失・破壊・個人データに対する損害が発生しないように、適切な技術的・組織的措置が採られるべきであると規定する。第8原則は、個人データが十分に保護されていない国や地域にデータを移転してはならないと規定する。イギリスにおけるデータ保護原則は、データ管理者が遵守すべき義務とされている。

第3項 罰則について

続いて、データ保護法における罰則について概要を述べる。

第1款 データ保護原則の違反

データ管理者がデータ保護8原則に違反した場合には、まず、情報コミッショナーから執行通知 (enforcement notices) が出される。執行通知について、1998年データ保護法40条(1)は以下のように定める。「データ管理者がデータ保護原則に違反したか、もしくは違反していることをコミッショナーが確信した場合には、コミッショナーはデータ管理者に対して通知（本法では「執行通知」という）を出すことができる。その通知は、データ管理者に対して、当該原則または諸原則の遵守のために、以下のいずれか一方または両方を行うように要求することができる。

(a)通知に明記されるであろう期間内に、明記された措置を行うこと、または、通知に明記されるであろう期間の後、明記された措置を行わないこと

(b)明記された期間の後、いかなる個人データ、もしくは通知に明記されたいかなる個人データの取り扱いも行わないこと、または、明記された目的で、もしくは明記された方法で個人データを取り扱わないようにすること」

データ管理者は違反があった、または違反が行われていると判断された当該データ保護原則につき、上記の執行通知を受けることになっており、通知の内容に基づいて是正措置を採ったり、データの取り扱いを中止したりすることを要求される。

また、執行通知とは別に、情報通知 (information notices)、特別情報通知 (special information notices) がある。前者は、個人データの取り扱いに利害のある者から、データ保護法が遵守されているのか否かについての評価 (assessment) の請求があった場合に、またはデータ保護原則に違反しているか否かを判断するという目的による情報請求があった場合に、情報コミッショナーがデータ管理者に対して、請求に関する指定された情報 (specified information) を提出すること、またはデータ保護原則の遵守を要求する通知を出すことができる、という制度である。後者は、データの取り扱いが特別目的 (special purpose) ⁴³のためだけに行われていないことをコミッショナーが疑う合理的な根拠がある場合には、コミッショナーはデータ管理者に対して、指定された情報を提出するように要求する通知を出すことができるという制度である。

そして、データ管理者が執行通知・情報通知・特別情報通知を無視した場合に、刑事罰が科される (47条1項)。このように、データ管理者はデータ保護原則に違反しても直ちには処罰されず、違反に対する是正通知を無視した場合に初めて刑罰の対象となるという点で、日本の個人情報保護法における主務大臣の命令に対する違反のように、間接罰方式となっている。

第2款 個人データの不法取得等の罪

データ管理者に対する処罰規定の他に、データ保護法には、「個人データの不法な取得等 (unlawful obtaining etc. of personal data)」を行った個人に対する処罰規定がある。データ保護法55条(1)項では、「何人も、データ管理者の同意がなければ、故意または無謀により (knowingly or recklessly) (a) 個人データもしくは個人データに含まれる情報を取得し若しくは開示し (obtain or disclose)、または (b) 個人データに含まれる情報について他の者に開示を周旋 (procure) してはならない」とされており、55条(3)項において、これらの行為が犯罪を構成するものであることが規定されている。一方で、55条(1)項の行為は、55条(2)項に該当する場合には許容される。55条(2)項は、「(a)個人データの取得、開示、または他の者に開示の周旋をする行為が、(i)犯罪を予防するため、または犯罪捜査のために必要である場合、(ii)制定法によって、法の規則によって、または裁判所の命令 (order of a court) によって要求され、または正当化される場合、(b)データや

⁴³データ保護法3条によると、(a) ジャーナリズムの目的 (b) 芸術目的 (c) 文学的目的の中の1つ以上に該当するものをいう。

情報を取得したり開示したり、事情によっては情報の開示を他の者に周旋したりする法律上の権利があるとの合理的な信念 (reasonable belief) を持って行為した場合、(c)データ管理者が取得、開示または周旋が行われたこととその状況を知っていれば、データ管理者の同意を得たであろうとの合理的な信念を持って行為した場合、(d)特別の状況において、取得・開示・周旋行為が公共の利害 (public interest) に資するものとして正当化される場合」には55条(1)項の対象にはならないと規定している。

55条(1)項所定の行為の他に、55条(4)項では(1)項に違反して個人データを売却する行為が処罰され、55条(5)項(a)号では(1)項に違反してデータを取得した上で個人データの売却を申し出る行為が、(b)号では売却を申し出た後に(1)項に違反してデータを取得する行為が処罰の対象となる。データの取得や開示・周旋に対しては正当化事由が存在するのに対して、売買やその申し出については正当化事由が規定されておらず、後者の行為態様は侵害性が高いものとしてより重い処罰が予定されている。

これらは選択的審理方法の犯罪 (either-way offenses) であり、治安判事裁判所 (Magistrates' Court) と刑事法院 (the Crown Court) のいずれでも審理できる。治安判事裁判所では罰金5000ポンドが法定刑の上限となるが、刑事裁判所では罰金額に制限がない。

以上、イギリスの1998年データ保護法の概要について整理した。1998年データ保護法について、以下のことが問題となる。第1に、データ管理者の同意なく情報を不正に取り扱った個人が55条による直接罰の対象となっているが、55条の射程範囲と意義は何かということである (第2節)。続いて、国王・政府から独立した第三者機関である情報コミッショナーが、個人情報の保護のためにどのような活動を行っているのかということである (第3節)。そして、センシティブな個人データの詳細と、その合法的な取り扱いの条件と、一般的な個人データの取り扱い条件との違いについて検討する (第4節)。

第2節 個人データの不法な取得等に対する直接罰規定について

本節では、1998年データ保護法における個人データ不法取得等の犯罪の意義と射程範囲について検討する。

前述の通り、1998年法55条では、データ管理者の同意なく個人データを取得・開示・開示の周旋・売却するといった幅広い行為が個人データの不正な取り扱いとして処罰の対象となっている。これは「情報窃盗」などの行為を処罰する規定の一例であり、日本の実定法には存在しないものである。個人情報の侵害に対する妥当な処罰のあり方を検討するにあたって、1998年データ保護法55条の成立条件について検討する。

第1項 1998年データ保護法55条の成立まで

1998年データ保護法55条では、データ管理者の同意なく個人データを取得、開示、他人に対し開示の周旋をした者を直接処罰する規定であるが、この法律の前身である19

84年法（Data Protection Act 1984）にはこのような規定は存在せず、これらは EU データ保護指令に由来するものでもない。1984年法5条（1）項では、データ利用者（data user）、またはコンピュータ・ビューロー（computer bureau）をも営むデータ利用者として登録簿に登録されていない限り、個人データを保有（hold）することが禁止されていた。5条（5）項では、（1）項に違反する者、または故意や無謀によって5条の他の規定に違反する者は有罪となることが規定されている。このように1984年法では、個人データの取り扱いについては登録が義務付けられていたので、5条（2）項以降では、登録されている個人データの種類や目的を超えて個人データを保有または使用（use）したり、登録外の者に個人データを開示したりする（disclose）等の行為が禁止されていた。登録をした者のみが個人データを取り扱うという前提に立っていたことから、無権限者が個人データを保有することを超えて、個人データを開示したり売却したりする行為を処罰の対象とするという発想がなかったものと思われる。しかし、データ管理者以外の個人がデータを不正に取り扱う行為を広く処罰する現行法55条が設けられるに至った背景には、後述するように、不正な行為によって、第三者が情報を入手するケースが増えて社会問題となっており、これを予防するために刑罰への期待が寄せられたことがある。

情報コミッショナー事務局（Information Commissioner's Office）が2006年5月10日に提出した報告書「プライバシーの価値とは何か？（What price privacy?）」（詳細については第3節で後述する）において、55条成立の間接的な原因となった具体的事件が紹介されている。それは、1992年11月に、当時の大蔵大臣であった Norman Lamont 氏のクレジットカードの購入記録に関する情報を銀行員が洩らしたというものである。その後、彼がロンドンの酒類小売店で購入したものについての報道が過熱し、「大蔵大臣が Julian Barnes で赤ワインを購入した」という雑誌記事も発表された。この事件において、個人の銀行や税金記録に関する情報と他の個人情報が開示されたという問題は、当時のデータ保護登録官（現在の情報コミッショナー）であった Eric Howe による1993年の年次報告で取り上げられた。Eric Howe は、個人情報への不正アクセスを試みたり実際に行ったりする者に対する処罰という考え方について論じた。第3節でも詳述するが、情報コミッショナーは個人データの保護のための厳罰化に積極的である。

続いて、1994年にはイギリス情報局長の Stella Rimington の私生活についてマスコミが報道するという事件⁴⁴が発生した。報道によって、彼女が火曜日の午後にもいつも買い物をする場所についての情報が開示されたが、この情報は彼女が利用する金融機関に偽の電話を掛けることで入手されたものであることが判明した。この件についての苦情がデータ保護登録官事務局（the Office of the Data Protection Registrar 現在の情報コミッショナー事務局）に寄せられたが、偽の電話によって情報を入手した者が「データ使用者」としての登録をしていなかったことにつき、故意も無謀もなかったということにより、事務局は訴追しないことを決定した。このような事件は、ジャーナリストや私立探偵等によって

⁴⁴ Rosemary Jay , Data Protection Law and Practice,3d ed, Sweet & Maxwell,2007,595.

個人情報が入手され得ることを明らかにした。

1994年3月の貴族院の議論で、政府は不正によって個人情報へのアクセスを得る行為について特別の犯罪規定を設けるつもりであることを発表した。これを受けて、1994年刑事司法及び公共秩序法（**Criminal Justice and Public Order Act 1994**）161条により、1984年データ保護法5条の罰則が拡大された。この法改正により、コンピュータに入力された個人情報の開示、開示の周旋、売却等の行為を処罰する条項が設けられ、1998年データ保護法では対象が個人データ一般に拡大された。

以上の法改正により、55条において処罰の対象となる行為の範囲が問題となる。1998年データ保護法55条は、データや情報を開示する者と、それらを直接入手したり開示を周旋したりする者を対象にしているが、間接的に情報やデータを入手する者や、情報やデータの入手によって最終的に利益を得る者は含まれていないようにも思われる。そして、55条（4）項と（5）項では、データや情報を売却する者と、売却を申し出る者が処罰されるが、データの購入者と購入を申し出た者については明記されていない。条文を文字通りに解釈すれば、私立探偵等から情報やデータを間接的に得る者は55条（1）項に抵触しないことになるだろう。

しかし、55条は犯罪となる範囲を1984年法より拡大しており、このことから、55条（1）項は、個人データや情報を直接入手した者に限定していないと考えられる⁴⁵。更に、1998年法は個人データの「取り扱い（**proceeding**）」の定義を、データについて行われ得ることのすべてに拡大していることから、55条（1）項における「取得（**obtaining**）」という単語は、単なる情報の呼び出し行為や、コンピュータ・スクリーン上の情報を読むこと等も含んでおり、同様に、私立探偵から情報やデータを入手した弁護士の活動等にも適用され得る⁴⁶。1998年データ保護法制定以前の事例として、**R v Brown**[1996] 2 WLR203 があり、債権回収会社を経営する友人を助けるために、警察官 **Brown** が、警察のコンピュータデータベースに貯蔵されている情報をコンピュータ・スクリーンに呼び出すよう同僚に依頼したところ、警察官は1984年法所定の、登録簿に記載された目的を超える個人データの使用の罪で告発されたというものがある。この警察官の行為は、単にコンピュータ・スクリーン上に表示されている情報を読んだだけにとどまっていたので、1984年法における「使用する（**use**）」に該当するか否かが問題となった。この争点につき、貴族院は、「使用する（**use**）」の概念は、データベースから情報を検索（**retrieval**）しただけの行為にまで拡大されないと判断した。一方、1998年データ保護法55条は、個人データに含まれる情報を「取得」する行為を犯罪としているので、現行法の下では **Brown** のようにコンピュータ・スクリーン上にある情報を読み取る行為も55条の罪で処罰される可能性がある⁴⁷。このように、個人データや情報を何らかの方法で知る行為は広く

⁴⁵Catrin Evans, *The Offence in Section 55 DPA-Unlawful Obtaining of Personal Data, Privacy and Data Protection*, 1 June 2003.

⁴⁶ Evans, *supra* note, 45.

⁴⁷ Carey, *supra* note 40, at 189.

55条でカバーされているといえる。

また、情報の「開示」行為に関する重要な判例として、*R v Rooney*[2006]EWCA Crim1841がある。被告人 *Jacqueline Mary Rooney* は警察職員であり、他の職員の個人データにアクセスして情報を第三者に開示したとして有罪となった。被告人の姉妹は警察職員 A と関係があったが、2003 年に別居した。その後 A は別の警察職員 T とイギリスの *Tunstall* という地域で同居を開始し、二人の詳しい住所が警察の職員データベースに掲載されていた。被告人は A と T の住所に関する情報に何度もアクセスし、A と関係のあった被告人の姉妹に、A と T が現在 *Tunstall* に住んでいることを伝えたが、正確な住所については言わなかった。被告人は、個人データを取得して第三者にそれを開示したとして訴追されて有罪となったが、被告人は正確な住所を言っていないことを理由に、自己の行為が「開示」に該当しないとして控訴した。これに対して裁判所は、データ保護法 55 条（1）項は個人データのみならず、個人データに含まれる情報を開示する行為を処罰対象としていることから、A と T が *Tunstall* に住んでいるという情報から正確な住所を特定することができないとしても、犯罪成立を妨げないとして被告人の控訴を棄却した。「個人データに含まれる情報」の範囲の解釈如何によって、処罰範囲の無限定な拡大が可能になるので、検討の余地があるだろう。

第2項 55条違反の犯罪の主観的要素

前項では、1998年データ保護法55条の成立までの流れと、55条の処罰対象となり得る行為について扱った。55条（1）項は、データ管理者の同意なく、(a) 個人データもしくは個人データに含まれる情報の取得または開示、(b) 開示の周旋を「故意または無謀」によって行った場合に処罰の対象となることを規定している。そして、データや情報の売却等の行為もまた、「故意または無謀」によって（1）項に違反することを前提とする。刑罰法規においては、故意犯のみを処罰するのが原則であるので、「無謀」の意義と範囲は重要な問題である。そこで本項では、主に「無謀」の有無が問題となった判例の検討を行う。

（1）*Data Protection Registrar v Amnesty International* [1995] Crim.L.R.633. (unreported)

この事件が発生した時期は、1984年データ保護法が適用されていた。被告のアムネスティ・インターナショナルのイギリス支部（以下、「アムネスティ」とする）は、他の慈善団体と各々のメーリングリストを交換（*exchanged mailing lists*）する協定を結んだ。交換の方法は、他の慈善団体のために運営され、ダイレクトメール発送業務を行っていたメーリングハウスに対して、アムネスティのメーリングリストを開示する（*disclosure*）というものであり、両者のやり取りは金銭の授受なしに行われた。データ登録官は、アムネスティが個人データを登録外の目的で使用（*use*）し、個人データを登録されていない者（メーリングハウス）に開示したことから、1984年法の5条（2）（b）項と5条（2）（d）

項の罪を犯したとして訴追した。アムネスティがデータを開示したことによって、アムネスティの支持者に対して、協定の相手方となった慈善団体への寄付を求めるメールが送られたので、メールの受取人の一人が登録官に苦情を申し立てたことが端緒である。登録官は、アムネスティはデータの使用と開示が登録内容に沿うものか否かを確認しなかったことにつき、無謀があったと主張した。

有給治安判事（*stipendiary magistrate*）は裁判の結論において、以下の理由により登録官の訴えを退けた。まず、過去の判例である *Lawrence*[1982]A.C.510 と *Caldwell*[1982]A.C.341 では、「深刻で有害な結果（*serious harmful consequences*）」が発生するという予見がなければ無謀の存在は認められないとされている。本件アムネスティの行為の結果は、寄付を要求する望まないメールが届いたことであり、これは「深刻で有害な結果」というよりも苛立たしい（*irritating*）と表現される感情的なものにすぎないと判断され、アムネスティに対して無罪が言い渡された。

これに対して、登録官は合議法廷（*Divisonal Court*）に控訴した。控訴審は、訴追者が 1984 年法 5 条における主観的条件である「無謀」の存在を証明するには、以下のことを示さなければならないと判示した。

①データ保護法 5 条が回避しようとしている損害（*mischiefs*）を発生させ得る可能性に対して、通常の分別ある個人としての注意（*attention of the ordinary prudent individual*）がなされていたことを示す状況と、そのような損害の発生する危険（*the risk of those mischiefs occurring*）が少なくないので、通常の分別ある個人はその危険を取るに足らないものとして扱うことは当然できないということ

②行為に出る前に、被告人（アムネスティ）がそのような危険の発生する可能性について何らの配慮もしなかったか、可能性については認識していたものの行動に移してしまったこと

無謀の有無の判断の際には、データ保護法 5 条（2）項において予定されている損害結果の予見（*foresight of the consequences identified in section 5(2) of the Act*）の有無が問題となったが、結果の予見という判断基準をこの文脈で用いるのは不適切だとする批判がある⁴⁸。論者によると、データ使用者として登録している者が登録されている個人データ以外のデータを保有（*hold*）した場合に 5 条（2）（a）項の犯罪が成立するので、データの保有による結果や損害の予測があったか否かを判断する必要性がないのは明確である。同項で予定されている損害は、保有されるべきではないデータが保有されることであり、それ以上の現在の、あるいは予想される結果について考慮する必要はない。5 条（2）（a）項の意義は明確であり、登録されたデータ使用者が、自己の保有するデータの性質について気づいていないということに注意を払わないことである。この犯罪は無謀によって損害を発生させるという点で軽い性質のものであり、同じ損害を故意によって発生させる犯罪よりも、常に軽く罰せられるべきである。したがって、無謀の有無を判断する際に深刻な

⁴⁸ [1995]Crim L R 633,634.

結果の予見可能性を求めることは、軽い犯罪をより重い性質の犯罪へと転化することにつながるという点で疑問であると解されている。論者は、データ使用者による 5 条違反の犯罪の中で最も単純な類型である (2) (a) 項を挙げて論じているが、当該犯罪による損害の程度がさほど深刻ではない上、故意犯よりも軽い犯罪の構成要素である無謀の有無を判断する際に「深刻な損害の予見可能性」を要求することは妥当ではないという趣旨であると思われる。

(2) Information Commissioner v Islington London Borough Council[2002]EWHC Admin 1036; [2002]All E.R.(D)381.

この事件も、1984年データ保護法が施行されていた時期に発生したものである。

あるソリシタから、自分の顧客に対して税金の支払いを求める文書を送付するために、自治体がソリシタの事務所の住所情報を用いたという旨の苦情が情報コミッショナー事務局に持ち込まれた。情報コミッショナー事務局の調査の結果、データを使用するにあたって義務付けられている登録の期間が終了していたことが判明し、自治体は催促状が来ていたにもかかわらず、多忙と事務的なミス (**pressure of work and clerical error**) によって登録更新をしていなかったことを認めた。登録が無効になっている間も、自治体による個人データの取り扱いが続いていたので、情報コミッショナー事務局は、自治体を無謀による 1984年データ保護法5条に違反で起訴した。

この事例において問題になったのは、データ使用のために登録を義務付けられているのは自治体であったが、個人データを使用したのは従業員であったということである。治安判事裁判所において公訴が棄却され、法律問題記載書 (**case stated**) の方法で上訴された。文書では、無謀の有無を判断する際に、自治体の行為と責任はどのように考慮されるべきであるかということと、確実な登録を怠ったことは無謀を構成するのに十分な要素であるのか否かということが問われていた。高等法院女王座部は、「この事件で問題となった自治体のような地域の団体が登録更新をしなかった場合、その不作為の認識があったことが合理的に推測され、このケースでは、自治体が関連する公務員の行為を通して、更新の必要性和、更新をしていなかったことに気づいていた場合には、その推測が強化される。その後、正当な範囲で業務を行う他の公務員の行為の結果として、自治体が登録なしに個人データを用いる場合は、自治体には禁止に対する違反につき、故意または無謀があったと考えるべきである」と判示した。

この事例は、登録更新を怠った主体と実際にデータの使用をした者が異なることから、自治体の無謀を検討する際には、データ使用における従業員の行動を合わせて考慮するという判断枠組みを提示するものである。本件はデータ使用にあたる職員を管理する立場にあったといえる自治体自らの無登録に関する無謀が問題となった事例であるが、従業員が55条に違反して情報を取得等した場合に、使用者の立場にある者は刑事責任を負うのかということも問題となっている。例えば、ソリシタに命じられて情報収集等を行っていた私立探偵が55条に違反し、ソリシタがその情報を私立探偵経由で得た場合、ソリシタが

私立探偵に対して55条に違反しないようにとの適切な助言をする等の予防措置を事前に採っていた場合は、当該ソリシタは情報やデータを「故意または無謀により」入手したとはいえないと解されている⁴⁹。

これらは55条違反の犯罪において無謀の有無が問題となったものとして代表的な判例であるが、無謀の意義が直接的に言及されているのは(1)のアムネスティ事件である。アムネスティ事件では、深刻で有害な結果が発生するという予見があったか否かという観点から無謀の有無が争われたが、前述の通り、このような理解はCaldwell[1982]AC341にも見られる。Caldwell事件では、「財産が破壊または損害されるか否かについて、行為者が無謀であったと認められるのは以下の場合である。(1) 財産が破壊または損害される明白な危険を創出する行為に出て、そして(2) そのような危険の可能性について何らの考慮せずに行為に出た場合、またはそのような危険を認識しながらも行為に出た場合である」と判示された。ここでいう「危険」というのは正当化されない危険のことであり、自動車の通常の運転や、医師による手術等は認められている。正当化される危険か否かは、行為者の主観によって決まるのではなく、裁判所が当該行為の社会的有用性と、深刻な侵害結果の発生する可能性を比較衡量して判断するのである⁵⁰。

Caldwell事件判決における無謀概念は、危険のあることを認識せず行為に出た場合と認識した上で行為に出た場合の両方をカバーしていたが、Caldwell事件以降に出されたG[2003]UKHL50によって、無謀の有無の基準が変更された。G事件では、「行為者が、1971年刑事毀棄法1条所定の無謀によって行為に出たか否かは、以下の観点から判断される。(i) 存在し、または存在するであろう危険を行為者が認識しているという状況、(ii) 発生するであろう結果の認識を行為者がしている場合の結果と、行為者が認識しているという状況下ではそのような危険を冒すのは不合理であるということ」と判示された。この判断は1971年刑事毀棄法の犯罪における無謀が問題となった事例に対するものであるが、行為者が危険を認識していたことと、危険を冒すことの不合理性によって無謀の有無を判断する手法は一般的に定着しているようである⁵¹。Caldwell事件判決の基準では、危険に対する認識があった場合もなかった場合も両方含んでいたのも、無謀と不注意(negligence)の区別が曖昧になるという問題があったが、G事件判決により、両者の区別を危険性に対する認識の有無で明確に区別することが可能になったと解されている⁵²。したがって、今後はデータ保護法55条違反の犯罪における「無謀」も、正当化されない危険性を認識した上で行為に出ることとして解釈されることになると思われる。

⁴⁹ Evans, *supra* note,45.

⁵⁰ Russell Heaton and Claire de Than,Criminal Law 3d ed, Oxford University Press,2010, 66.

⁵¹Heaton et al, *supra* note 50, at 73.

⁵²Heaton et al, *supra* note 50, at 73.

第3節 情報コミッショナーによる個人情報保護の現状について

前節までは、1998年データ保護法55条の規定の意義について検討してきた。続いて、本節では55条の運用の在り方を含んだ情報コミッショナーの実務について扱うこととする。

1998年データ保護法は、女王から独立した第三者機関として情報コミッショナー (Information Commissioner) と審判所 (The tribunal) を置いている。情報コミッショナーは個人情報保護に関して直接的な監督を行っており、51条(1)項では「データ管理者が善良な実務を守ることを促進し、特に、データ管理者が本法に基づく要件を遵守することを促進することに関し、本法に基づき自らの権能を行使する」ことが情報コミッショナーの義務であると規定されている。具体的な業務には、データ管理者からの通知事項を登録簿に記録する(18条・19条)、データ保護原則に違反したデータ管理者に対して執行通知を送る(40条)、違反者を訴追する(60条(1)項)といったものがある。そして、52条(1)項には「コミッショナーは、両議院に対して、本法における自らの権能の行使に関する年次報告書を提出しなければならない」と規定され、52条(2)項には「コミッショナーは両議院に対して、自らが適切であると判断した権能について、他の報告書を適宜提出することができる」と規定されている。このように、情報コミッショナーは個人情報保護の推進のための活動を行っており、議会に対して責任を負っている。情報コミッショナーは1998年データ保護法52条(2)項に基づいて、「プライバシーの価値とは何か? (What price privacy?)」という報告書を2006年5月10日に、そして「続・プライバシーの価値とは何か? (What price privacy now?)」という第2報告書を2006年12月13日に提出している。これら2つの報告書では、個人情報の適切な保護のために罰則を強化すべきであるという提言がなされており、この報告書を受けて法改正も行われている点で興味深い。そこで、本節第1・2項ではこの2つの報告書から、刑罰に対する情報コミッショナーの考え方と実務について詳述する。

続いて、2010年4月から、情報コミッショナーにはデータ保護原則の重大な違反に対して制裁金を科す権限が与えられた。そこで、本節第3項では、情報コミッショナーによる制裁金の実務について検討する。

第1項 報告書「プライバシーの価値とは何か? (What prices privacy?)」

まず、この報告書では情報コミッショナーのリチャード・トーマス (Richard Thomas) 氏による序文があり、刑罰に関する問題意識が表れているので、少々長くなるが以下引用する。

「個人のプライバシーを保護することは、データ保護の法律における私の責任の中心的なものである。1998年データ保護法55条は、故意または無謀により、データを保有する機関 (organisation holding the data) の同意なく、秘密の個人データ (confidential personal data) を入手、開示、または開示を周旋することについて刑罰を設けている。今、

わが職員（筆者注：情報コミッショナー事務局の職員であると思われる）と警察による調査の結果、そのような情報の不法な売買に向けられた産業が広がっていることが明らかになった。

個人情報とは、それが有名人、政治家、その他の公的な人物に関する恥ずかしい秘密であろうと、またはいくらかの借金をしていると思われる私人の所在であろうと、価値のあるものである。これらの不正取引における全てのケースは、個人の私的な情報が含まれており、情報を保有する機関はその開示を認めていないという点で共通している。コンピュータに貯蔵されていることが多く、特定の個人として一人の人間を浮かび上げ得るジグソーパズルのピースのような情報がある。このような情報における取引は、個人のプライバシーに対する深刻な脅威となるので、これを本法の特別な権限に従って、議会に対して提出する最初のレポートとする。

現在、55条違反の犯罪には拘禁刑が設けられていない。秘密の個人情報の不正な周旋または売却に関するケースが裁判所に持ち込まれた場合、少額の罰金（**derisory fine**）か条件付き刑の免除（**conditional discharge**）にすぎない有罪判決が下されることが多い。軽い刑罰は世論におけるデータ保護に関する犯罪の重さを低く評価し、裁判のシステムにおいてさえ、犯罪の本当の重大性を隠蔽してしまう。同様に、刑罰が軽ければ、本来は私的なものにとどまっているべき秘密の情報を購入したり提供したりする行為を予防することは困難である。私が提案する解決策は、正式起訴による有罪判決を受けた者（**persons convicted on indictment**）に対して最大2年間の拘禁刑を、陪審によらない有罪判決（**summary conviction**）の場合は最大6か月の拘禁刑を導入することである。より多くの人々を刑務所に送ることが目的なのではなく、情報を購入する者であろうと提供する者であろうと、このような不正な取引に関わろうとする全ての人々を思いとどまらせることが目的である。

個人は、第三者が個人の情報に対する不正アクセスに成功した時に被害を受ける唯一の存在ではない。企業にも、顧客の信用と公共部門における信頼を失うリスクがある。情報社会の基盤とシステムが安全でない限り、情報社会を適切に構築することはできない。改革型政府（**Transformational Government**）のスローガンの下、政府は連携した公共サービスと連携したコンピュータ・システムのプログラムを作り出しているので、ギャップを埋めることはより切迫性を帯びる。しかし、政府の保有する情報へのアクセスが増加していることは、本来であれば法によってその入手を否定されている情報への手段を購入・詐欺・交換することを欲する者に対して道を開くものではないことを確認する必要がある。

これらの問題と重罰化の必要性は、憲法事項省（**Department for Constitutional Affairs**）に挙げられた。私が今のところ受け取った前向きな回答は励みとなるものである⁵³。このように、深刻化する個人情報への侵害行為に対する抑止力として、刑罰が期待されている

⁵³ What price privacy?

http://www.ico.org.uk/for_the_public/topic_specific_guides/~media/documents/library/Corporate/Research_and_reports/WHAT_PRICE_PRIVACY.pdf,3.

ことがわかる。

続いて、この報告書では、情報コミッショナー事務局への苦情受付の実態と罰金刑の実態調査の結果が「本法における苦情と訴追 (Complaints and prosecutions under the Act)」において記されている⁵⁴。これによると、1998年データ保護法が施行された2000年3月1日からの6年間で、情報コミッショナーに寄せられた苦情で55条に関するものは約1000件であり、自らのプライバシーが侵害されたと考える個人からの苦情が多い。情報コミッショナーは自らの訴追権限に基づいて、2002年11月中旬から2006年1月までの間、イングランドとウェールズの刑事裁判所と治安判事裁判所に対し、25件の訴追を行った。25件のうち、22件が有罪、2件が訴えの取り下げ (withdrawal)、1件が裁判官の命令による中止 (discontinuance on the orders of the judge) である。本報告書の別表 A⁵⁵に詳細が記載されており、22件の有罪のうち、1件は刑の絶対的免除 (absolute discharge)、5件が条件付き刑の免除 (conditional discharge) で、1犯罪あたりの罰金額は9件の場合で50ポンドから150ポンドで、複数事案において2000ポンドから3000ポンドであった。罰金の合計額が法定上限の5000ポンドの事案は1件のみであった。別表Aに記載されている訴追事例には、データ保護法55条に違反して個人データを取得または開示するものが多い。

情報コミッショナーは苦情の受付と訴追のみならず、犯罪の実態調査⁵⁶も行っている。情報コミッショナーは、秘密の個人情報が組織的に取引されていることを疑っていたので、デーヴォン&コーンウォール警察管区 (Devon & Cornwall Constabulary) の召喚状 (warrant) に基づき、組織的な法律違反・闇市場の証拠収集のため、サリー州 (Surrey) の建物等の捜査を行い各種の証拠を確保した。その結果、違法な情報取引の実態が明らかとなった。報告書によると、情報を購入するのはメディア (特に新聞)、保険会社、債権者、夫婦・家族関係の紛争の関係者、詐欺の意図を有する者や、証人や陪審員の脅迫を目的とする者などである。秘密の個人情報を得る方法は2つに大別され、一つは職務を通して情報にアクセスできる者を買収することである。もう一つは、データ主体や公務員に成りすまして情報を得る「ブラッキング (blagging)」という方法である。私立探偵がブラッキングに関わっており、得られた情報は仲介者を経て最終購入者に渡される。このような個人情報の違法な売買における料金の一覧も報告書に掲載されている。この中で最も低額なのは選挙人名簿の住所情報で、1件につき17.5ポンドである。最も高額なのは携帯電話の登録内容の750ポンドで、次に高額なのは犯罪情報の500ポンドである。機密性の高い情報の方がより高額で取引されていることがわかる。

このように、情報コミッショナーは個人情報の違法な取引による個人のプライバシーの侵害が発生しているという調査結果に基づいて、現行の55条には罰金刑しか設けられ

⁵⁴What price privacy? supra note53,12-13.

⁵⁵ What price privacy? supra note53, 38-39.

⁵⁶What price privacy? supra note 53,at 15-16,22,24.

ていないことを批判する⁵⁷。報告書は、個人情報の不正取得等に対する刑罰が軽いことは犯罪の重大性を矮小化することにつながり、判決も低額の罰金刑に留まっていることを指摘し、犯罪の予防のためには拘禁刑を設けるべきであると主張する。報告書は、データ保護法60条(2)項を改正し、55条違反の罪の法定刑を引き上げ、最大2年間の拘禁刑もしくは罰金またはその両方、陪審によらない有罪判決の場合は最大6か月の拘禁刑もしくは罰金またはその両方が違反者に科せられるべきであると提案する。「最大2年」という法定刑は、秘密の情報を不法に開示する行為につき「本条の罪を犯した者は、正式起訴による有罪宣告によって、2年を超えない拘禁刑または罰金、あるいはその両方に処せられる」と規定するIDカード法(ID Cards Act 2006)27条を参照したものである。

そして本報告書は、重罰化と共に、情報提供の流れに関わる全ての者が55条で有罪となり得ることも強調されるべきであると主張する⁵⁸。それまで、私立探偵(private investigators)は、情報取得のために他人を使ったり、仕事を他の私立探偵に下請けさせたりすることによって、刑罰から距離を取ろうとしていたが、このようなアウトソーシングを行ったとしても正犯(principal)は処罰を免れないことが指摘されている。私立探偵と何名かの仲介者が協力して情報取得が行われている実態に即した指摘であると考えられる。

第2項 第2報告書「続・プライバシーの価値とは何か？(What prices privacy now?)」

情報コミッショナーは、前項で扱った報告書の半年後に第2報告書を提出した。第1報告書では個人情報の不正取引の実態が詳述されていたが、第2報告書でも、不正取引に対して、強力な抑止とより深い認識と、組織によるコントロールが必要であると解されている。このような問題意識に基づくものとして、第2報告書では、2006年5月以降も個人情報の不正取引の事件が発生しており、情報コミッショナー事務所は2件の55条違反事件について訴追を行い、1件については警告(caution)を受け入れさせたことが述べられている⁵⁹。

まず、第1のケースとして、1998年データ保護法55条に違反して金融機関から入手した情報につき、私立探偵業者に関わっていない個人が情報コミッショナー事務所の警告を受け入れたことが挙げられている。続いて、訴追が行われたケースのうちの1つは、私立探偵会社を経営するAnthony Gerald Cliffordが、55条違反の罪について2006年11月3日に有罪を認めたというものである。Cliffordは多くの個人についての情報を取得した上で、それを売却したり、情報開示を周旋したりしており、情報を取得するためにブライッキングの技術を用いていた。

⁵⁷What price privacy? supra note 53,at 27.

⁵⁸ What price privacy? supra note 53,at 29.

⁵⁹ What price privacy now?

http://www.ico.org.uk/for_the_public/topic_specific_guides/~media/documents/library/Corporate/Research_and_reports/what_price_privacy_now_report.ashx,6-8.

もう1つのケースは、2006年11月14日、私立探偵であった Anderson 夫妻は、不法に情報を取得・売却した罪について認めたというものである。妻は14個の罪について、夫は11個の罪について罪状を認めたところ、妻には合計で4200ポンドの罰金、夫には合計で3300ポンドの罰金が科せられた。Anderson 夫妻はイギリス歳入税関庁 (Her Majesty's Revenue and Customs)、イギリスの大手電気通信事業者であるブリティッシュ・テレコミュニケーションズ (British Telecommunications plc) の他、様々な銀行を含む多くの機関から、ブラッキングの手法によって、電話番号や所得税の情報などの個人情報取得した。個人情報が不正に取得される多くの事例において、「ブラッガー (blagger)」が金融機関等に潜り込み、正規の職員を欺いて情報を開示させるということが行われている。

このように、情報コミッショナーは第1報告書の提出以後も、個人情報の不正取引の取締のために活動を続けており、第1報告書の刑罰に関する提案は行政府にも影響を及ぼした。2006年7月24日、憲法事項省(the Department for Constitutional Affairs)は、意図的かつ故意による個人データの悪用 (deliberate and wilful misuse of personal data) に対して刑罰を強化する政府協議 (government's consultation) を開始した。この協議文書 (consultation document)は、現行法の刑罰は個人データの不正取引を防止するために有効ではないという第1報告書の考え方に明確に言及しつつ、政府は1998年法60条を改正して、略式裁判では6月の拘禁刑を、正式裁判では2年の拘禁刑を導入することを提案した。個人情報の不正取引の防止のためには、55条に拘禁刑を導入する切迫した必要性があるという、第1報告書から一貫した情報コミッショナーの考え方が政府にも受け入れられているが、第2報告書の結論部分において、最も深刻なケース (the most serious cases) にのみ拘禁刑が用いられるべきであるとする情報コミッショナーの意見が記載されている。

情報コミッショナーによる報告書によって法案提出がなされ、2008年刑事司法及び入国管理法 (Criminal Justice and Immigration Act 2008) が2008年5月8日に成立した。この法律の77条は個人データの不法取得等に対する処罰を変更する権限 (Power to alter penalty for unlawfully obtaining etc. personal data) について以下のように定めている。

「77条(1)項 主務大臣(The Secretary of State)は、命令 (order) により、1998年データ保護法55条違反で有罪となる者に対し、次のような責任を負わせることができる。

(a)陪審によらない有罪判決の場合、所定期間 (specified period) 内の拘禁刑、もしくは法定上限額を超えない金額の罰金 (a fine not exceeding the statutory maximum)、あるいはその両方を科すこと

(b)正式起訴による有罪の場合、所定期間内の拘禁刑、もしくは罰金、あるいはその両方を科すこと

77条(2)項 第(1)項(a)(b)が定める「所定期間」は命令によって定められるが、以下の

期間を超えてはならない。

(a)陪審によらない有罪判決の場合は、12か月（または、北アイルランドでは6か月）

(b)正式起訴による有罪の場合は、2年

このように、法定刑の上限が情報コミッショナーによる提案に従ったものになっている。情報コミッショナーは刑罰の発動に対して積極的な姿勢を有しているが、最も深刻なケースにのみ拘禁刑が用いられるべきであると述べていることから、主務大臣の裁量を認めているのは刑罰の濫用を防ぐ趣旨によるものであると考えられる。

第3項 制裁金について

前述の通り、2010年4月から、情報コミッショナーには、データ保護原則の違反に対して制裁金（civil monetary penalty）を科す権限が与えられた。情報コミッショナーの2009年・2010年報告書によると、制裁金は重大なデータ保護原則違反を対象としており、上限は50万ポンドである⁶⁰。制裁金の言語に“civil”という単語を用いていることから、制裁金は刑罰としての罰金とは区別されることがわかる。制裁金が科され得る状況と、情報コミッショナーが個別のケースについて、どの程度の制裁金を科すのかということとは、國務長官によって承認された法的な指針（statutory guidance）に従う⁶¹。

2012年・2013年の報告書では、制裁金実務について次のように記載されている。

2012年に情報コミッショナーによって制裁金が科された違反事例は23件であり、2011年の合計件数の2倍を超えている。情報コミッショナーによると、制裁金制度は情報保護についての注意を喚起し、法令遵守を促すための手段であるので、制裁金には一般予防効果が期待されているようである。制裁金が科される事例の3分の2は、最も多くのセンシティブデータを扱う地域の健康行政セクターであり、イギリスの国営医療サービス事業団体は100万ポンドの制裁金を科された⁶²。

制裁金制度が導入されてから日が浅く、制裁金実務に関する情報コミッショナーの報告や、制裁金に関する先行研究は少ないものの、深刻な違反に対してのみ制裁金を科するという方針は一貫しているようである。イギリスデータ保護法には、センシティブデータの不正取得等を一般的な個人データと区別して処罰する特段の規定は設けられていないが、上記の通り、制裁金が科される事例の3分の2が、センシティブデータの違法な取り扱いが問題となったケースであるという事実がその代替措置となっている側面もあるだろう。

⁶⁰Information Commissioner's Office Annual Report 2009/10
http://www.ico.org.uk/upload/documents/library/corporate/detailed_specialist_guides/annual_report_2010.pdf,36.

⁶¹ Information Commissioner's Office Annual Report 2009/10,supra note 60,at 36.

⁶² Information Commissioner's Office Annual Report 2012/2013
http://www.ico.org.uk/about_us/performance/~media/documents/library/Corporate/Research_and_reports/ico-annual-report-201213.ashx,32-34.

第4節 センシティブな個人データ (sensitive personal data) に関する法的規制

第1項 センシティブな個人データに含まれるデータについて

1998年データ保護法には、センシティブな個人データ(sensitive personal data)という、日本の法律には規定されていない概念がある。日本では「センシティブ情報」と呼ばれることも多い。データ保護法2条によると、次のデータが「センシティブな個人データ」となる。

- (a)データ主体の人種または民族的出自
- (b)データ主体の政治的信条
- (c)宗教的信仰または類似の性質を持つ他の信仰
- (d)労働組合のメンバーであるか否か(1992年労働組合及び労働関係法における意味の範囲内で)
- (e)身体的または精神的な健康もしくは状態
- (f)性生活
- (g)犯罪をしたこと、または犯罪をしたと申し立てられていること、または
- (h)データ主体が犯した犯罪、もしくは犯したと申し立てられている犯罪に対する訴訟手続、そのような訴訟手続による処分、もしくはそのような訴訟手続において裁判所が下した刑の宣告

データ保護法2条は、上記のデータのみをセンシティブな個人データとして規定している。したがって、金融情報や年齢に関する情報はセンシティブな個人データには該当しない⁶³。人間の寿命の確率的研究に関するデータ (biometric data) がセンシティブな個人データに該当する可能性が検討されているが、データ保護法2条におけるセンシティブな個人データの一覧によって明確にカバーされているとはいえないことから疑問視されている⁶⁴。

国籍に関する情報はセンシティブな個人データに該当するか否かということが問題となる。ある個人がアメリカ国籍を有している場合には、外国からの移民である可能性もあるので当該個人の民族的な背景が特定される可能性は高くないが、ウガンダ国籍の場合には当該個人の人種や民族的出自が特定されやすいことから、国籍がセンシティブな個人データに該当するか否かを明確に判断するのは困難であるとする指摘⁶⁵がある。また、名前がそれ自体でセンシティブな個人データに該当するか否か、苗字のデータを取り扱うことによって、データ主体の人種や民族的な出自に関するデータを集めることになるか否かということも問題となっている。情報コミッショナーによると、苗字のデータの取り扱いが、顧客の一般的なデータベースなどの氏名リストを作成するようなものだったのか、それとも

⁶³ Richard Morgan and Ruth Boardman , Data Protection Strategy : implementing data protection compliance,Sweet & Maxwell,2003,7.

⁶⁴Jay, supra note 44,at 272.

⁶⁵Morgan et al ,supra note 6 ,at 93.

苗字から判明し得る人種や民族的出自の内容と関係のあるものだったのかによって異なるとされている⁶⁶。

ここまではデータ自体の取り扱いの問題であるが、写真がセンシティブな個人データに該当するか否かが問題となった事例として、*Naomi Cambell v MGN*[2002]EWHC 299 がある。この事例は、原告のナオミ・キャンベルが麻薬中毒から抜け出すための会合に出席した際の写真をイギリスの大衆紙ミラーが報道したというものである。裁判所は、キャプション付きの写真に含まれた情報は、彼女の身体的精神的な状態についての明確な情報であり、それゆえ彼女が麻薬中毒であることはセンシティブな個人データに該当すると判断した。

以上より、たとえ本人が他人に知られるのを好ましくないと考えるような性質のデータであっても、データ保護法2条で列挙されているデータに合致する内容のものであるかが慎重に検討されているといえる。センシティブな個人データが一般的な個人データよりも厳格な条件の下で取り扱われることから、センシティブな個人データの範囲が拡張されることによるデータ処理への萎縮効果を防ぐ趣旨なのではないかと思われる。

第2項 データの取り扱いの条件

センシティブな個人データの取り扱いについては、データ保護法の附則3で以下のよう規定されており、データを取り扱うには、以下の10個の「センシティブな個人データ取り扱いの目的に関する条件」の中の少なくとも1つを満たさなければならない。

1 データ主体の明示的な同意 (explicit consent) のある場合

2(1)データの取り扱いが、雇用に関するもので、データ管理者に付与された権利の行使または課せられた義務の履行のために必要な場合

(2)国務長官 (Secretary of State) の命令によって

(a) 特定され得るケースにつき (1) 項の適用を排除する場合、または

(b) 特定され得るケースにつき、命令の中で明記されたそのような更なる条件も満たされない限り、(1) 項の条件が満たされたとはみなされないことを規定している場合

3 (a) (i) データ主体またはその代理人の同意を得ることができないか、(ii) データ主体の同意を得ることができないとデータ管理者が考える合理的な理由があるが、データ主体または他の者の重要な利益を保護するためにデータの取り扱いが必要な場合、または

(b) データ主体またはその代理人の同意が不当に留保されている状況下で、他人の重大な利益を保護するためにデータの取り扱いが必要な場合

⁶⁶Carey, *supra* note40,at 87.

- 4 (a) 情報の取り扱いが、非営利で政治・哲学・宗教・労働組合の目的によって設立された団体の適法な活動の中で実施され、
- (b) データ主体の権利や自由を適切に保護するために取り扱われ、
- (c) 団体のメンバーである個人か、団体の目的との関係で定期的に連絡を取る個人のいずれかの者のみに関係するものであり、
- (d) データ主体の同意なく第三者に個人データを開示することを含まない場合

5 データ主体の慎重な措置の結果として公知された個人データに含まれる情報である場合

- 6 (a) データの取り扱いが、法的手続の目的で、または法的手続に関して必要な場合、
- (b) 法的なアドバイスを得るために必要、または
- (c) 法的権利を確立、行使、または防御するために必要である場合

7 (1) データの取り扱いが、

- (a) 司法の運営のために必要
- (aa) 貴族院か庶民院のいずれかの権能の行使のために必要
- (b) 制定法によって人に与えられる権能の行使のために必要、または
- (c) 国王、大臣または省の権能の行使のために必要である場合

(2) 国務大臣が命令によって、

- (a) 特定され得るケースにつき (1) 項の適用を排除する場合、または
- (b) 特定され得るケースにつき、命令の中で明記されたそのような更なる条件も満たされない限り、(1) 項の条件が満たされたとはみなされないことを規定している場合

8 (1) 情報の取り扱いが医療目的のために必要であり、

- (a) 健康に関する専門職が、または
- (b) それと同等の守秘義務を負う者が引き受けた場合

(2) この項において、「医療目的」は、予防医療、医学診断、医学研究、ケアの提供と治療、ヘルスケアサービスの運営の目的を含む

9 (1) 情報の取り扱いが

- (a) 人種または民族的出自に関する情報を含むセンシティブな個人データに関するもので
- (b) 異なる人種または民族的出自を持つ人々の間における機会または待遇の均等を促進または維持する目的のために必要であり、そして

(c) データ主体の権利と自由に対する適切な保護のために行われる場合

(2) 国務大臣は命令によって、(1) (a) と (b) 項の範囲内で、情報の取り扱いが (1) (c) 項の目的のために扱われているか否かについて明記することができる。

10 このパラグラフの目的のために国務大臣によって下された命令の中に明記された状況下で個人データが扱われる場合

以上がセンシティブな個人データを取り扱うための条件である。一般的なデータの取り扱いに関する附則 2 よりも条件が具体的で厳格であるという違いがある。そして、センシティブな個人データを取り扱うには附則 2 の条件と附則 3 の条件の両方を満たすことが要求される⁶⁷。ここからは、附則 3 に挙げられた条件のうち、附則 2 との相違が顕著な主要な条件について検討する。

まず、附則 3 の 1 項ではデータ主体の「明示的な同意」の必要性が明記されている。一般的なデータの取り扱いのための条件を規定する附則 2 では、「データ主体がデータの取り扱いについて同意している (The data subject has given his consent to the processing)」ことが条件の 1 つとして挙げられており、明示的でなくても同意があればよいとされているのに対して、データの重要性に鑑みて明確な同意が必要であるとされている。

附則 3 の 1 項は、書面による同意でなければ無効であるとするものではないので、明確であれば口頭での同意も認められる。しかし、「明示的な」という言葉は「明らかで不明瞭なところがない」という意味で解釈される傾向にあるので、同意が不明確であるという批判を回避するために、データ管理者は書面によって同意の存在を示すことが多い⁶⁸。

情報コミッショナーによって 2001 年 10 月に出された法的指針 (Legal Guidance) は「明示的な同意」な同意の内容について、「データ主体の同意が絶対的に明白 (absolutely clear) なものでなければならない。適切なケースにおいて、同意はデータの取り扱いについての具体的な項目 (specific detail of the processing)、扱われるデータの種類 (the particular type of the to be processed)、取り扱いの目的 (the purposes of the processing)、個人に影響を与えるデータの取り扱いの特別な状況 (special aspects of the processing which may affect the individual) をカバーするべきである」と述べている。このことから、情報コミッショナーも書面による同意を絶対的に要求してはいないが、データ主体が自らのデータを処理されることにつき、その種類や目的といった詳細について認識した上で、一切の曖昧なところのない明白な同意をしていることを要求しているといえる。

続いて、附則 3 の 3 条 (a) では「データ主体または他の者の重大な利益の保護」について規定されている。情報コミッショナーによると、「重大な利益」は生死に関わる状況 (life

⁶⁷Carey, *supra* note 40, at 88.

⁶⁸ Jay, *supra* note 44, at 275.

and death situations) であると解釈されている⁶⁹。一般的な個人データの取り扱いの条件を定める附則 2 の 4 条にも、「データ主体の重要な利益の保護のためにデータの取り扱いが必要であること (The processing is necessary in order to protect the vital interests of the data subject)」という類似の規定がある。しかし、附則 3 の 3 条は附則 2 の 4 条とは異なり「データ主体以外の者」という文言が加えられていることから、共同体の利益に資するという性質も有している⁷⁰。例えば、データ主体が伝染病に罹患しており、他の者にも伝染する危険がある場合、データ主体の健康状態に関するデータを用いることは附則 3 の 3 条によって正当化され得る。データ主体が意識不明または所在が不明の場合、データ主体がデータの取り扱いについて同意をすることはできないので、本条によって関連するデータを開示することが可能になる。データ主体が単に開示を拒否している場合にも、健康に関する権限を持つデータ管理者も、附則 3 の 3 条に基づいてデータ開示をすることができる⁷¹。附則 3 の 3 条が、医療目的のためのデータの取り扱いについて規定する附則 3 の 8 条といかなる関係にあるのかということについては明らかではないが、後述の附則 3 の 8 条はデータの取り扱いが健康に関する専門職によって行われることを要求している一方で、3 条はそのような限定をしていないという相違が見られる⁷²。

続いて、附則 3 の 7 条は司法運営等のための取り扱いについて規定している。附則 2 の 5 条の規定と類似しているが、附則 2 の 5 条 (d) が定める「公共の利益のために運営され、公的な性質を有する機能の行使 (for the exercise of any other functions of a public nature exercised in the public interest by any person)」という項目が附則 3 には存在しない。このような規定が欠けていることで、公共の利益を追求する慈善団体やその他の機関は、附則 3 の 7 条の下でセンシティブな個人データの取り扱いを正当化されない⁷³。このように、附則 3 の 7 条の下でセンシティブな個人データを扱う目的が司法の運営、議会の運営といった、範囲が比較的明確なものに限定することにより、データの扱いによってデータ主体の利益が損なわれる危険性を低減しようとしているものと思われる。

附則 3 の 8 条は、医療の目的によるデータの取り扱いに関する条文である。本条にいう「医療目的」の例が 8 条 (2) 項に列挙されているが、医療に関するその他の目的も含まれる⁷⁴。データを取り扱う主体である「健康に関する専門職」には、医師、歯科医師、看護師、薬剤師等の幅広い職業の者が該当する。

附則 3 の 9 条は、人種または民族的出自に関するセンシティブな個人データについての規定である。本条は異なる人種や民族的出自を有する者同士の機会と待遇の均等を促進・維持のためにデータが取り扱われることに限定しているが、データが他の目的よりも、そ

⁶⁹Morgan et al ,supra note63,at96.

⁷⁰Carey, supra note40,at 89.

⁷¹ Carey, supra note40,at 89-90.

⁷²Carey, supra note40 ,at 90.

⁷³Morgan et al,supra note 63,at 97.

⁷⁴Carey, supra note40 ,at 91.

のような機会と待遇の均等のために用いられていることをデータ管理者はどのように明らかにするのかという問題がある。本条の違反を回避するためには、データ管理者がそのような目的で人種や民族的出自に関するデータが取り扱われているか否かを注意深く吟味することが求められる⁷⁵。

附則 3 の 10 条は、国務大臣の制定した命令によってデータが取り扱われる場合についての規定である。本条を根拠として制定された命令として、センシティブな個人データの取り扱いに関する 2000 年データ保護命令 (Data Protection (Protecting of Sensitive Personal Data) Order 2000 SI 2000/417) がある。2000 年データ保護命令は 10 条から成り、センシティブデータの取り扱いのための条件を規定している。この命令で規定されている条件には、データの取り扱いが犯罪を予防したり見つけたりするのに必要である場合、一定の政治的機関による政治的意見についての情報を取り扱う場合、データの取り扱いがデータ主体に影響がなく、調査のために必要な場合等がある。2000 年データ保護命令に規定されている条件のいずれかを満たしていれば、1998 年データ保護法における附則 3 を遵守したということになる。

以上のように、附則 3 の条件は附則 2 よりも多く、制限的である。実際には、センシティブな個人データを合法的に取り扱うことができるか否かは、多くの機関がデータ主体の明示的な同意を得られるか否かに依存している⁷⁶。

第 5 節 小括

本章では、イギリス 1998 年データ保護法における個人データの不正取得等の犯罪の意義と、情報保護のための第三者機関である情報コミッショナーの刑罰に対する考え方、実際の実務と、センシティブな個人データの意義とその取り扱いのための条件について検討してきた。

まず、データ保護法 55 条は個人データを不正に取り扱う行為を広く処罰している。55 条のように違反者を直接的に処罰する規定を設けるに至った背景には、第 2 節の第 1 項で挙げたような個人データ関係の事件があり、それが社会問題に発展したことがある。特に、ブラッキングの手法を用いたり、数名の仲介者や私立探偵を使ったりすることで情報を不正に入手することも多く、情報の不正取引は悪質化・組織化している。犯罪は故意犯処罰が原則であるが、イギリス社会のこのような実態に鑑みると、故意または無謀によって情報を入手した場合も処罰の対象となるのは一つの規制方法としてあり得る。一方、日本では情報漏洩の事件が多発しているが、過失によるものも少なくない。刑事法の原則から見れば、過失犯の処罰を可能にするのは生命や身体などの重大な法益の侵害があった場合に限られるので、日本法において認識ある過失または認識のない単純な不注意による過失で情報漏洩が発生した場合に刑罰を発動させるためには、更なる根拠が必要となる。

⁷⁵ Jay, *supra* note 44, at 286.

⁷⁶ Morgan et al, *supra* note 63, at 99.

次に、イギリス1998年データ保護法では、女王から独立した第三者機関である情報コミッショナーがデータ保護のための監督を行っている。情報コミッショナーは、犯罪の捜査や訴追、法改正についての提言も行っており、その権限は広い。2010年4月からは、データ保護原則の違反に対して制裁金を科す権限も付与された。情報の不正取得や違反以外の一般的な刑事事件を訴追する検察官ではなく、情報についての専門機関である情報コミッショナーが捜査や訴追を行うという制度には、訴追や刑罰の恣意的な濫用を防ぐという意義がある。また、制裁金制度も違反に対する抑止力となっていると考えられる。

そして、このような権限を与えられているのみならず、毎年報告書を提出することを義務付けられることで、情報コミッショナーが実務を適切に行っているか否かがチェックされている。イギリスの情報コミッショナーのような専門の第三者機関を設けて一定程度の権限を付与する法制度が日本にも必要か否かは、情報の保護に関する既存の機関の実務の現状に鑑みて検討する必要があるが、イギリスの情報コミッショナーの制度には一定以上の意義がある。また、情報コミッショナーの報告書にも記載されていたように、情報コミッショナーは個人データの保護のための厳罰化に対して積極的な姿勢を採っている。イギリスでは個人データの不正取扱に対して刑罰を発動することについて、日本ほどの抵抗感がないように思われるが、イギリスで発生している個人データの不正取扱の事件が立法事実となり、刑罰を用いることに対して説得力を持たせているのであろう。そして、専門機関である情報コミッショナーが、現状分析や調査を行った上で厳罰化の提言をしていることが、刑罰への更なる後押しとなっている。

続いて、イギリスの1998年データ保護法では、センシティブな個人データが一般的な個人データとは区別されている。センシティブな個人データは、健康状態、思想的信条、人種、民族的出自といった、それが侵害されたり不当に取り扱われたりした際にプライバシーの侵害の程度が大きいとされるデータであり、データ保護法附則3所定の条件は、附則2に規定されている一般的な個人データの取り扱いの条件よりも多く、厳格である。イギリスのデータ保護法では、データの重要性によって一般的な個人データとセンシティブな個人データを区別しているが、センシティブな個人データを不正に取り扱う行為をそれ以外の個人データの場合に比べて重く処罰する旨の規定は存在しない。また、センシティブな個人データを取り扱うにあたり、データ管理者は附則3と附則2の条件のうち1つ以上を満たす義務があり、その義務に違反した場合にはデータ保護原則1条の違反となるので、情報コミッショナーからの是正通知を受けることになる。是正通知についても、センシティブな個人データについて違反があった場合には一般的な個人データの違反の場合に比して厳しい通知を行うといった区別はデータ保護法上ではなされていない。イギリス1998年データ保護法が、センシティブな個人データという概念を設け、一般的な個人データより厳格に保護されるべきものとして位置づけている一方で、刑罰の加重や、データ管理者の違反に対する通知の種類等に差異が設けられていない理由は定かではないが、違反や情報の不正取得が行われた後の制裁よりも、センシティブな個人データが不当に扱

われることに対する事前の予防に重点を置くのがデータ保護法の趣旨ではないかと思われる。前述の通り、センシティブな個人データを取り扱う際には附則 3 の条件と附則 2 の条件をそれぞれ 1 つ以上満たすことが要求される。データ主体の明示的な同意があれば、附則 3 の 1 条と附則 2 の 1 条の要件を両方満たすことが可能になるが、データ主体が同意していない、または拒否している場合はデータの取り扱いが困難になる。例えば、附則 3 の 7 条に規定されている司法運営のためにデータを取り扱う場合には、附則 3 の 7 条と附則 2 の 5 条の内容が重なり合うので、附則 3 の条件を満たす場合には同時に附則 2 の条件も満たすことが可能になろう。しかし、センシティブな個人データを取り扱おうとする理由や目的がより抽象的になればなるほど、両方の条件を満たすことは困難となり、安易なデータの取り扱いに対する抑止力が働く。このように、センシティブな個人データについては、データ管理者の責任を重くすることで不正な取り扱いや違反の予防を図っているのではないかと考えられる。

確かに、データ取り扱いのための条件を厳格化することは、違反を抑止するのに一定の効果があるだろう。しかし、情報コミッショナーの第 1 報告書には個人データの不正取引を抑止し、個人のデータに対する有効な保護を行うためにはデータ保護法 55 条違反の罪の法定刑を引き上げ、拘禁刑を設けるべきであると記載されていたが、センシティブな個人データについては特段の言及がなかったことには疑問がある。予防のために厳罰化をすべきであるというのであれば、侵害や違反があった場合により重大なプライバシー侵害につながるセンシティブな個人データの不正取得の罪の法定刑を一般的な個人データの場合に比して重くするという発想にならないのはなぜだろうか。個人情報不正取得等を直接的に処罰する規定の在り方を検討する際には、センシティブな個人データとそれ以外の一般の個人データとの間に法定刑の差を設けるべきか否かが問題となるだろう。

第 4 章 フランス法における個人情報保護

本章では、フランスにおける情報処理・情報ファイル及び諸自由に関する法律 (La loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978) について扱う。この法律は、1978 年に制定されて 2004 年、2011 年に改正されているが、1978 年法と呼ばれている。

具体的な検討に入る前に、1978 年法が成立するまでの背景とその後の改正の流れについて述べる⁷⁷。フランスにおいて、プライバシー (la vie privée) や人格 (la personnalité) の保護の必要性が自覚されるようになったのは 1960 年から 1970 年代である。報道機関によってプライバシーが侵害される事例が増加したことを受けて、1970 年 7 月

⁷⁷立法の流れについては、多賀谷一照「フランスのプライバシー保護立法と運用の実態」ジュリスト臨時増刊・情報公開・プライバシー(1981年)248～249頁、Agathe Lepage, Patrick Maistre du Chambon, Renaud Salomon, Droit pénal des affaires 3e édition, Lexis Nexis, 2013, p.207-211.

1970年の法律は、私的生活の尊重に対する権利 (*droit au respect de la vie privée*) を設けた。1970年代は、個人の自由に対する脅威となり得るほどに情報科学の発展した時代でもあった。行政のファイルと個人の目録のために自動化されたシステム (*système automatisé pour les fichiers administratifs et le répertoire des individus*. 略称はSAFARI) という計画のあることが、1974年3月21日のル・モンド紙の記事によって明らかになったが、市民を番号によって識別し、行政が保有する個人の情報を統合してデータベース化するこの計画は大衆の強い批判を受けた。批判を鎮めようとして、政府は1974年12月、法務大臣 (*garde des Sceaux*) の支配下に「情報処理と自由委員会 (*Commission informatique et libertés*)」を設けた。この委員会は、個人の自由に対して危険を及ぼすことなく情報科学を発展させるための措置を提案することを義務付けられていた。この委員会は、コンセイユ・デタ (*Conseil d'État*) の副院長が委員長を務め、司法関係者・学識経験者等の12名の委員で構成された。委員会は1975年6月に報告書を作成し、政府はこの報告に基本的に従う形の法案を1976年に国民議会に上程した。この法案が両院議員で審議され、調整を経て可決された。

1970年に新設されたフランス民法典9条1項は、「何人も自己の私生活を尊重される権利を有する」と規定し、2項では「裁判官は、被った損害の補償は別として (*sans préjudice de la réparation du dommage subi*)、係争物寄託 (*séquestre*)、差押え (*saisie*) の他、私生活の内奥に対する侵害を回避する又は停止させるのに適切なすべての措置を命ずることができる。緊急の場合は、これらの措置は急速審理 (*référé*) によって命じられる」⁷⁸とされている。このように、1978年法以前にも、私生活の尊重に関する権利を定める法律は存在していたが、情報の問題は技術的な性格を有する。その上、情報処理の局面における個人の保護の問題は、ただプライバシーの問題のみを検討すればよいものではなくなっていた。一定の情報は個人的な性質を有し、個人情報の中でも性別、人種的または民族的出自、職業に関する情報、仕事で用いるメールアドレスなど、必ずしもプライバシーとは関係のないものもある。このことから、委員会は立法によって行政委員会を創設することを提案する。この提案によって、情報に対する規制を行う独立行政機関として、情報処理・自由全国委員会 (*Commission nationale de l'informatique et des libertés*. 以下、CNILと略す) が1978年法に規定されることとなった。

1978年法はフランスにおける国内的な要請を受けて成立したが、1980年代から1990年代にかけて、個人情報保護の問題が国際的に議論されるようになった。情報科学技術の発展、特にインターネットの発展は情報流通を容易化したが、このような技術の発展によって情報が売却や取引の対象となり、諸外国と同様に、情報は財産的価値を有するに至った。そして、膨大な量の情報を取り扱う企業にとっても、情報は重要な関心事と

⁷⁸フランス民法9条の邦訳は、稲本洋之助「フランス民法典第1篇—その原始規定(1804)と現行規定(1971)—」(東京大学社会科学研究所「家」制度研究会・1972年)6頁を参照した。

なった。このような国際的な情勢から 1995 年に EU データ指令が出され、2004 年に法改正が行われた。1978 年当時と比して、CNIL の権限が強化されている。

第 1 節 1978 年情報処理・情報ファイル及び諸自由に関する法律の概要

本節では、フランス 1978 年法における情報処理の諸規則と CNIL の権限、そして刑法における情報侵害行為の処罰規定について概要を述べる。

第 1 項 基本事項について

(1) 法律の目的、規制対象

1978 年法 1 条は、法律の目的を以下のように規定する。

「情報処理は、市民の各々に奉仕するものでなければならない。情報処理の促進は、国際協力において行われなければならない。情報処理は、人間のアイデンティティ (*identité humaine*)、人権 (*droits de l'homme*)、私生活 (*la vie privée*)、個人の自由または公的な自由 (*libertés individuelles ou publiques*) を侵害してはならない」⁷⁹。

本法の保護対象である個人情報 (*données à caractère personnel*) は、「自然人に関するあらゆる情報のうち、識別番号または個人に固有の一つ若しくは複数の要素を参照することで、直接または間接に個人を識別しまたは識別可能なもの」と定義されている (第 2 条)。

本法で「個人情報処理」という行為は、「個人情報に関わる全ての操作または操作の全体、特に収集 (*collecte*)、記録 (*enregistrement*)、編集 (*organisation*)、保存 (*conservation*)、適用 (*adaptation*)、もしくは修正 (*modification*)、抽出 (*extraction*)、閲覧 (*consultation*)、利用 (*utilisation*)、転送 (*transmission*)、配布 (*diffusion*)、もしくは他の方法による伝達 (*communication*)、結合 (*rapprochement*)、相互接続 (*interconnexion*)、アクセス停止 (*verrouillage*)、消去 (*effacement*)、または破棄 (*destruction*) のような、情報に関する操作または操作の全体」として定義されている (第 2 条)。

(2) 個人情報処理責任者の定義とその義務

そして、個人情報処理責任者 (*responsable d'un traitement de données à caractère personnel*) は、情報処理の目的と方法を決定する個人、あるいは公的な機関、部局、組織であると規定されている (第 3 条 I)。

情報処理が適法とされるためには、情報の関係者 (*la personne concernée*) の同意を得るか、以下の 5 つの要件のうち 1 つを満たさなければならない (第 7 条)。

① 処理責任者に課せられる法的義務の尊重

② 関係者の生命の保護

⁷⁹ 1978 年法の邦訳は、清田雄治「フランスにおける個人情報保護法制の現況—2004 年フランス新個人情報保護法の成立と憲法院判決—」愛知教育大学社会科学論集 42・43 号 (2005 年) 277～312 頁、「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 (平成 20 年 3 月)」におけるフランスの章 (下井康史) を参照した (<http://www.caa.go.jp/seikatsu/kojin/h21report2.pdf>)。

- ③処理責任者または名宛人の行う公的な役務上の任務遂行
- ④関係者が当事者となる契約または関係者の要請に基づく契約前の措置の遂行
- ⑤関係者の基本的利益、権利、自由を尊重するという条件下で、処理責任者または名宛人の追求する正当な利益の実現

上記のように、情報処理の適法化要件の一つとして処理責任者の法的義務が挙げられているが、法的義務には（１）情報提供者に対する告知義務、（２）情報収集を行わない場合の告知義務、（３）安全措置等がある。

まず、（１）情報提供者に対する告知義務について、本法３２条１項は「情報収集の対象者は、前もって知らされている場合を除き、情報処理責任者またはその代理人（*son représentant*）から、以下のことを告知される。①情報処理責任者、または代理人の身元、②情報処理の目的、③回答の義務的または任意的性格、④回答がなかった場合に発生し得る結果、⑤情報の名宛人と、その範疇、⑥この章の第２節に規定されている個人の権利、⑦EU外への情報の転送について」と規定している。

続いて、（２）情報収集しない場合の告知義務について、本法３２条３項は「情報処理責任者または代理人は、情報の記録または第三者への伝達が検討されている場合には、３２条１項に列挙された事項を、遅くとも情報の最初の伝達の際に告知するべきである」ことを定める。犯罪の予防や捜査、立証または起訴を目的とした情報処理の場合、告知義務に関する３２条の規定は適用されない（３２条６項）。

そして（３）安全措置について、本法の３４条は「処理責任者は、情報の安全を保持するため、特に情報の歪曲、破損、または許可されていない第三者によるアクセスを排除するために、情報の性質と情報処理から生じる危険性の観点から、あらゆる有効な予防措置を行わなければならない」と定めている。以上が情報処理責任者の法的義務であり、これらの義務の全てを履行すれば個人情報処理が適法なものとして認められる。

（３）センシティブ情報の定義と収集の適法化要件

（２）で述べたように、１９７８年法では個人情報処理の適法化要件が規定されているが、本法８条では、特別な保護を要するものとして「センシティブ情報（*données sensibles*）」の定義とその収集の適法化要件が定められている。８条１項では、人種的または民族的出自、政治的・哲学的・宗教的意見、労働組合への所属が直接的に、または間接的に明らかになる個人情報と、健康もしくは性生活に関する個人情報を収集したり処理したりすることが原則的に禁止されている。

８条２項では、このようなセンシティブ情報の処理が認められるための例外的な場合について以下のように規定する。

①関係者が情報処理について明示的な同意（*consentement exprès*）を与えている場合（関係者の同意によっても、８条１項に規定されている禁止が解除され得ないことを法律が予定しているような場合を除く）。

- ②情報処理が人の生命の保護のために必要であるが、関係者が法的無能力または物理的な不可能によって同意を与えることができない場合。
- ③営利を目的としない宗教、哲学、政治、労働組合の結社またはその他のあらゆる組織によって行われる情報処理であり、この結社・組織の目的に対応する情報を対象とし、その結社・組織の構成員または定期的にその結社・組織と接触する個人のみに関するものであり、関係者の明示的な同意がなければ第三者に伝達されない場合。
- ④関係者によって公表されている個人情報に対する処理が行われる場合。
- ⑤裁判上の権利の証明、行使または防御に必要な処理が行われる場合。
- ⑥医療専門職または刑法 226-13 条が規定する職業上の守秘義務を有する者によって、予防医療（*médecine préventive*）、医学的診断（*diagnostics médicaux*）、診療または治療の提供（*administration de soins ou de traitements*）、健康サービスの管理（*gestion de services de santé*）の目的のために必要な処理が行われる場合。
- ⑦統計に関する義務、連携および秘密に関する 1951 年 6 月 7 日法を遵守し、統計情報国家評議会（*Conseil national de l'information statistique*）の意見を受けて、本法 25 条の定める条件下で、国立統計経済研究所（*l'Institut national de la statistique et des études économiques : INSEE*）または省の統計部局が実施する統計処理が行われる場合。
- ⑧医療分野の研究のために必要な処理であり、本法第 9 章に定める方式に従う場合。

続いて、8 条 3 項と 4 項も、情報処理が例外的に認められる場合について定めている。8 条 3 項は、CNIL が情報処理の目的を考慮して、本法に適合することを事前に承認した匿名化の方法による短期間の処理が行われる場合について、8 条 4 項は、公益上の必要性があり、CNIL が情報処理を許可した場合はセンシティブ情報の処理が適法化されることを規定する。

（４）犯罪等に関わる情報と収集の適法化要件

また、1978 年法では上記のセンシティブ情報の他に、犯罪（*infractions*）、有罪判決（*condamnations*）、保安処分（*mesures de sûreté*）に関する個人情報も、原則的に処理が禁止されている。本法 9 条によると、情報処理が例外的に認められるのは以下の場合である。

- ①司法機関、公的機関、公的サービスを管理する法人が、その法的な権限の枠内で情報処理をする場合
- ②司法補助職に就く者が、法律の定める任務の遂行のために必要最低限の範囲で情報処理する場合
- ③知的財産権法 321-1 条および 331-1 条所定の法人が、その管理する権利資格者として情報処理を実施する場合、または、同法 I、II、および III 部 II に規定されている権利の防御の確保のため、当該権利を侵害された被害者のために情報処理を実施する場合

なお、現在の 9 条 2 項と 3 項の間に、「犯罪の被害者である法人、もしくは当該法律に定

められた要件において、その予防、不正行為の摘発および被った損害の回復という厳格な目的で、上記被害者のために活動する法人が情報処理を行う場合」という例外規定が存在したが、2004年7月29日の憲法院の違憲判決によって削除された。

このように、1978年法では一般的な個人データとは区別された枠組として、センシティブ情報と、犯罪等に関する情報があり、これらの情報の処理の適法化要件は、一般的な個人データのそれに比して厳格で具体的である。

(5) 個人の権利

続いて、1978年法における個人の権利について概観する。本法38条によると、「すべての自然人は正当な理由 (*des motifs légitimes*) がある場合、自己に関する個人情報処理の対象となることを拒否する権利を有する」。一般的な情報処理に対する拒否には「正当な理由」が求められる一方で、個人情報が市場調査や販売目的に利用される場合には、負担を負うことなく (*sans frais*) これを拒否する権利が認められる (38条)。

このような拒否権の他に、個人には情報に関する質問権や、情報の訂正・利用停止・消去を要求する権利なども認められている。本法39条Iによると、全ての自然人は自己の身元を証明した上で、個人情報処理責任者に対して以下のことを質問することができる。

- ①自己の個人情報が当該情報処理の対象になっているか否かの確認
- ②当該処理の目的、処理される個人情報の種類、個人情報が開示される第三者あるいはその種類についての情報
- ③必要に応じて、EU 非加盟国に在住する者に対する個人情報の転送についての情報
- ④自己の個人情報、およびその取得元に関して個人情報処理責任者が保有する全ての情報に関するアクセス可能な情報の提供
- ⑤自己に対して法的効力を有する決定が、自己の個人情報の自動処理に基づいてなされた場合、当該自動処理の基礎となった論理 (*logique*) を知ることができ、それに異議を申し立てることを可能にするような情報。ただし、個人に知らされる情報は知的財産法所定の著作権を侵害するものであってはならない。

また、個人情報処理責任者に対して自己の個人情報の複写を要求する権利も認められているが、当該質問や要求が、その数・反復性・体系性から見て不当なものであることが明らか場合は、個人情報処理責任者はそれらを拒否することができる (39条II)。

続いて、本法40条では「全ての自然人は、自己の身元を証明した上で情報処理責任者に対して、情報が不正確・不完全・不明確・あるいは過去のものであるか、収集や利用、提供、保存が禁止されている場合に、情報の訂正・修正・更新・利用停止・消去を求めることができる」とされている。このような請求がなされた場合、情報処理責任者は個人に費用の負担をさせることなく必要な処理を行ったことを証明しなければならない (40条)。

以上、1978年法が定める基本事項について概観した。次項では、フランス個人情報保護法制における重要な第三者機関である CNIL の概要について述べる。

第2項 情報処理・全国自由委員会（CNIL）

（1）独立性とメンバー構成

イギリス1998年データ保護法と同様、フランス1978年法にも情報の取り扱いを規制する第三者機関に関する規定がある。この第三者機関は情報処理・自由全国委員会（Commission nationale de l'informatique et des libertés）であり、CNILと略される。CNILの主な権限は、事前規制、義務違反行為に対する制裁、政府および民間団体への助言等であり（11条）、これらの権限の行使にあたり、CNILの委員はいかなる機関からの指図（instruction）を受けず（21条）、独立した機関であることが保障されている。

CNILは、次の17名のメンバーで構成される（13条I）。

- ①国民議会（フランスの下院 l'Assemblée nationale）および元老院（フランスの上院 le Sénat）によって任命された議員各2名
- ②経済・社会・環境評議会（Conseil économique, social et environnemental）の総会で選出された委員2名
- ③conseil d'Etat（Conseil d'État）の総会で選出された現職の構成員または元構成員2名
- ④破毀院（Cour de cassation）総会で選出された現職の構成員または元構成員2名
- ⑤会計院（Cour des comptes）総会で選出された現職の構成員または元構成員2名
- ⑥デクレ（décret）によって任命される、情報処理または個人の自由に関する有識者3名
- ⑦国民議会および元老院議長によって任命される、情報処理に関する有識者2名

（2）事前規制

CNILは、個人情報の取り扱いに対して事前規制と事後規制を行う。まず、1978年法における事前規制は届出（déclaration）と許可（autorisation）の2つに分かれている。

I 届出

個人情報を自動化処理する際には、原則として CNIL に届出をしなければならない（22条I）。通常の届出は23条に定められているが、個人情報処理が日常的（courantes）なものであり、プライバシーや個人の自由を侵害しないと考えられるものについては24条所定の簡易届出（déclaration simplifiée）の対象となる。CNILが、処理される情報の種類や処理目的などの簡易化基準（normes simplifiée）を公示し、基準の中の一つに合致する情報処理は簡易届出の対象となる。その一方で、23条による通常の届出では、処理責任者の身元と住所、情報処理の目的、処理の対象となる個人情報、処理される情報の保存期間などの多くの事項を CNIL に申告することが義務付けられる。

II 許可

CNILによる許可を必要とする情報処理の主なものは、以下の通りである（25条I）。

- ①自動処理か否かを問わず、8条所定のセンシティブ情報の処理のうち、1）国立統計経済研究所または省の統計関係部局の一つが行う統計処理、2）短期匿名処理（bref délai d'

un procédé d'anonymisation) の対象となるもの、3) 公益 (l'intérêt public) を理由とするもの

②遺伝学的情報 (des données génétiques) に関する自動処理。ただし、医師や生物学者による情報処理で、予防医療、医学的診断、診療や治療のための投薬を目的とするものを除く。

③自動処理か否かを問わず、犯罪・有罪判決・保安処分に関する情報処理。ただし、情報の関係者の保護という司法補助者の任務に必要な情報処理を除く。

④情報処理の性質 (nature)、範囲 (portée)、目的 (finalités) から、法的利益 (bénéfice d'un droit) や給付 (prestation) の利益、契約 (contrat) の利益を個人から剥奪するおそれがあるものの、法令の規定が欠如している場合の情報処理

⑤公的なサービスを管理する法人 (または複数の法人) に属し、異なる公益に関する目的を有するファイルの相互接続 (interconnexion)、および、別の個人に属し、主たる処理目的が異なるファイルとの相互接続

⑥個人識別全国名簿における個人登録番号を記載した個人情報に関する処理、および個人登録番号を含まないものの同名簿への参照を必要とする処理

⑦個人の社会的困窮に関する評価 (appréciations sur les difficultés sociales) を含む情報の自動処理

⑧個人の調査に必要な、生物測定学的な (biométriques) 情報を含む自動処理

以上のような、センシティブ情報やそれに類似した情報に関わる情報処理を行う場合には届出以前に CNIL から許可を得る必要があり、その意味で一般的な情報よりも手厚く保護されている。

(2) 事後規制

ここからは、違反に対する事後規制について概観する。情報処理責任者が1978年法に違反した場合、CNILによる制裁の対象になる。まず、CNILは義務を履行しない情報処理責任者に対して、対審手続の上で (après une procédure contradictoire) 警告 (avertissement) を発することができる (45条I)。この警告が制裁としての性質を有する (Cet avertissement a le caractère d'une sanction) ことも併せて規定されている。また、CNILは期限を定めて違反を止めるよう催告する (mettre en demeure) こともできる。情報処理責任者が、自己に出された催告に従えば制裁の手続は終了するが、情報処理責任者が催告に従わなかった場合、CNILは対審手続を経て、次のような制裁 (sanction) を行うことができる。

①国家による情報処理の場合を除き、金銭的制裁 (sanction pécuniaire) を科すことができる。制裁の金額は、違反の重大性と、違反によって得られた利益を比較衡量して決定される。初犯であれば、150000ユーロ、5年以内に違反が繰り返された場合は (En cas de manquement réitéré) 300000ユーロが制裁金の上限である。一方、企業が対象と

なる場合は、300000ユーロを上限として、総売上額の最大5%までとされている。刑事裁判が同一事実または付帯事実について判断するのに先立って CNIL が金銭的制裁を確定させた場合、CNIL による制裁金額は、刑事裁判の確定した金額から控除され得る（47条）。

②22条の届出の対象となる処理の場合は処理中止命令（*injonction de cesser le traitement*）を、25条による許可決定の場合には撤回（*retrait*）を命じることができる（45条I2号）。

③処理の実行または処理されたデータの利用が、本法1条に規定される権利と自由の侵害をもたらす場合に、CNIL は対審手続を経て、国务院（*Conseil d'Etat*）のデクレ（*décret*）によって定義される緊急の手続（*une procédure d'urgence*）を開始することができる（45条II）。

本条にいう「緊急の手続」には、1）最大3か月までの処理実施の中断の決定（*décider l'interruption de la mise en œuvre du traitement*）、2）最大3か月までの一定の個人情報に対するアクセス停止（*verrouillage*）、3）1条に規定されている権利と自由に対する侵害が重大で差し迫っている（*grave et immédiate*）場合、急速審理（*référé*）によって、必要に応じては罰金強制（*astreinte*）を用いて権利と自由の保護に必要な措置を採ること等がある（45条II・III）。

これらの制裁に加えて、1978年法51条では CNIL の活動を妨害する行為が処罰の対象となっている。犯罪類型は、1）任務遂行の拒否、2）文書の提出拒否、隠匿、消去、3）虚偽情報の提示、直接のアクセスが可能な形式において（記録の）内容を含まない情報を提示する行為であり、1年以下の拘禁刑と15000ユーロ以下の罰金が科される。

このように、1978年法は CNIL からの制裁と、CNIL に関する犯罪について規定している。CNIL は広範な権限を有しているものの、法律違反に対して直ちに強い制裁を科すのではなく、催告に従わなかった場合に初めて金銭制裁を科すというのがフランス個人情報保護法の特徴である。後述するように、情報処理者にとっては刑罰よりも CNIL による制裁の方が影響力を有している。

第3項 刑法典における処罰規定

続いて、フランス刑法典には個人情報の侵害を処罰する規定がいくつか設けられている。1978年法50条は「本法の規定に関する犯罪は、刑法226-16条から226-24条において予定され、抑止される」と規定していることから、個人情報に関する犯罪が刑法典に規定されているのである。刑法典に規定されている主な犯罪類型を以下列記する。

①刑法226-16条 1978年法の定める事前手続に違反して個人情報を処理したり、処理を行わせたりする行為は、故意ではなく怠慢（*négligence*）による場合も含めて5年以下の拘禁刑および300000ユーロ以下の罰金が科される（226-16条から

226-24条まで、法定刑は全て共通している⁸⁰)。1978年法45条Iの2項についても同様。

②226-16-1-A条 1978年法24条I・IIの条件下で個人情報の処理を行ったり行わせたりした場合、簡易化基準 (les normes simplifiées) または免除基準 (les normes d'exonération) に対する違反は怠慢による行為も含めて処罰される。

③226-16-1条 1978年法の条件下で認められた処理が行われた場合を除いて、個人識別全国名簿 (répertoire national d'identification des personnes physiques) における個人登録番号 (le numéro d'inscription des personnes) を含んだ情報を処理したり処理させたりする行為は処罰される。

④226-17条 1978年法34条の定める安全措置を採ることなく個人情報を処理したり処理させたりする行為は処罰される。

⑤226-18条 詐欺的 (frauduleux)、あるいは不誠実 (déloyal)、不正な (illicite) 手段で個人情報を収集する行為は処罰される。

⑥226-18-1条 本人が反対しているにもかかわらず (malgré l'opposition de cette personne)、市場調査、特に販売目的のために個人情報を処理する行為、または正当な理由に基づき反対している場合に個人情報を処理する行為は処罰される。

⑦226-19条 法律が規定している場合を除き、利害関係者の明示的な同意 (consentement exprès de l'intéressé) なく、人種的または民族的出自、政治的・哲学的または宗教的意見、労働組合への所属が直接または間接的に明らかになる個人情報、または健康もしくは性的指向 (orientation sexuelle) または性同一性 (identité sexuelle) に関する情報を情報記憶装置 (mémoire informatisée) に入力または保存する行為は処罰される。

同様に、法律が規定している場合を除き、犯罪、有罪判決、保安処分に関する情報をコンピュータ・メモリーに入力または保存する行為は処罰される。

⑧226-19-1条 健康の分野における研究の目的で、1) 情報収集もしくは情報の対象となった個人にアクセス権、訂正権、拒否権、伝達される情報の性質およびその名宛人について予め告知せず情報処理をする行為と、2) 関係者が反対している場合、または法律の定める説明された上での明示的な同意がない場合、あるいは本人が死亡していて遺族が明示的に拒否している場合に情報処理をする行為は処罰される。

⑨226-20条 法令によって、許可または意見の申請 (la demande d'autorisation ou d'avis) によって、または CNIL への事前の届出によって定められた期間を越えて個人情報を保存する行為は処罰される。しかし、法律によって定められた条件に従って、歴史的・

⁸⁰ 2004年の改正の際、当初は刑罰を軽くして、懲役3年および45000ユーロの罰金を上限にすることが議論されていた。しかし、CNILがこれに反対し、刑罰を軽くしないばかりではなく、逆に加重することを主張したので、改正によって、大多数の犯罪は5年以下の懲役および30000ユーロ以下の罰金が上限となった。

統計的・科学的目的のために情報の保存が行われた場合を除く。

法律によって定められた場合を除いて、所定の期間を越えて歴史的・統計的・科学的な目的以外の目的によって情報を処理する行為も処罰される。

⑩ 2 2 6 – 2 1 条 個人情報登録 (enregistrement)、分類 (classement)、転送 (transmission) またはその他の処理の際に、個人情報を保有する者が、情報の自動処理を許可する法律の規定や CNIL の活動・決定、あるいは情報処理のための事前届出に定められた目的を逸脱する行為は処罰される。

⑪ 2 2 6 – 2 2 条 情報の登録、分類、転送またはその他のすべての情報処理の際に、漏洩すれば本人への敬意 (considération) や私生活の内奥 (l'intimité de sa vie privée) を侵害するような情報を収集した上で、本人の許可なく、情報を受け取る資格がない第三者に知らせる行為は処罰される。

そして、軽率または怠慢によって (par imprudence ou négligence) 上記の漏洩をする行為は 3 年の拘禁刑および 1 0 0 0 0 0 ユーロの罰金刑を科される。

このように、1 9 7 8 年法に規定された情報処理のための手続等に違反する行為の他、不正に情報を収集したり漏洩したりする行為が処罰の対象となっている。

以上、フランスの 1 9 7 8 年法の概要について整理した。1 9 7 8 年法について、以下のことが問題となる。

第 1 に、フランス刑法典における処罰規定の成立要素が問題となる。フランス刑法 2 2 6 – 1 6 条から 2 2 6 – 2 4 条では、1 9 7 8 年法に関する犯罪について規定されており、その中で情報の不正な取り扱いを直接処罰する規定は 2 2 6 – 1 8 条 (詐欺的・不誠実・不正な手段による情報収集の罪)、2 2 6 – 1 8 – 1 条 (本人の拒否にもかかわらず市場調査のために行う情報処理の罪)、2 2 6 – 1 9 条 (センシティブ情報の入力・保存についての独立した処罰規定)、2 2 6 – 2 2 条 (本人への敬意や私生活の内奥を侵害する情報を無権限の第三者に知らせる罪) である。個人情報の侵害に対する妥当な処罰のあり方を検討するために、フランス刑法における上記の処罰規定の成立要素と射程範囲に関する分析を行う (第 2 節)。

第 2 に、CNIL が法律違反に対して制裁権を有しており、その中には金銭制裁も含まれている。CNIL による金銭制裁と刑罰はいかなる関係にあるのかということについて、CNIL の位置づけも含めて検討する (第 3 節)。

第 2 節 刑事罰について

本節では、個人情報の不正な取り扱いを直接処罰するフランス刑法の犯罪類型について分析する。

第 1 項 詐欺的・不誠実・不正な手段による情報収集の罪 (刑法 2 2 6 – 1 8 条)

フランス刑法 2 2 6 – 1 8 条では、詐欺的・不誠実・不正な手段による情報収集が処罰されることは前節で述べた通りである。そこで、本項では 2 2 6 – 1 8 条の犯罪の構成要

素や射程範囲等について扱う。

本罪は故意犯なので、行為者は情報収集の方法が詐欺的、不誠実、または不正であることを認容していなければならない⁸¹。続いて、本罪の行為態様についての議論がある。226-18条では、本罪所定の手段によって情報を収集する行為のみが処罰の対象となり、情報を記憶したり (*mémoriser*) 広めたり (*diffuser*) する行為は本罪の成否とは無関係のはずである⁸²。しかし、破毀院 (*la Cour de cassation*) は、本罪の前身である法改正前の1978年法42条の犯罪が成立するためには「当該情報が詐欺的、不誠実、不正な手段によって収集されたということのみならず、当該情報が自動処理か否かを問わず、ファイルに記録されるか保存されていなければならない」と判断した⁸³。この事件では、債権取立会社の管理人である **Riou** が、債務者の氏名や住所などの情報を自動処理していたことに加え、債務者の住む不動産の所有者・管理人などに対して、債務者の仕事や交友関係、両親について、支払い能力についての詳細を知らせるように要求する手紙を送り、債務者の返済能力についての記録を収集していた。**CNIL** の要請により、**Riou** は1978年法に定められている **CNIL** への事前の届出をせずに情報処理を行い、不誠実な手段によって情報を収集したとして軽罪裁判所 (*tribunal correctionnel*) に訴追された。破毀院は情報収集の方法の争点につき、「不誠実な方法」によって収集された情報はファイルに記録も保存もされていなかったことから、不誠実な収集の罪について無罪を言い渡し、原判決を破毀した。

更に、「詐欺的・不誠実・不正な手段」の意義も問題となる。条文におけるこれらの文言は曖昧であり、判例においてもこれらの文言の明確な定義付けがなされていないものの、判例が226-18条の罪を成立させた事例の集積によって、その内容を窺い知ることができる。判例によると、保険業者が情報の関係者に無断で (*à l'insu de la personne concernée*) フランス電力・ガス会社 (**EDF-GDF**) から新規契約者の住所の情報を購入する行為は、買収 (*corruption*) を手段として用いていることから、不誠実な手段による情報収集行為とされる⁸⁴。インターネットの発達によって、個人情報収集のための不可視的な手段が増えたことに伴い、226-18条の適用される余地にも変化がもたらされた⁸⁵。匿名の政治的な調査を装って、調査に関する電子メールをインターネット利用者に送ったが、実際は調査に対する回答は回答者のメールアドレスと共にファイルに保存されていたという事件につき、裁判所は「不誠実な方法」による情報収集であると判断した⁸⁶。つまり、情報収集にあたって本人に対して正確な告知をせず、本人の不知を利用するような性質の行為が「不誠実」な情報収集であると解していると思われる。

続いて、オフィスオートメーションサービス協会 (**Alliance Bureautique Services**. 以下、

⁸¹ Lepage et al, supra note 77, p.234-235.

⁸² Lepage et al, supra note 77, p.235.

⁸³ Cass.crim., 3 nov 1987 : Bull.crim.1987, n°382.

⁸⁴ TGI Paris, 16 déc.1994 : JurisData n°1994-600554.

⁸⁵ Lepage et al, supra note 77, p.235.

⁸⁶ T.corr.Nanterre, 4 juin 2004, inédit.

ABS) は 2002 年と 2003 年に、インターネットを通じてメールアドレスを入手した個人に対して、個人がメールの受け取りを希望していないにもかかわらず宣伝のための電子メール (スパムメール) を送ったところ、CNIL の要請により、刑法 226-18 条の罪にあたるとして訴追されたという事件がある。ABS は情報を収集するために、<Robot Mail>と<Freeprospect>という、インターネットを通して情報を「取り込む (aspirer)」ことのできるソフトウェアを用いていた。

この事件につき、パリ控訴院は、ABS は情報の関係者に無断で情報を収集するという不誠実な手段を用いており、それによって情報関係者が情報処理に対する拒否権を行使することができなくなったとして、刑法 226-18 条の罪が成立すると判断した。破毀院も控訴院の判断を肯定して、被告人の上告を棄却した⁸⁷。学説は、本件破毀院判決は CNIL よりも厳格で明確な判断基準に従っているとして肯定している⁸⁸。ここでは、情報収集について本人に告知せず、本人の拒否権行使を妨害する結果となったことが「不誠実」な方法による情報収集であると解された。情報処理責任者は情報処理にあたり、本人に告知をする義務があるのは第 1 節で述べた通りである。告知義務に違反したり、または不十分な告知によって情報収集したりするような行為は 226-18 条における処罰の対象となり得る。

第 2 項 市場調査等のための情報処理の罪 (刑法 226-18-1 条)

本条では、①本人が反対しているにもかかわらず、市場調査、特に販売目的のために個人情報进行处理する行為、または②正当な理由に基づき反対している場合に、個人情報进行处理する行為が処罰される。本罪は故意犯である。第 1 節の第 1 項で述べたように、1978 年法 38 条では、個人は正当な理由のある場合に情報処理を拒否する権利があり、情報処理が市場調査や商業目的によるものである場合には、個人は何らの負担をすることなく情報処理を拒否する権利があることが規定されており、刑法 226-18-1 条と 1978 年法 38 条は共に、個人の拒否権を保護している。

情報処理に対して反対の意思表示をするためには、情報処理を告知されている必要があるが、告知がなされていないために情報処理が行われていることを知らない場合は本罪の対象となるのか否かが問題となっている。

情報処理に対する反対の意思表示がなかった場合の犯罪の成否が問題になったケースには以下のものがある。2 つの金融機関が本人に知らせずに、本人の信用に関する情報を経済利益団体である「未払情報処理中央機関 (Groupement d'intérêt économique《Centrale Professionnelle d'Information sur les Impayés》)」に転送して、当該団体がこの情報の記載されたファイルの情報処理を行ったところ、ファイルに個人の信用や返済についての情報が記載されていた。そこで、本人はクレジットカードの交付を拒否された際に、自分の信用情報がファイルに記載されていることを知ったというケースである。このように、本

⁸⁷ Cass.crim., 14 mars 2006 : Bull.crim. 2006 n°69.

⁸⁸ Agathe Lepage, *informatique et Liberté* : Comm.com. électr. 2006, comm131.

人に知らせず情報処理をする行為が1978年法の42条と改正前の刑法226-18条の罪に該当するとして、CNILの要請により、上記の経済利益団体の代表者が訴追された。

パリ控訴院は、本人の反対にもかかわらず個人情報を処理する犯罪（改正前の226-18条）が成立することを肯定した。控訴院によると、改正前の1978年法26条は、情報がファイルに記載される前に、当該情報が処理の対象となることを本人に告知することを想定しており、本人が情報処理について告知されていないゆえに拒否の意思表示をすることができないとしても犯罪が成立する。この判決に対して破毀院は、1978年法（改正前）は、第三者を通して（auprès de tiers）情報収集する情報処理責任者に対して、処理について関係者に告知するいかなる義務も設けていないとして控訴院の判決を破毀した。

実際に、改正前の1978年法は、情報処理責任者に対して、直接的ではなく第三者から間接的に収集された情報について告知するいかなる義務も設けていなかった。一方、2004年法による1978年法の改正以来、情報収集が直接的であるか間接的であるかということにかかわらず、告知義務が予定されるようになったが、情報が第三者を通して収集されたことについての告知がされなかった場合、告知がなかった以上、本人は拒否の意思表示をすることができず、拒否権を行使できないということになるのかという問題が生じる。確かに、情報処理に関する事前の告知の欠如は、明らかに拒否権の行使を妨害するものであるが、刑法226-18-1条は、本人の拒否にもかかわらず情報を処理する行為のみを処罰する規定であって、拒否が示されることを前提としていることから、本人に無断で情報処理を行うことによる拒否権行使の妨害は、それ自体で226-18-1条における処罰の対象とはならず、不誠実な方法による情報収集ということで226-18条の対象になり得る⁸⁹。そのように解すれば、情報処理責任者の告知義務の有無や程度にかかわらず、情報の関係者が処理に対して反対の意思表示を示していない限り、226-18-1条の成否はおおよそ問題にならない。本人が反対意思を表示できなかった場合にも226-18-1条の犯罪が成立するとなれば、226-18条との区別が曖昧になり、両者が別個の犯罪規定として設けられている意義も小さいものになるだろう。

したがって、226-18条と226-18-1条は共に個人の意思に反する情報処理を処罰する犯罪であるが、条文の文言上も解釈上も226-18-1条は、226-18条とはその射程範囲が明確に区別された規定であり、本人が反対意思を表示した場合の情報処理に限って成立の余地があるといえる。

第3項 センシティブ情報の入力・保存の罪（刑法226-19条）

本条では、利害関係者の明示的な同意なく、人種的または民族的出自、政治的・哲学的または宗教的意見、労働組合への所属が直接または間接的に明らかになる情報等のセンシティブ情報をコンピュータ・メモリーに入力または保存する行為が処罰される。このようにセンシティブ情報の不正な取り扱いを処罰する独立した規定を設けていることは、フラ

⁸⁹Lepage et al, supra note 77, p.244.

ンス情報法の特色であるといえる。そこで、本項では第一に、刑法 226-19 条と、その前提となっている 1978 年法 8 条の成立過程と、8 条について問題となった憲法院判決について概観することで、センシティブ情報をめぐる議論を整理した後、判例等を通して本罪の成立要素について述べる。

第 1 款 刑法 226-19 条・1978 年法 8 条の成立過程と憲法院判決について

(1) 成立過程

現行刑法 226-19 条の前身は、改正前の 1978 年法 31 条と 42 条である。改正前の 1978 年法 31 条は、センシティブ情報の取り扱いについて以下のように規定する。

「1 本人の明示的な同意 (*accord exprès de l'intéressé*) のある場合を除き、人種的出自、政治的、哲学的もしくは宗教的意見、労働組合への所属を直接的に、もしくは間接的に明らかにするような記名情報 (*données nominatives*) を、情報記憶装置 (*mémoire informatisée*) に入力または保存することを禁止する。

2 しかし、教会または宗教的、哲学的、政治的団体もしくは労働組合は、その構成員または通信相手 (*correspondant*) を、自動処理によって登録することができる。この点につき、いかなる監督 (*contrôle*) もされない。

3 公共の利益 (*intérêt public*) のため、コンセイユ・デタのデクレに基づき、委員会の提案 (*proposition*) もしくは適合意見 (*avis conforme*) により、上記の禁止に例外を設けることができる」。

センシティブ情報の取り扱いを原則的に禁止することを定め、2・3 項が例外について規定する旧法 31 条は、現行 1978 年法 8 条と同様の構成となっている。そして、旧法 42 条において、31 条違反の行為が処罰の対象となる旨が規定される。旧法ではセンシティブ情報の取り扱いについての原則と例外のほか、違反に対する罰則が同一の法律で定められていたが、1992 年の新刑法典および新刑事訴訟法の実施に関する法律 (*Loi n° 92-1336 du 16 décembre 1992*) 41 条により、1978 年法の規定に関する犯罪は現行刑法典の 226-16 条から 226-24 条によって処罰されることとなった。

そして、旧 1978 年法 31 条も、1995 年 EU データ指令 8 条に準拠する形で 2004 年に改正される。EU 指令 8 条 1 項では、加盟国はセンシティブ情報の取り扱いを禁止しなければならない旨を規定する。2 項 (a) 以降では例外が設けられている。2 項 (a) 項は、本人の明示的な同意のある場合は情報処理が認められるが、データ主体 (*data subject*) の同意があったとしても、センシティブ情報の取り扱いの禁止が解除されないことが加盟国の法律によって規定されている場合を除くとされている。この規定は現行 1978 年法 8 条 2 項 1 号に受け継がれている。

EU 指令 8 条 2 項 (c) は、データ主体または他の者の生命の保護のために情報処理が必要であるが、本人の法的または物理的な無能力のために同意を与えることができない場合を例外として規定しており、現行 1978 年法 8 条 2 項 2 号に受け継がれている。

EU 指令 8 条 2 項 (d) は、財団、協会その他の非営利の政治的、哲学的、宗教的な団体、もしくは労働組合の目的のための団体によって行われる適法な活動であり、適切な保障を与えられる範囲内において情報処理が必要な場合が例外的に認められると定める。ただし、当該情報処理が上記の団体の構成員のみに関するものであるか、または団体の目的に関連した定期的な契約を締結している者のみに関するものであり、当該データが本人の同意なしに第三者に提供されないことを条件とする。この規定は現行 1978 年法 8 条 2 項 3 号に受け継がれている。

EU 指令 8 条 2 項 (e) では、情報処理が、明らかに本人によって公表されたデータに関する場合、または裁判における権利の確認、行使もしくは防御のために必要な場合は処理が認められる。この規定は現行 1978 年法 8 条 2 項 4・5 号に受け継がれている。

EU 指令 8 条 3 項は、データ処理が予防医療、診療もしくは治療の提供または健康サービスの管理のために必要な場合、ならびに国内法もしくは国の管轄機関が決めた規則により職業上の守秘義務を負う医療専門職者により、もしくは同等の守秘義務を負うものによってデータ処理が行われる場合には例外的に認められると規定する。この規定は現行 1978 年法 8 条 2 項 6 号に受け継がれている。

EU 指令 8 条 4 項は、「適切な保障の留保のもとで、加盟国は重要な公共の利益を理由にして、国の法律もしくは監督機関の決定により、第 2 項所定のもの以外の適用除外を定めることができる」と規定する。これは、公益上の必要があり、CNIL が情報処理を許可した場合はセンシティブ情報の処理が適法化されることを定める現行 1978 年法 8 条 4 項に引き継がれている。

EU 指令 8 条 5 項は、「犯罪、有罪判決、保安処分に関するデータの処理は、公共機関の監督のもとでのみ、または適切かつ独自の保障を定める国内の規定に基づき加盟国が適用除外を定めた場合は、その適切かつ独自の保障が国内法により定められた時に限って行うことができる。ただし、刑事の有罪判決データの網羅的な収集は、公共機関の管理のもとでのみ行われる。加盟国は、行政罰もしくは民事の判決に関するデータについても、公共機関の管理のもとで処理されることを規定することができる」と定めている。この規定における「犯罪、有罪判決、保安処分に関するデータの処理」についての箇所は、そのまま導入する形ではないものの、現行 1978 年法 9 条 1 項に受け継がれている。

このように、センシティブ情報を他の一般的な情報と区別して保護するという考え方は、EU 指令以前のフランス 1978 年法に導入されていたが、EU 指令 8 条を全面的に受け入れることによって現行の条文となっている。EU 指令以前に「センシティブ情報」という考え方を導入している点はフランスの特徴であるが、ここには差別を法的に予防・禁止するという独自の問題意識があるように思われる。まず、1939 年 4 月 21 日のデクレ・ロワによって、1881 年出版自由法に、人種的または宗教的出自を理由とする名誉毀損罪と侮辱罪という概念が導入された。次に、「人種差別との戦いに関する 1972 年の法律 (Loi n° 72-546 du 1 juillet 1972 relative à la lutte contre le racisme)」によって、1881 年

出版自由法の名誉毀損罪・侮辱罪に関する規定が改正され、出生または特定の民族、国家、人種もしくは宗教への帰属の有無を理由とする差別、憎悪、暴力を教唆する言論と（２４条）、民族・国家・人種・宗教への帰属を理由とする名誉毀損（３２条）と侮辱（３３条）が犯罪化された。また、フランス刑法２２５－１条と２２５－２条では、出身、性別、家庭環境、政治的意見、組合活動、人種などを理由とした差別によって財物・役務の提供を拒否したり、採用を拒否したりする行為が処罰の対象となっている。これらの規定からわかるように、フランス法には、人種や政治的思想、宗教などによって個人が不利益を被ることを予防・禁止するという問題意識が歴史的に存在する。それがセンシティブ情報を他の個人情報と区別するという法的な発想につながっているのではないだろうか。

（２）２００４年憲法院判決

ここまでは、センシティブ情報の取り扱いに関する現行１９７８年法８条と、８条違反を処罰する刑法２２６－１９条が成立するまでの大まかな流れを確認した。旧法３１条から現行法８条への改正により、センシティブ情報の取り扱いが認められる例外事項が具体的に、詳細になっている。そして、これらの例外は刑法２２６－１９条における「法律の定めによる場合」に該当することになるが、現行法８条と「私生活を尊重される権利」との適合性が問題となったケースとして、２００４年７月２９日憲法院判決⁹⁰がある。現行法８条１項はセンシティブ情報の収集や処理を原則的に禁止しており、８条２項５号は裁判上の権利の証明、その行使、防御のために必要な場合には情報処理が認められる旨を規定しているが、私生活を尊重される権利を侵害するとの提訴⁹¹が憲法院に対してなされた。この提訴に対して憲法院は、「共和国は、欧州共同体および欧州連合に加盟する。欧州共同体と欧州連合は、それらを設立する条約に基づき、一定の権限を共同で行使することを自由に選択した諸国家によって構成される」と規定するフランス憲法８８－１条を参照する。この条文により、「共同体指令を国内法に導入することは、憲法上の要請であり、それを拒否することができるのは、憲法上の明確な反対の規定（*disposition expresse contraire*）がある場合に限られる」ということを前提とした上で、そのような規定が存在しない場合には、管轄権は共同体裁判官（*juge communautaire*）にのみ属すると判断した⁹²。続いて憲法院は、問題となっている規定は、１９９５年１０月２４日の９５／４６／EU指令８条２項（e）の規定から必要な帰結（*conséquences nécessaires*）を導き出したものにすぎないので、８条の規定は私生活を尊重される権利を侵害するという不服に対して判断する権限は憲法院にはない⁹³として、８条に関する提訴を退けた。

２００４年憲法院判決は、現行法８条２項５号の合憲性を憲法院が正面から判断することを拒否するものである。本件に対しては、旧法３０条と３１条よりもセンシティブ情報

⁹⁰ Décision n°2004-499 DC du 29 juillet 2004.

⁹¹ Décision n°2004-499 DC du 29 juillet 2004, *supra* note 90, Con6.

⁹² Décision n°2004-499 DC du 29 juillet 2004, *supra* note 90, Con7.

⁹³ Décision n°2004-499 DC du 29 juillet 2004, *supra* note 90, Con8.

の処理が認められる基準が緩やかな EU 指令 8 条に沿って 1978 年法の改正が行われたので、結果的に現行法では旧法よりもセンシティブ情報の保護が薄くなっているという批判がある⁹⁴。前述の通り、現行 1978 年法 8 条は EU 指令 8 条をほぼ全面的に取り入れたものであり、法改正には EU 指令の国内法化の要請が重要な意味を有している⁹⁵ので、旧法 31 条と現行法 8 条を比較することに妥当性はないとも思われる。

しかし、法改正により、センシティブ情報の処理が認められる例外の範囲が拡大したことは事実である。また、現行法 26 条 2 項は、8 条 1 項所定のセンシティブ情報に関する処理は CNIL の理由付きの意見が公表された後に、コンセイク・データのデクレによって許可されることが定められている。この規定は旧法 31 条 3 項と同趣旨であるが、センシティブ情報の処理それ自体を法律ではなく、CNIL やコンセイク・データという行政機関の判断に基づくデクレに委ねることには批判⁹⁶もある。

もちろん、CNIL もコンセイク・データも、センシティブ情報の取り扱いを例外的に認めるデクレを無限定に発することはできないが、このような裁量は現行法 8 条 2 項以降の例外規定と相俟って、センシティブ情報に対する保護を薄くする結果を導くだろう。そうであれば、センシティブ情報はその他の一般的な個人情報よりも重要なものであるからこそ、情報処理が認められるための規則も一般的な個人情報に対するそれと区別するという立法趣旨も、単なる確認規定以上の意義を有しないものになっており、センシティブ情報という概念そのものの意義も揺らぐことになるのではないだろうか。

それに伴い、刑法 226-19 条における「法律が規定している場合」の範囲も拡大することになる。CNIL の意見とコンセイク・データのデクレによって処理が許可され得ることが、1978 年法 26 条 2 項で定められているので、CNIL やコンセイク・データの判断によってこの要件が左右される可能性もある。このようなデクレはセンシティブ情報の処理の例外を認めるので、処罰範囲の縮小を後押しするものではあるものの、行政機関の判断によって、処罰範囲が左右されるという事態が果たして妥当であるかは疑問である。

第 2 款 226-19 条の罪の成立要素について

ここでは、刑法 226-19 条の罪の成立要素について扱う。本条では個人についての上記のセンシティブな属性を直接的または間接的に明らかにする情報が対象となっているが、特に「間接的に明らかにする情報」の意義が問題となる。過去の判例では、アルジェリア戦争でフランス側についたアルジェリア人兵士とその家族であるアルキ (harki) に与えられた援助についてのファイルは、彼らの宗教的信念を間接的に明らかにする情報であ

⁹⁴ Alexandre Mairot de la Motte, La réforme de la loi informatique et libertés et la droit au respect de la vie privée, AJDA, 29 novembre 2004, p.2271.

⁹⁵ 市川直子「フランスにおける個人データ保護法制」城西大学経済経営紀要 23 巻 (2005 年) 57 頁。

⁹⁶ 清田雄治「フランスにおける個人情報保護の憲法的保障」政策科学 13 巻 3 号 (2006 年) 55 頁。

るとされた⁹⁷。一方、2004年法による改正前の226-19条について、個人の性的指向には言及していないものの、フランスの有料テレビ放送の「カナルプリュス (Canal+)」の加入者がポルノ映画を購入したという情報をコンピュータ・メモリーに入力する行為が問題となり、裁判所はポルノ映画の購入情報によって当該加入者の個人的な趣味嗜好を直接的に明らかにすることはできず、間接的に明らかにすることさえできないとして226-19条の対象から除外した⁹⁸。1978年法は、センシティブ情報の処理に対して本人の「明示的な同意」のあることを適法化要件のひとつとして規定していることにより、刑法226-19条の犯罪にも「本人の明示的な同意」が存在しないことが求められている。

本罪は故意犯である。したがって、行為者は、関係者の明示的な同意がないにもかかわらずセンシティブ情報をコンピュータ・メモリーに入力または保存しているということを認識していなければ、本罪は成立しない⁹⁹。

第4項 本人への敬意・私生活の内奥を侵害する情報漏洩の罪（刑法226-22条）

本罪では、情報の登録、分類、転送またはその他のすべての情報処理の際に、本人への敬意や私生活の内奥を侵害するような情報を収集した上で、本人の許可なく、情報を受け取る資格がない第三者に漏洩する行為が処罰の対象となる。そして、情報に関する他の犯罪類型とは異なり、本罪は軽率または怠慢による漏洩も処罰され得る。

「名声」や「私生活」という文言の意義については、名誉毀損罪と民法9条（私生活の保護）・刑法226-1条（私生活の侵害に関する犯罪）に関する判例が提示する意義と必ずしも一致するわけではないとされる¹⁰⁰。EDF-GDF（フランス電力・ガス会社）の従業員が、新しい使用契約者の氏名と住所の情報を売却したという事件につき、個人の住所は民法9条による「私生活の秘密の保護」の対象となるにもかかわらず、裁判所は刑法226-22条の罪の成立を肯定しなかった¹⁰¹。住所が本罪の客体とならなかったのは、刑法226-22条が単なる「私生活」を侵害するような情報の収集を対象としているのではなく、私生活の「内奥」に対する侵害を対象としていることによると考えられる。

また、一つの情報処理によって、刑法における情報に関する複数の罰条に触れる場合の犯罪の個数が問題となる。金融会社（établissement de credit）が、地元の300人の商業者に対して氏名・住所・口座番号に関する情報処理のリストを送ったところ、その情報は経済的に問題のある900人に関するものであったという行為につき、裁判所は、①銀行に関する法律で規定された職業上の守秘義務に違反する罪、②改正前の1978年法42条における、情報処理の際の安全措置義務違反の罪、③個人の評判（réputation）や名声を

⁹⁷CE,5 juin 1987 :JurisData n°2005-068122 ;JCP G 1988,II,20997.

⁹⁸CE,9 févr.2005:JurisData n°2005-068122.

⁹⁹Lepage et al, supra note77, p.250.

¹⁰⁰Lepage et al,supra note77,p.240.

¹⁰¹TGI Paris,16 déc 1994 :JurisData1994-600554.

傷つけるような記名情報を漏洩する罪の3つの犯罪の成立を肯定した¹⁰²。特に、226-22条につき裁判所は、金融機関が漏洩した情報は正真正銘のブラックリスト (*véritable liste noires*) であることから、個人の名声や評価を下げる種類の情報であると判断している。

続いて、「公証人の被害者を保護するヨーロッパ連盟 (*Ligue européenne de défense des victimes de notaires*)」の代表者の指示で運営されているインターネット上のサイトに、犯罪や問題行為について非難された公証人の記名情報が記載されたところ、情報公開について関係のある公証人からの反対があったにもかかわらず、団体の代表者はこれに応じず、さらに記載された情報は誤りであったという事件でも、一つの情報公開という行為が複数の罰条に触れている。裁判所は、①情報処理に際して CNIL に届出をしなかったことで、法律に規定されている手続を遵守しなかった罪 (226-16条)、②情報の関係者の正当な拒否があるにもかかわらず、情報公開を中止しない罪 (226-18-1条)、③犯罪に関する情報を入力する罪 (226-19条2項)、④個人の名声や評判を傷つける情報を漏洩する罪 (226-22条) の4つの犯罪が成立すると判断した¹⁰³。特に、この事件において関係する公証人は、たとえ情報が誤っていたとしても犯罪や問題行動について公然と非難されていることから、公開された情報は226-19条2項の客体であるのみならず、公証人の名声を侵害する性質を有する情報であると解されている。

学説においても、事案の具体的事情によっては刑法226-22条の罪と刑法226-13条における職業上の守秘義務違反 (*violation du secret professionnel*) の罪や、1881年7月29日出版自由法29条における名誉毀損罪 (*diffamation*) の両方の犯罪の成立する余地のあることが指摘されている¹⁰⁴。特に、名誉毀損罪、職業上の守秘義務違反の罪、センシティブ情報に関する罪、個人の名声や評判、私生活の内奥を侵害する情報を漏洩する罪の4つは重なり合うところが多く、各々の犯罪規定の存在意義が問われ得る。しかし、フランス刑法において別個の犯罪規定として存在している以上、名誉を侵害する罪と秘密を侵害する罪、そして情報を漏洩するなどして不正に取り扱う罪は、それぞれ別個の法的な位置づけを有しており、名誉と秘密、そして個人情報とは異なる法的な利益として解されていると思われる。

なお、前述の通り本罪では故意行為のみならず、軽率 (*imprudence*) または怠慢 (*négligence*) による過失行為も処罰の対象となるので、ここでは軽率ないし不注意による過失の概要について述べる。

まず、フランス刑法121-3条の1項¹⁰⁵では「罪を犯す意思 (*intention de le commettre*)

¹⁰² CA Rennes 13 janv.1992,D.1993somm.54p.

¹⁰³ CA Bourges,11 janv 2007 :Comm.com. électr.2007,comm.126.

¹⁰⁴ Lepage et al,supra note77, p.241.

¹⁰⁵フランス刑法121-3条は1994年の新刑法典成立以来、1996年と2000年に2度の改正が行われて、現在の条文に至っている。1994年段階では121-3条は以下のように規定されていた。「1 重罪または軽罪は、それを行う意思がない場合には成

がなければ重罪 (crime) も軽罪 (délit) も成立しない」とされ、故意犯処罰の原則が掲げられている。次に、121-3条の2項は、「前項の規定にかかわらず、法律が定める場合、他人を意図的に危険にさらすときは軽罪が成立する (il y a délit en cas de mise en danger délibérée de la personne d'autrui)」と定める。

続いて、121-3条の3項には「法律の定めによる場合 (lorsque la loi le prévoit)、軽率 (imprudence)、怠慢 (négligence)、または法律もしくは規則によって定められた注意義務 (une obligation de prudence)、もしくは安全義務 (obligation de sécurité) に違反するという過失によるときは、行為主体がその任務 (ses missions) または職務 (ses fonctions) の性質、権限 (ses compétences)、同じく当該行為主体が有する能力 (pouvoir) と手段 (moyens) から導かれる通常の注意 (diligences normales) をしなかったことが証明された場合、同じく軽罪が成立する」と規定されており、これが刑事の過失 (faute pénal) を処罰する根拠条文となる。そして、121-3条4項は「前項に規定された場合で、損害 (dommage) を直接惹起することはなかったものの、損害の発生を実現し得る状況を作り出し、もしくは作出させ、または損害発生を回避するための措置を採らなかった自然人 (personnes physiques) は、法律または規則によって規定された注意義務もしくは安全義務に明確な意思の下で (de façon manifestement délibérée) 違反したか、明確に特徴づけられた過失 (faute caractérisée) を犯し、その過失が、無視することのできない特に重大な危険 (risque d'une particulière gravité qu'elles ne pouvaient ignorer) に他者をさらすものであることが証明された場合に、刑事責任を負う」と規定する。4項の規定は相当因果関係を立法化したものであると指摘されている¹⁰⁶。

軽率または怠慢による過失と注意義務・安全義務違反は、非故意犯罪において行為者への非難が認められるための心理的要素である。刑法226-22条との関係では、「軽率または怠慢による過失」の意義が問題となる。

刑事の過失 (faute pénal) は、行為者が自己の行為によって損害結果 (conséquences dommageable) が生じることを予見していなかった場合や、損害結果が発生することを考えなかった場合や、または行為者が結果発生を回避するために必要な用心をしていなかった

立しない。2 ただし、法律に特別の規定がある場合、軽率、怠慢、または他者の身体を意図的に危険にさらす時には軽罪が成立する。3 不可抗力の場合、違警罪は成立しない。1996年の改正では121-3条2項が次の条文に変えられた。121-3条2項「ただし、法律に特別の規定がある場合、他者の身体を意図的に危険にさらすときは軽罪が成立する」、121-3条3項「同様に、法律に特別の規定がある場合、軽率、怠慢、または法律もしくは規則によって規定された注意義務もしくは安全義務に違反するとき、行為者が場合によっては、その任務または職務の性質、権限や行為者の能力や手段を考慮して、通常の注意を払った場合を除いて軽罪が成立する」。1996年改正により、刑法上の過失と免責の基準が明確化された。そして、2000年改正では121-3条3項が上記のように修正され、121-3条4項が新設された。

¹⁰⁶末道康之「過失犯規定に関するフランスの刑法改正について」捜査研究591号(2001年)65頁。

た (ne pas prendre les précautions nécessaires pour les empêcher de survenir) 場合に成立する¹⁰⁷。行為者のこのような心理状態は、結果の発生に対する「不注意 (imprévoyance)」であると包括される。この「不注意」が過失の本質であり、過失はさらに「認識ある過失 (faute consciente)」と「認識なき過失 (faute inconsciente)」に二分される¹⁰⁸。認識ある過失は、行為者が結果発生の危険性を認識していたが、結果の発生を意欲せず、結果が発生しないと信じていた場合である¹⁰⁹。フランス刑法では結果発生を意欲していなければ故意が認められないので、いわゆる「未必の故意 (dol éventuel)」は認識ある過失として扱われる¹¹⁰。一方、認識なき過失は、行為者が結果発生の危険性を予見していなかった場合である。

このように、フランス刑法における過失は結果発生の危険性についての認識の有無で分けられるが、「軽率」「怠慢」による過失はいずれに該当するのであろうか。認識ある過失と同様に扱われる未必の故意について「認識ある軽率 (imprudence consciente) が問題となる」「未必の故意は軽率 (imprudence) に相当する」と述べることで、《imprudence》という用語を用いる見解¹¹¹からは、軽率による過失は「認識ある過失」であり、怠慢による過失が「認識なき過失」に該当するのではないかとも思われる。実際に、フランス刑法では未必の故意が認識ある過失として扱われていることを紹介する際に、《imprudence consciente》という用語を「認識ある過失」と訳出する日本の学説¹¹²もある。

しかし、「軽率」は「認識ある過失」で、「怠慢」は「認識なき過失」という対応関係にあると断言せず、過失を「認識ある過失」と「認識なき過失」の二つに区別するものの、軽率または怠慢という概念の相違について明言しない学説¹¹³もあることから、「軽率＝認識ある過失」「怠慢＝認識なき過失」という単純な対応関係にあるとはいえず、「軽率または怠慢による過失 (faute d'imprudence ou négligence)」という包括的な概念が「認識ある過失」「認識なき過失」に二分されていると解する余地もある。フランス刑法における過失論の詳細については今後の研究に委ねるが、いずれにしても、刑法226-22条は「軽率または怠慢によって (par imprudence ou négligence)」と規定することにより、認識なき過失によって所定の情報が漏洩された場合も処罰の対象としており、故意行為のみを処罰する他の犯罪類型よりも違法性の程度が重いと解されていることは間違いないだろう。

以上、本節では個人情報データの不正な取り扱いを処罰する刑法の規定について分析した。1978年法の違反が行われる件数は多いが、裁判の場で有罪判決が下されるケースはそれ

¹⁰⁷ Jean Pradel, *Droit pénal général*, Cujas, 18^{éd}, 2010, p.417, André Vitu et Roger Merle, *Traité de Droit criminel tome1*, Cujas, 7^{éd}, 1997, p.757.

¹⁰⁸ Pradel, *supra* note107, p.417, Vitu et al, *supra* note107, p.758.

¹⁰⁹ Pradel, *supra* note107, p.417, Vitu et al, *supra* note107, p.758.

¹¹⁰ Henri Donnedieu de Vabres, *Traité de Droit criminel et de législation pénale comparée*, Sirey, 3^{éd}, 1947, p.81.

¹¹¹ Donnedieu de Vabres, *supra* note110, p.81.

¹¹² 木村亀二 (著) 阿部純二 (増補) 『刑法総論 (増補版)』 (有斐閣・1978年) 210頁。

¹¹³ Pradel, *supra* note107, p.417.

ほど頻繁ではない¹¹⁴。処罰される例が少ないことの背景には、1978年法の性格が技術的・専門的であり、情報について専門的な知識の乏しい裁判官には理解し難いことが指摘されている¹¹⁵。

第3節 CNILによる制裁

第1項 CNILによる制裁の実態

本節では、CNILによって行われている制裁の現状について扱う。2004年の法改正により、CNILは違反に対する制裁権を有するようになった。本項では、CNILが毎年提出している活動報告書 (*rapport d'activité*) に基づき、初めて制裁が行われた2006年から2012年までの毎年の変化を確認しながら、CNILの制裁がどのように運用されているのかということについて分析する。

2006年のCNIL報告書によると、2006年6月28日に、CNILによる最初の制裁が行われた。100件を超える制裁手続のうち、金銭的な制裁 (*sanctions financières*) は11件で、処理中止または是正の指示 (*injonctions*) は7件であった。金銭的制裁の金額は、300ユーロから45000ユーロの間で推移している。制裁の決定件数が少ないのは、CNILの催告 (*mise en demeure*) に従う団体が多いからであると説明されている。2006年には73件の催告があり、催告の対象となった機関の82%がCNILの要請に従ったので、CNILは制裁手続を終わらせた¹¹⁶。制裁手続の対象となり得る主な機関または活動領域のうちの40%は商業、36%が銀行、残りは私立探偵、報道、テレコム、各種協会、政治である。そして、制裁手続の対象となり得る法律違反の21%は個人のクレジット返済事故に関するファイル (*fichier national des Incidents de remboursement des Crédits aux particuliers*、略称はFICP) と消費のクレジット事故に関するファイル (*fichier des incidents de crédits à la consommation*、FCC) に関する問題であり、16%が私生活の内奥に対する重大な侵害 (*atteinte grave à l'intimité de la vie privée*)、9%がセンシティブ情報について、8%が情報処理の拒否権についてである¹¹⁷。

2006年にCNILによって発動された制裁の中で特に重いものは、Crédit Lyonnais とCrédit Agricole という2つの銀行に対して、それぞれ45000ユーロ、20000ユーロの金銭制裁を科したケースである¹¹⁸。前者の事件では、銀行の顧客からCNILに対して、借金を返済したにもかかわらず、銀行における信用のトラブルのリストに情報が記載されている、返済トラブルがなかったにもかかわらずキャッシュカードの取り消しの対象となったという苦情が寄せられた。CNILは銀行に説明を求める等の対策を行ったが、銀行から

¹¹⁴ Lepage, *supra* note 88.

¹¹⁵ Lepage, *supra* note 88.

¹¹⁶ 27ème rapport d'activité 2006 de la Commission nationale de l'informatique et des libertés, p.23. <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/074000422/0000.pdf>.

¹¹⁷ 27ème rapport d'activité, *supra* note 116, p.24.

¹¹⁸ 27ème rapport d'activité, *supra* note 116, p.23.

全ての回答を得ることはできず、銀行は CNIL の活動に協力しなかった。そこで、CNIL は、CNIL の活動への妨害と、不正確なデータをファイル内に記載していたことを理由に銀行に対して 4 5 0 0 0 ユーロの制裁を発動した¹¹⁹。後者の事件でも同様に、銀行の顧客の側から返済トラブルのファイルに誤って情報が記載されているという類似の苦情が CNIL に寄せられた。銀行が取り扱った情報は正確ではなく、無権限の第三者がデータにアクセスするのを回避するための義務が履行されていないことが調査により明らかになり、CNIL の催告を受けた銀行は誤ったデータを修正した。しかし、同様の違反が繰り返されないと考えるだけの対策が提示されていなかったのも、CNIL は当該銀行に対して 2 0 0 0 0 ユーロの制裁を発動した¹²⁰。2 0 0 6 年の報告書では、これらの金銭制裁について、すべての情報処理責任者には CNIL の活動に協力する義務と、情報処理に関する透明性 (transparence) を担保する義務があることから、CNIL への協力が不足している場合は制裁の対象になると説明されている¹²¹。

2 0 0 7 年は、1 0 1 件の催告があり、警告が 5 件、金銭制裁は 9 件であった¹²²。金銭制裁の対象になるのは、主に債務者の情報を入手しようとする会社である¹²³。2 0 0 7 年報告書においても、違反の抑止に対する CNIL の重要性が述べられており、8 0 % の関係機関が問題となっている違反を中止させていることが指摘されている¹²⁴。

2 0 0 8 年は、催告が 1 2 6 件、警告が 1 件、金銭制裁が 9 件である。2 0 0 6 年、2 0 0 7 年に比して CNIL の処理する制裁手続の件数は多いものの、ここでも CNIL の要請に短期間で従う機関が多いことから、制裁手続がすぐに終了する件数も増えているという報告書の記載がある¹²⁵。2 0 0 8 年には、事前の同意なく広告のファックスや大量のメールを送信したり、または拒否権の実際の行使 (un réel exercice du droit d'opposition) を認めることなく商業的な内容の電話をかけたりする多くの企業が CNIL による制裁の対象となった¹²⁶。

また、2 0 0 8 年は、インターネット上における個人情報の公開や再利用についての多数の法律違反が制裁の対象とされた年であると位置づけられている。フランスの教員評価サイトである《note2be》につき、1 9 7 8 年法の違反が問題となった。CNIL は、サイト

¹¹⁹ Fabrice Mattatia, CNIL et tribunaux : concurrence ou complémentarité dans la répression des infractions à la loi informatique et libertés? : Rev.sc.crim.2009, pp.324-325.

¹²⁰ Mattatia, supra note 119, p.325.

¹²¹ 27ème rapport d'activité 2006, supra note 116, p.24.

¹²² 28ème rapport d'activité 2007 de la Commission nationale de l'informatique et des libertés, 47p. http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL-28era_pport-2007.pdf.

¹²³ 28ème rapport d'activité 2007, supra note 122, p.48.

¹²⁴ 28ème rapport d'activité 2007, supra note 122, p.47.

¹²⁵ 29ème rapport d'activité 2008 de la Commission nationale de l'informatique et des libertés, 47p. <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/094000211/0000.pdf>.

¹²⁶ 29ème rapport d'activité 2008, supra note 125, p.48.

上に記載されている評価は、権限があるとは断言できない第三者による主観的なものであり、このサイトは教員の公的な評価における混乱を発生させると判断した上で、教員は情報がサイトに掲載される前に同意を表明する機会が与えられるべきであったことから、当該サイトに対して是正のための催告を行った。同様に CNIL は、関係者に告知せず、不動産業者に転売するためにインターネットを通して個人の不動産の広告を収集した会社に対して、このような不誠実な情報収集（ces collectes déloyales）を中止するようにとの催告を行った¹²⁷。

2009年は、催告が91件、警告が4件、金銭制裁が5件であり、前年までと同様に金銭制裁の件数は少ない。違反の中で特に多いのは、事前手続の欠如と、個人の情報へのアクセス権や、情報処理への拒否権に関することと、無権限の第三者に情報を提供することであり、責任者には違反の予防が求められている¹²⁸。

2010年は、催告が111件、警告が4件、金銭制裁が4件である。2010年報告書によると、CNILに持ち込まれる手続は2009年の段階では減少しているものの、2007年から一定程度の増加傾向にある¹²⁹。しかし、CNILの催告による要請が遵守される割合と、それに伴う手続の終了の割合が高いのは例年通りであることから、催告手続の教育的性格（caractère pédagogique）と有効性（efficacité）がうかがえるとの指摘がある¹³⁰。また、グーグル社のストリートビュー撮影車が、データ撮影の際に、セキュリティ対策の不十分な無線ネットワークから、関係者に知らせずメールやインターネット閲覧記録などの個人情報を収集した事件につき、CNILは2011年3月に100000ユーロの罰金をグーグル社に科したことが記載されている。CNILは金銭制裁を科す前の2010年5月に、グーグル社に対して是正を求める催告を行っているが、グーグル社がこの要請に従わなかったので金銭制裁を発動するに至っている¹³¹。この事件は、1978年法の違反に対して直ちに金銭制裁が科されるのではなく、催告に従わない悪質なケースのみが金銭制裁の対象になるという CNIL の実務の傾向の好例である。

2011年は、催告が65件、警告が13件、金銭制裁が5件、処理中止命令が1件である。報告書によると、制裁手続の終了件数が2009～2010年より多いことが2011年の特徴であり、手続終了の割合は、CNILの催告が情報処理機関に対して1978年法への注意を払わせ、法律違反の状態を是正させる効力を有していることの表れである¹³²。

¹²⁷ 29ème rapport d'activité 2008 ,supra note125,p.48.

¹²⁸ 30ème rapport d'activité 2009 de la Commission nationale de l'informatique et des libertés,52p.http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL-30era pport_2009.pdf.

¹²⁹ 31ème rapport d'activité 2010 de la Commission nationale de l'informatique et des libertés,23p.http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL_rapport_annuel_%202010.pdf.

¹³⁰ 31ème rapport d'activité 2010 ,supra note129,p.23.

¹³¹ 31ème rapport d'activité 2010 ,supra note129,p.22.

¹³² 32ème rapport d'activité 2011 de la Commission nationale de l'informatique et des libertés,79p.http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/RA2011_CN

実際に、警告は催告が事前に出されたか否かにかかわらず行われる一方で、金銭制裁は催告に従わないことをもって初めて適用されることから、CNIL による取り締まりの効力の程度は金銭制裁の件数よりも警告の件数に反映される。そして、2011 年は不誠実な方法による情報収集の他、情報関係者の情報処理への拒否権の侵害に対して 10000～100000 ユーロの金銭制裁が科されている¹³³。

2012 年は、催告が 43 件で、警告が 9 件、金銭制裁が 4 件、処理中止命令が 1 件であった。不誠実な方法による情報収集や拒否権の侵害などが、金銭制裁の対象になっている¹³⁴。

以上、CNIL の制裁実務につき、毎年の変化を概観した。CNIL による制裁の中で最も重いのは金銭的な制裁であり、次項で述べる刑事罰との関係が問われるところであるが、警告や催告の段階で CNIL の要請に従う情報処理者が多いことから、金銭制裁が発動される割合はすべての年度において少ない。したがって、CNIL による取り締まりは一定以上の効果を上げていると考えられる。

第 2 項 CNIL の制裁と刑事罰

前項では、CNIL による制裁の運用のあり方について概観した。CNIL によって金銭制裁が発動される件数は少ないものの、金銭制裁と裁判所による刑罰との関係が問題となる。

1978 年法に違反してセンシティブ情報を収集した企業について、CNIL からの金銭制裁と刑事裁判所からの罰金の両方を科されたケースがある。まず、同一の企業が 1978 年法の違反を 2 度行った例について見ていくことにする。

(1) 複数回の違反が行われた事例

2002 年の大統領選以来、Impact Net 社はインターネット利用者に対して政治調査(世論調査)を行うようになった。この調査は匿名ということになっていたが、インターネット利用者に対して、いずれの候補者に投票しようと考えているのか、生まれた年、職業、メールアドレス等を正確に知らせるように求めていた。しかし、実際には調査への回答と共にメールアドレスが同一ファイルの中に集積されており、政治的な考え方についての情報は匿名化されていなかったことになる。この事件についての 2004 年 6 月 4 日ナンテール軽罪裁判所(Tribunal correctionnel de Nanterre) 判決によると、メールアドレス等の情報は回答者を特定し得るので、調査対象者に対して、調査は個人を特定するものではないと信じ込ませたことは、刑法 226-18 条所定の不誠実な方法による情報収集にあたる。続いて、収集された情報は政治に関わるものであるから、刑法 226-19 条の罪

IL_FR.pdf.

¹³³ 32ème rapport d'activité 2011 ,supra note132,p.80.

¹³⁴ 33ème rapport d'activité 2012 de la Commission nationale de l'informatique et des libertés,58p.http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL_RA2012_web.pdf.

にも該当しており、当該企業は CNIL に情報取り扱いの届出をしていたものの、届出内容と実際の取り扱いとは一致しておらず、目的を逸脱した情報処理であったということで、刑法 226-21 条にも違反すると判断された。以上の罪により、Impact Net 社の社長は 5000 ユーロの罰金を科された。

上記の刑事裁判後に、Impact Net 社は再び 1978 年法に違反してセンシティブ情報を処理したということで、最終的に CNIL による金銭制裁を科された。FAC インターナショナル社は、主に外国出身者に関する保険サービスを行う会社であり、Impact Net 社との契約に基づき、個人情報が Impact Net 社から FAC インターナショナル社に転送されていた。転送された情報には、アフリカのマグレブ (Maghreb) 出身のフランス在住者の住所の情報が含まれており、これが個人の出自に関するセンシティブ情報であるとして、1978 年法 8 条に違反しているのではないかとされた。CNIL は Impact Net 社に対して催告を出して、次のことを要求した。第一に、アフリカのマグレブ出身のフランス在住者に関する情報をどのように収集したのかを全て説明することである。第二に、当該情報の取り扱いが、個人の人種的・民族的出自を直接的または間接的に明らかにするものではないと解するに足りる弁明を CNIL に対して行うことである。Impact Net 社はこの催告を受けて、CNIL に回答を行った。その回答によると、FAC インターナショナル社は当該個人に関係するデータベースを使用することを希望していたので、Impact Net 社は FAC インターナショナル社に対して電話帳のファイルを貸していたということが判明した。しかし、Impact Net 社は、CNIL の上記の催告による説明要求があったにもかかわらず、当該情報処理が個人の person 的・民族的出自を直接的にまたは間接的に明らかにするものではないと認められるに足りる弁明をすることができなかったため、CNIL の催告に従わなかったとして 15000 ユーロの金銭制裁を科せられた¹³⁵。

このように、Impact Net 社は 1978 年法について二度の違反を行い、一つ目の違反には裁判所による罰金刑が科され、二つ目の違反には CNIL による金銭制裁が科された。CNIL による制裁金は 15000 ユーロであり、裁判所による罰金刑の金額より高額になっているので、このような状況は、刑法における累犯 (récidive) または 1978 年法 47 条における「繰り返された違反 (manquement réitéré)」に該当するのだろうか。まず、フランス刑法 132-13 条 1 項は、「自然人の場合は 10000 ユーロ以下の罰金に問われる重罪または軽罪についての確定判決を受けた法人が、刑の満了 (expiration) または時効 (prescription) から数えて 10 年以内に、同じ軽罪で刑事責任を問われた場合、法律がその罪に対して予定している刑罰の 10 倍の刑が適用され得る」と規定し、刑法 132-14 条は「ある軽罪で確定判決を受けた法人が、刑の満了または時効から数えて 5 年以内に、同じ軽罪または累犯の規則 (règles de la récidive) から見て類似の軽罪で刑事責任を問われた場合、法律が自然人について当該軽罪に予定している刑罰の 10 倍の刑が適用され得る」と規定することによって、累犯の場合に刑を加重している。

¹³⁵ Délibération CNIL du 31 janv.2008.

続いて、1978年法47条によると、初犯であれば150000ユーロ、5年以内に違反が繰り返された場合は300000ユーロが制裁金の上限とされており、金額が加重されている。しかし、このImpact Net社のケースは刑法における累犯でも、1978年法における「繰り返された違反」でもない。CNILは、ナンテールの裁判所での判決を把握していたものの、1978年法47条に規定されている「繰り返された違反」は、すでに企業がCNILからの制裁を受けた場合のみに適用されると解した¹³⁶。同様に、裁判所の判決の側から見ても、法人の累犯について規定する刑法132-13条と132-14条は、重罪または軽罪が繰り返された場合を想定して刑の加重について規定しているので、刑事裁判の前にCNILが金銭制裁を行ったとしても、刑法における累犯にはならない¹³⁷。CNILによる金銭制裁は行政的な制裁であって、刑罰ではないので、後に行われたいずれか一方が、前に行われたもう一方による罰金額または制裁金額を参照した上で金額を加重するという関係にはならないといえる。したがって、1回目の違反について罰金刑が科された後、再度の違反に対するCNILの制裁金の金額が増えるのは法によって予定されていることではない。同一の情報処理主体が複数回の違反を行った場合、CNILまたは刑事裁判所は、前の違反の際の制裁金額または罰金刑の金額を参照することなく金額を算定する裁量が認められているといえるだろう。

(2) 同一の違反に対する金銭制裁と罰金刑

また、上記のケースでは同一の企業が2回の違反を行い、それぞれ裁判所による罰金とCNILによる金銭制裁を受けたが、同一の企業による一つの違反に対して裁判所による罰金刑とCNILによる金銭制裁の両方が科された場合、これは「二重処罰の禁止」に反するだろうか。1978年法47条は、「刑事裁判が同一事実または付帯事実について判断するのに先立ってCNILが金銭的制裁を確定させた場合、CNILによる制裁金額は、刑事裁判の確定した金額から控除され得る」と規定している。この条文から見れば、CNILによる制裁と裁判所による罰金刑は、一方が他方を排除する関係には立っていないようである。一つの違反事実に対して金銭制裁と罰金刑が併科されることは法的に否定されないが、47条はこの2つの金額の調整について一つの方法を提示しているのである。例えばCNILが3万ユーロの金銭制裁を確定した後、刑事裁判官の決定した罰金額が5万ユーロであったとする。この際、刑事裁判官はその裁量によって、5万ユーロの罰金額から3万ユーロの金銭制裁額を引いて、最終的に2万ユーロの罰金刑とすることができるということである。金額の控除はあくまでも裁判官の裁量なので、金銭制裁額を割り引くことなく、3万ユーロの金銭制裁とは別に5万ユーロの罰金刑を科すことにも法的な問題はないといえる。このように、47条の条文によれば2つの金額調整を可能にしつつ、併科することも法的に排除されない。

¹³⁶ Mattatia, *supra* note119 ,p.324.

¹³⁷ Mattatia, *supra* note119,p.324.

また、コンセイユ・デタは、「CNILは、その性質・構成・職務権限から見て、『公正な裁判を受ける権利』を規定する人権と基本的自由の保護のための条約（ヨーロッパ人権条約）6－1条における裁判所（tribunal）として認められる行政機関である」と判断しているものの、1978年法45条以下において、CNILの催告に従わなかった場合でなければ金銭制裁を科すことができないと定められていることから、CNILを法律違反の罪名決定（qualification）について判断する機関としてみることはできないと判断する¹³⁸。このことから、コンセイユ・デタはCNILを刑事裁判所とは別個の性格を有する機関であると解しているように思われる。CNILが刑事裁判所ではなく、行政的な組織である以上、やはりCNILによる金銭制裁は刑罰ではなく、両方を科すことには法的な問題はないだろう。併科することが情報保護政策的に妥当であるか否かは、また別の問題である。

このように、1978年法の違反にはCNILによる金銭制裁と刑事罰の両方が予定されている。この二つを併科するか否かということをも別として、刑事裁判所による罰金よりも、CNILによる金銭制裁の金額の方が高額であることが指摘されている¹³⁹。論者はその理由を2つ挙げている。一つは、1978年法の違反によってCNILから注意を受ける情報処理責任者は、CNILの催告に従うことによって制裁を回避することが可能であり、制裁は警告や催告に従わなかった場合に発動されるからである。もう一つは、刑事裁判官にとって、1978年法違反の犯罪は、それまで裁判官が取り扱ってきた一般的な犯罪に比して軽微であると考えられているのではないかということである。1978年法違反の犯罪によって個人に対する物理的な侵害が発生するわけではなく、犯罪による損害の量を判断するのは容易ではないことから、裁判官は判断に際して慎重な態度を採っているのではないかとの分析が加えられている¹⁴⁰。

第4節 小括

本章では、フランス1978年法における情報処理のための諸規則と、様々な行為態様の情報侵害を処罰する刑法の重要な規定の意義と射程範囲、そして情報処理の取り締まりにつき強力な権限を有するCNILの実務の実態について検討してきた。

フランスの個人情報保護法制において、情報の不正な取り扱いに対して抑止力となり得るのは刑法による処罰とCNILによる制裁である。刑事罰の規定について、本論文では、いわゆる情報窃盗や第三者提供などの行為を直接的に処罰する規定を設けることの妥当性を検討するという問題意識から、刑法226－16条以下の規定の中でも、不正手段による情報収集の罪（226－18条）、本人の拒否にもかかわらず情報処理をする罪（226－18－1条）、センシティブ情報の処理の罪（226－19条）、本人への敬意や私生活の内奥を侵害する情報の第三者提供の罪（226－22条）を中心的に取り上げた。この

¹³⁸ CE référé n°311974 du 19 février 2008.

¹³⁹ Mattatia, *supra* note119,p.328.

¹⁴⁰ Mattatia, *supra* note119,p.328.

中で、情報窃盗を処罰する規定として典型的なのは226-18条である。この規定は、「詐欺的、あるいは不誠実、不正な手段」による情報収集を広くカバーするものであるので、本人の同意なく、あるいは本人に告知せず個人情報を入手するという、個人情報の侵害の中で最も頻繁に発生する違反行為に対する抑止が期待される。

この226-18条のみで情報侵害のケースの大半をカバーできるようにも思われるが、行為態様や対象となる情報の種類によって犯罪規定を細分化するのがフランス情報法制の特徴である。226-19条では、政治的・宗教的意見や人種的・民族的出自などの、いわゆるセンシティブ情報といわれる個人情報を、本人の明示的な同意なく入力・保存する行為が処罰の対象となる。この規定は、センシティブ情報はその重要性ゆえに他の一般的な個人情報とは区別されるべきであるという趣旨に照らして、1978年法8条が本人の単なる同意では足りず、明示的な同意のある場合に処理を認めていることに従っている。

しかし、本章第2節第3項第1款でも述べたように、現行1978年法8条は本人の明示的な同意のある場合以外にも、センシティブ情報の処理が認められるための例外を数多く認めているので、このことに応じて226-19条の処罰範囲も限定的なものになっている。処理が認められる例外を多くすることによって、センシティブ情報という特別なカテゴリーの存在意義が希薄になっている。1995年のEU指令8条に従ってセンシティブ情報の取り扱いについての規則を定めたという点ではイギリスの1998年データ保護法と同様であるが、イギリス法ではセンシティブ情報の不正な取り扱いを個別に処罰する規定は存在せず、データの不正取得等を処罰する55条が一括してカバーする形になっている。このようなイギリスの刑事罰規定と比較しつつ、フランス刑法226-19条の存在意義も見直されるべきであろう。

そして、本人の名声や私生活の内奥を侵害するような情報を無権限の第三者に提供する行為が226-22条で処罰される。この規定は、226-18条などの犯罪類型と異なり、故意のみならず過失（軽率または怠慢）による行為も処罰の対象となる。フランス刑法における「軽率または怠慢による過失」という概念は、「認識ある過失」と「認識なき過失」の両方を含んでいるので、226-22条の枠組では、ある個人の前科や、社会からは受け入れられないような奇妙な生活習慣などの個人情報の処理の後に、情報を知る権利のない第三者に不用意に漏らしてしまう行為までもが処罰の対象となる。このように、226-22条が認識なき過失の場合まで処罰の対象としている理由の一つは、情報の重要性であろう。「本人の名声や私生活の内奥を侵害」し得る情報に該当するのは、住所や年齢などの基本的な個人情報ではなく、過去の問題行動や前科、出自、親類に犯罪者が存在することといった内部的な情報であると思われる。そのように解すれば、226-22条が対象とする情報は226-19条におけるセンシティブ情報とも重複する部分があり、本人の名声や私生活の内奥を侵害する情報を第三者に漏洩するという行為は、フランス1881年出版自由法29条の名誉毀損罪とも重複する部分がある。これらの複数の罰条に該当し得る、違法性の高い行為であるからこそ、認識なき過失まで処罰されているのではな

いだろうか。第二に、センシティブ情報の取り扱いに関する例外は1978年法8条により多く認められており、その収集や保存などが可能になる余地は少なくないが、センシティブ情報を無権限の第三者に提供することが正当化される余地は狭いということである。したがって、重要性の高い情報を無権限の第三者に提供するという行為の違法性は高くなるだろう。そのように解すれば、226-19条とは異なり、226-22条が独立した処罰規定として存在する意義は否定できるものではないと思われる。

このように、フランス刑法では様々な情報侵害行為が処罰の対象となっている。しかし、裁判所による刑事罰よりも、CNILの制裁の方が1978年法違反の行為の防止に重要な役割を果たしているようである。CNILは情報処理を取り締まる専門機関であり、日常的に情報の取り扱い状況を観察したり、必要があれば調査したりしている。CNILは1978年法の違反を発見すると、直ちに金銭制裁を科すのではなく、まず催告をして改善を促すことが1978年法45条に規定されている。CNILの年次報告書では、催告や警告、金銭制裁の件数が記載されていたが、催告を受けて多くの情報処理者や企業が指示に従うという状況で一貫している。催告に従わない等の悪質なケースのみが金銭制裁の対象となるので、金銭制裁はおのずから少数にとどまっている。このことから、情報処理者にとってCNILによる金銭制裁は脅威であることがわかる。その一方で、裁判所による刑事罰が果たす役割はCNILの制裁に比して小さいようである。法律上、同一の違反に対してCNILの金銭制裁と刑事裁判による罰金刑の両方を科すことは排除されていないものの、罰金の金額はCNILの金銭制裁よりも低い傾向にある。そして、1978年法の違反件数は少なくないにもかかわらず、刑事罰が科される件数は少ないことが指摘されている。このような実態は、刑事裁判官はCNILに比して情報法に関する知識や経験が乏しいことと、情報に関する犯罪は殺人や傷害などの従来型の犯罪に比して、被害の程度を算定することが困難であることにより、刑事裁判官が1978年法違反行為を処罰することに謙抑的になっているのではないかという分析がなされているのは、本章第3節で述べた通りである。

CNILは、処理中止命令や警告などの強力な権限を与えられている。そして、CNILの制裁の中でも金銭制裁は重大の脅威となっている。CNILの専門性と権限により、法律違反の抑止に対する重要性は裁判所を上回っているが、悪質なケースについては刑事罰が適用される余地がある。このような役割分担によって、刑法の謙抑性が結果的に尊重されているように思われる。日本法において、情報窃盗などの行為を直接的に処罰する規定を創設するにあたり、刑罰の濫用にあたるのではないかという危惧がされている。しかし、フランス1978年法のように、専門的な第三者機関が取り締まりの権限を有していれば、刑罰が前面に出されることは自ずから少なくなるだろう。

第5章 ドイツ法における個人情報保護

第1節 連邦データ保護法の概要

本章では、ドイツにおける連邦データ保護法¹⁴¹（Bundesdatenschutzgesetz、略称はBDSG）について扱う。

具体的な検討の前に、データ保護法が成立するまでの背景について述べる¹⁴²。イギリス・フランス等の諸外国と同様に、情報化によって個人情報が頻繁に取り扱われるようになったことが立法の背景となっている。コンピュータの情報処理によって、再び独裁者や国家が市民の権利を脅かすことのないように、個人情報保護法制を整備する必要があるとの問題意識から、1970年10月、ヘッセン（Hessen）州において世界で初めての個人情報保護法が採択された。そして、ドイツ連邦政府は1977年に連邦データ保護法を制定し、1978年に施行された。

その後の1983年12月、連邦憲法裁判所による「国勢調査判決」¹⁴³が出され、自己の情報をどこまで公開するかということを決める「自己情報決定権（Recht auf informationelle Selbstbestimmung）」が基本権として承認された。本判決によると、誰が、いつ自己についての情報を知ったのかを市民が知ることができない社会秩序は、自己情報決定権とは両立しない。「人格の自由な発展」の基本権は、自己の個人情報の提供と使用を自身で決定する個人の権利を保障しているので、特に情報流通の透明性が保障され、個人の記録は秘密の伝達経路の中に隠されてはならず、その手段を本人が統制できなければならない、と解されている。この判決を受けて1990年に連邦データ保護法が改正され、1991年に施行された。1990年法における主な改正事項には、①公的機関によって発生した人格権侵害を含む損害に無過失損害賠償責任が認められたこと、②民間機関の損害賠償責任は無過失ではないものの立証責任が当該機関に科せられたこと、③保護の対象となる記録に文書記録が含まれるようになったこと等がある。

続いて、1995年EUデータ指令を受けて、2001年に再度の改正が行われた。EU指令に伴って改正された事項につき、特に重要なものは次のとおりである。まず、①EU指令8条を受けて、ドイツ連邦データ保護法3条9項にも「特別な種類のデータ」（いわゆる

¹⁴¹ドイツ連邦データ保護法の邦訳は、平松・前掲注（31）、藤原静雄「改正 連邦データ保護法（2001年5月23日施行）」季刊行政管理研究99号（2002年）76～94頁を参照した。

¹⁴²データ保護法成立までの経緯については、野村武司「改正ドイツ連邦データ保護法」社会科学研究所（山梨学院大学社会科学研究所・1993年）123～160頁、山下義昭「ドイツ連邦データ保護法の改正と残された課題（1）（2）」クレジット研究27号（2002年）184～193頁、クレジット研究29号（2003年）91～110頁、平松・前掲注（31）256頁以降と、藤原静雄「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」（2008年3月）におけるドイツの章・112頁以降を参照した。URL: <http://www.caa.go.jp/seikatsu/kojin/h21report3.pdf>。

¹⁴³BverfGE 65,1.人口、職業、住居、事業所などの国勢調査が、ドイツ基本法2条1項における「人格の自由な発展を求める権利」に反するか否かが争われた事件である。

「センシティブデータ」である。詳細は後述する) という概念と、その取り扱いのための例外的適法化要件が導入された。特別な種類のデータを収集するための適法化要件は、EU 指令における要件を援用するものとなっている。② 1990 年データ保護法は、第三者機関である連邦データ保護観察官（以下、連邦監察官とする）と監督官庁に対して、データ保護法違反の十分な根拠のある場合に限って監査を認めていたが、EU 指令 28 条 3 項にはそのような制限が設けられていないので、2001 年データ保護法ではこの規定が削除され、権限が拡張されている。

また、EU 指令に依拠していない改正事項として、ビデオ監視がある。一般市民が立ち入ることのできる場所におけるビデオ監視は、2001 年改正前のドイツの公的または民間機関によって行われていたが、2001 年改正法 6b 条によって、ビデオ監視に法的根拠が与えられるようになった。6b 条によると、ビデオ監視は①公的機関の職務遂行のため、②住居権の行使のため、③正当な利益を行使するために、具体的に確定された目的につき必要性があり、かつ、本人の保護に値する利益が優越するとの根拠がない場合に限って許容される。

このように、連邦データ保護法は EU データ指令を受けて多くの改正がなされたが、2009 年 8 月 14 日にも法改正が行われ、2009 年 9 月 1 日に施行されている。2009 年の法改正では、個人信用調査会社へのデータの提供（28a 条）と、本人との契約関係の開始・実行・終了について判断する目的で、本人との将来的な契約関係の可能性を示す数値 (Wahrscheinlichkeitswert) のデータを収集または利用する（いわゆるスコアリング）ための条件（28b 条）についての規律が新しく設けられた。

第 1 項 基本事項について

データ保護法の目的は、「自己の個人データの扱いによって人格権 (Persönlichkeitsrecht) を侵害されることから、個人を保護すること」である（1 条 1 項）。

本法では「個人データ (Personenbezogene Daten)」が保護の対象となり、個人データの収集 (Erhebung) と処理 (Verarbeitung) および利用 (Nutzung) が規制対象となる（1 条 2 項）。ここでいう「収集」は本人に関するデータを入手することであり（3 条 3 項）、「処理」は個人データを蓄積 (Speichern)、変更 (Verändern)、提供 (Übermitteln)、封鎖 (Sperren)、または消去 (Löschen) することである（3 条 4 項）。そして、「利用」は「処理」に関係しない個人データのあらゆる使用である（3 条 5 項）。

本法 3 条 1 項によると、個人データは「特定のまたは特定しうる自然人 (本人) の人的または物理的状況に関する個別の記載事項 (Einzelangaben)」と定義される。この条文からは、個人に関する事実的な事項のみが対象となるように思われるが、個人についての評価を含む全ての情報が含まれると広く解されている¹⁴⁴。そして、イギリス 1998 年データ保護法とフランス 1978 年法と同様に、ドイツ連邦データ保護法にも、取り扱いに特

¹⁴⁴Gola/Klug, Grundzüge des Datenschutzrechts, C.H.Beck, 2003, S. 40.

別な配慮を必要とする「センシティブ情報」という概念がある。連邦データ法3条9項では、「特別な種類の個人データ (Besondere Arten personenbezogener Daten)」と呼ばれており、「人種のおよび民族的出自、政治的意見、宗教的または哲学的な信条、労働組合への加入、健康または性生活に関する事項」と定義されている。特殊な種類の個人データの適法な取り扱いのための要件については後述する。

この法律において、本人には次の権利が認められている。それは、①自己業務目的で本人に知らせることなく個人データが蓄積された場合に、データの種類や収集・利用・処理の目的と責任機関について通知 (Benachrichtigung) を受ける権利 (33条1項)、②自己に関して蓄積された個人データ、データが譲渡される相手、データが蓄積される目的などについての開示 (Auskunft) 請求権 (34条)、③データの訂正 (35条1項)、消去 (35条2項)、封鎖 (35条3項) の権利、④異議を申し立てる (widersprechen) 権利 (35条5項、20条5項) である。

第2項 個人データの収集・処理・利用の適法化要件

(1) 一般的な個人データについて

①官民共通の規定

個人データの取り扱いが認められるためにはいくつかの条件がある。まず、官民共通の規定について述べる。個人データを収集・処理または利用するためには、データ保護法もしくは他の法規定によって許容され、または命じられているか、または本人が同意している必要がある (4条1項)。次に、個人データは原則的に本人から収集されなければならない。本人以外からの収集が認められるのは、法規定が定め、または不可避であるとしている場合、本人からの収集が均衡を欠く過度の出費を要すると考えられる場合などであって、保護に値する重大な本人の利益が侵害される根拠 (Anhaltspunkte) が存在しない場合である (4条2項)。

次に、自らまたは委託によって個人データを収集、処理または利用する公的および民間機関は、データ保護法の規定の実施、特にこの法律の附則に挙げられた要請の実施を保障するために、必要な技術的・組織的措置 (technischen und organisatorischen Maßnahmen) を講じなければならない (9条第1文)。このような措置が必要とされるのは、もっぱら、達成しようとする目的と費用が「適切な比例関係 (angemessenen Verhältnis)」にある場合である (9条第2文)。

9条の附則は以下の通りである。

個人データが自動的に処理または利用される場合、行政庁内または企業内の組織は、データ保護の特別の要請に適合するように編成されなければならない。その際、特に、保護される個人データまたはデータの範疇の種類に応じて、次のような措置が講じられなければならない。

- 1 個人データが処理または利用されるデータ処理施設 (Datenverarbeitungsanlagen)

に無権限者が立ち入るのを禁止すること（立ち入りの監督）

2 データ処理システムが無権限者に利用され得るのを防ぐこと（アクセスの監督）

3 データ処理システムの利用権限者が、もっぱらその介入権限に服するデータのみに入介入できると、個人データが処理、利用の際および蓄積後に無権限で読まれたりコピーされたり、変更または除去され得ないことを保障すること（介入監督）

4 個人データが電子工学的な転送の際、またはその輸送中、またはデータ記録媒体への蓄積中に、無権限で読まれたりコピーされたり、変更または除去されたりする可能性のないことと、データ伝送の装置を通して、いかなる機関への個人データの提供が予定されていたかを審査し、確定することが可能であることを保障すること（譲渡の監督）

5 個人データの、データ処理システム内への入力、変更または除去の有無、およびその行為者を、事後的に審査、確認することが可能であることを保障すること（入力の監督）

6 委託によって処理される個人データは、委託者の指示通りにのみ処理することができるということを保障すること（委託の監督）

7 個人データが、偶然の破壊または喪失から保護されていることを保障すること（処理の監督）

8 異なる目的のために収集されたデータが、別々に処理できることを保障すること

②公的機関の個人情報処理に関する規定

続いて、公的機関による個人情報処理の適法化要件は、データ保護法 13 条から 16 条に規定されている。まず、13 条 1 項によると、当該個人データを知ることが責任機関の任務遂行のために必要な場合に限ってデータの収集が許容される。次に、個人データの蓄積、変更および利用は、責任機関の権限に属する任務の遂行のために必要であり、かつ、データの収集目的のために行われる場合に限って認められる。データの収集が事前に行われない場合、データは蓄積された目的のためにのみ変更または利用され得る（14 条 1 項）。そして、他の目的のための蓄積、変更または利用は、本人が同意している場合、本人の利益のためになることが明らかであり、他の目的のためであることを知ることによって本人が同意しないと想定する理由がない場合、第三者の権利の重大な侵害を予防（Abwehr）するために必要な場合等には例外的に認められる（14 条 2 項）。

15 条と 16 条は公的機関によるデータの提供について規定する。まず、15 条 1 項によると、公的機関から別の公的機関へのデータの提供は、①当該データ提供が、提供する機関、もしくはデータの提供を受ける機関の所掌事務を遂行するために必要である場合と、②データ保護法 14 条による利用が許容されるための要件が満たされている場合に許される。次に、16 条 1 項によると公的機関から民間機関へのデータ提供は、①当該データ提供が、提供する機関の権限に属する任務を遂行するために必要であり、かつ、データ保護法 14 条によって利用が許容されるための要件が満たされている場合、または、②データの提供を受ける第三者が、提供されるデータを知ることにつき正当な利益のあることを疎

明（darlegen）し、かつ、本人が提供させないことについて保護に値する利益を有しない場合に許容される。

③民間機関の個人情報処理に関する規定

続いて、民間機関による個人情報処理の適法化要件については、データ保護法 28 条以下で規定されている。

28 条 1 項は、自己の業務目的の遂行のための手段として個人データの収集、蓄積、変更もしくは提供し、または利用することは、次のいずれかに該当する場合に許容されることを規定する。

①本人との契約関係または契約類似の信頼関係のために使用する場合

②責任機関の正当な利益を保護するために必要であり、かつ、処理もしくは利用させないことについて、本人の保護に値する利益が優越すると推定する理由がある場合

③データが一般にアクセス可能であるか、または責任機関がそれを公表することが許されている場合。ただし、処理または利用させないことについての本人の保護に値する利益が明らかに優越する場合はこの限りではない。

続いて、29 条 1 項は第三者提供の目的で個人情報を収集・蓄積・変更するための条件について、29 条 2 項は提供が許容されるための条件について規定する。

29 条 1 項によると、宣伝（Werbung）、興信所（Auskunfteien）、名簿業者（Adresshandel）に役立つデータの収集、蓄積、変更は、次の場合に許容される。

①収集、蓄積または変更を拒否することについて、本人の保護に値する利益があると推定する理由がない場合

②データが一般に公表されている情報源から収集することができるか、または責任機関が公表してよい個人データである場合。ただし、収集、蓄積、変更を拒否することについて本人の保護に値する利益が明らかに優越する場合はこの限りではない。

③28 条 a の 1 項または 2 項の必要条件が充足される場合。28 条 a 2 項第 4 文におけるデータは、収集または蓄積されてはならない。28 条 1 項第 2 文と 3 項 3 b は適用されるべきである。

次に、29 条 2 項は、1 項による目的の範囲内での提供は①データを提供される第三者が、当該データを知ることについて正当な利益を疎明する場合で、かつ②データの提供を拒否することについて、本人の保護に値する利益があると推定する理由がない場合に許容される旨を定めている。

（２）特別な種類の個人データについて

第 1 項で述べた通り、データ保護法では人種や宗教に関するデータは「特別な種類の個人データ」として区別されている。ここでは、特別な種類の個人データの適法な取り扱いのための条件について概要を述べる。

第一に、特別な種類の個人データが収集、処理または利用されるためには、明示的（*ausdrücklich*）で当該データと関連する同意が必要である（4 a 条 3 項）。これは、公的機関と民間機関に共通の条件である。

①公的機関による情報収集等に関する規定

続いて、1 3 条 2 項によると、以下のいずれかに該当する場合には、公的機関による特別な種類の個人データの収集が認められる。

①法令の規定があるか、または重要な公益上の理由により、収集が不可欠である場合

②本人が 4 a 条 3 項に基づいて同意した場合

③本人の身体的または法的な理由から同意を与えることができない場合であって、本人の、または第三者の生死に関わる利益（*lebenswichtiger Interessen*）の保護のために必要な場合

④本人が公表したことが明確な個人データが問題になっている場合

⑤公的な秩序に対する著しい危険を防止するために必要な場合

⑥公共の福祉（*Gemeinwohl*）に対する重大な不利益の防止、または公共の福祉上重大な利益の保護のために必要な場合

⑦健康への配慮（*Gesundheitsvorsorge*）、医学上の診断（*medizinischen Diagnostik*）、健康管理（*Gesundheitsversorgung*）または公衆衛生業務（*Gesundheitsdiensten*）の取り扱いもしくは公衆衛生業務のために必要であり、かつ、これらのデータの処理が医師または同様の守秘義務（*Geheimhaltungspflicht*）を有する者によって行われる場合

⑧学術研究（*wissenschaftlicher Forschung*）のために必要であり、かつ、研究計画の実施についての学術上の利益が、データ収集を拒否する本人の利益に著しく優越し、かつ研究目的が他の方法で達成できないか、またはその達成のために均衡を欠く過度の出費を要する場合

⑨防衛（*Verteidigung*）、または危機の克服（*Krisenbewältigung*）もしくは紛争の阻止（*Konfliktverhinderung*）もしくは人道的措置（*humanitäre Maßnahmen*）の領域における連邦の公的機関の、国家を超えた義務もしくは国家間の義務（*wisichenstaatlicher Verpflichtungen*）の遂行のために必要な場合

ここまでは、特別な種類の個人データの収集に関する規定であるが、1 4 条 5 項 1 号・2 号は、このようなデータの蓄積・変更・利用の際の条件について定めている。1 4 条 5 項 1 号によると、上記 1 3 条 2 項 1 号から 6 号と 9 号による収集が認められる場合に蓄積・変更・利用が許容され、1 4 条 5 項 2 号には、学術研究の実施に必要な場合、という 1 3 条 2 項 8 号と同一の規定が置かれている。そして、1 4 条 6 項は、上記 1 3 条 2 項 7 号の目的のために特別な種類の個人データの蓄積・変更・利用は、1 3 条 2 項 7 号に掲げられた者（医師または医師と同様の守秘義務を有する者）に適用される守秘義務規定に従う旨を規定する。このように、1 3 条 2 項の規定の内容とほとんど重複しており、特別な

種類の個人データの収集、蓄積、変更、利用には共通のルールが適用されるといえる。

②民間機関による情報収集等に関する規定

データ保護法 28 条 6 項から 9 項は、民間機関による特別な種類の個人データの取り扱いについての条件を定めている。

28 条 6 項によると、自己の業務目的のための特別な種類の個人データの収集、処理、利用は、本人が 4a 条 3 項による同意をしない場合には以下の各号の場合に認められる。

①本人の身体的または法的な理由から同意を与えることができない場合であって、本人の、または第三者の生死に関わる利益の保護のために必要な場合

②本人が公表したことが明確な個人データが問題になっている場合

③法律的な請求権 (*rechtlicher Ansprüche*) の主張 (*Geltendmachung*)、行使 (*Ausübung*)、または防御 (*Verteidigung*) に必要であり、かつ、収集、処理、利用を拒否する本人の保護に値する利益が優越することを推定させる根拠が存在しない場合

④学術研究のために必要であり、かつ、研究計画の実施についての学術上の利益が、データ収集を拒否する本人の利益に著しく優越し、かつ研究目的が他の方法で達成できないか、またはその達成のために均衡を欠く過度の出費を要する場合

続いて、28 条 7 項第 1 文によると、「健康への配慮、医学上の診断、健康管理または公衆衛生業務の取り扱い、もしくは公衆衛生業務のために必要であり、かつ、これらのデータの処理が医師または同様の守秘義務を有する者によって行われる場合」には特別な種類の個人データの収集が認められる。そして、第 2 文によると、上記 28 条 7 項第 1 文における目的のためにデータを処理・利用する場合には、第 1 文に掲げられた者（医師および医師と同様の守秘義務を有する者）に適用される守秘義務規定に従う。

28 条 8 項第 1 文によると、上記 6・7 項以外の目的のためには、28 条 6 項 1 号から 4 号まで、または 28 条 7 項第 1 文の要件のもとでのみ、提供・利用することができる。そして、28 条 8 項第 2 文によると、このようなデータの提供と利用は、国家および公共の安全 (*staatliche und öffentliche Sicherheit*) にとつての重大な危険 (*erheblichen Gefahren*) の防止のために、ならびに著しく重大な犯罪行為 (*Straftaten von erheblicher Bedeutung*) の追求 (*Verfolgung*) のために必要な場合にも認められる。

28 条 9 項第 1 文によると、政治的、哲学的、宗教的または労働組合的で、営利目的を追求しない組織は、組織活動にとって必要である限り、特別な種類の個人データを収集、処理または利用することができる。第 1 文の規定は、組織の構成員 (*Mitglieder*) の個人データ、または組織の活動目的との関係で、組織と定期的な接触 (*regelmäßig Kontakte*) を有する者の個人のデータにのみ適用される (28 条 9 項第 2 文)。

4a 条 3 項に基づく本人の同意がある場合に限り、この個人データを組織外の者または他の機関に提供することができる (28 条 9 項第 3 文)。

29 条 5 項によると、民間機関が提供目的のために、特別な種類の個人データの業務上

収集と蓄積を行う場合には、上記 28 条 6 項から 9 項までの規定が準用される。

このように、公的機関と民間機関では重複する条件もあるが、民間機関の方が、特別な種類の個人データを扱うことが認められるための例外が若干多く設けられている（上記 28 条 9 項には政治的・哲学的・宗教的または労働組合的な団体のためのデータ処理の規定があるが、この条項は公的機関によるデータの取り扱いには設けられていない）。

第 3 項 連邦データ・情報自由保護観察官（連邦観察官）

イギリス 1998 年データ保護法とフランス 1978 年法と同様に、ドイツ連邦データ保護法においても、情報処理等を取り締まる第三者機関が置かれている。しかし、イギリスが情報コミッショナーを、フランスが CNIL を置いているのとは異なり、ドイツでは単一の監督機関が国内のデータ処理等を一括して監督するのではなく、監督機関が 3 層に分けられている。ドイツの連邦公的機関と、民営化された鉄道・郵便・通信事業は「連邦データ・情報自由保護観察官（Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. 以下、連邦観察官とする）」によって監督され、州の公的機関は州のデータ保護観察官（Landesbeauftragte für den Datenschutz）によって監督される。そして、民間機関と公法上の競争企業は監督官庁（Aufsichtsbehörde）による監督を受ける。まず本項では、連邦公的機関と一部の民営化事業を監督する連邦観察官の制度概要について述べる。

（1）連邦観察官の地位

連邦観察官は、連邦政府（Bundesregierung）の提案に基づき、ドイツ連邦議会（Deutscher Bundestag）の過半数以上の可決によって選出される（22 条 1 項第 1 文）。選出される際に 35 歳以上であること（22 条 1 項第 2 文）以外に、連邦観察官の資格要件についての規定はない。

連邦観察官は独立して（unabhängig）職務を行い、データ保護法にのみ従う（22 条 4 項第 2 文）。連邦観察官は連邦政府の法的監督の下にある（22 条 4 項第 3 文）。これらの条文は、連邦観察官が独立した第三者機関であることの根拠となる。内務大臣の指揮命令に服することはなく、データ保護法のみ拘束される。

（2）連邦観察官の職務

①苦情処理

データ保護法 21 条では、連邦公的機関による自己の個人データの収集、処理、利用の際に自己の権利を侵害されたと考える者は誰でも、連邦観察官に助力を求めることが認められている。各個人に与えられた苦情申立ての権利により、苦情処理は連邦観察官の主要な任務となっている。連邦観察官は、職務において打ち明けられた事実や申し立てを行った人物について証言を拒否する権利があり（23 条 4 項）、職務上知り得た事実について守

秘義務がある（２３条５項）。このような証言拒絶権と守秘義務によって、個人の苦情申立ての権利は担保されている。

②監督と調査

データ保護法２４条１項では、連邦の公的機関がこの法律の規定とデータ保護に関する他の法律の規定を遵守しているか否かを、連邦観察官が監督する（kontrollieren）ことが定められている。連邦観察官とその委任を受けた者（Bundesbeauftragten und seine Beauftragten）は、監督任務の遂行にあたって、次の権限を与えられている（２４条４項）。

１ 質問への回答（Auskunft）、並びに２４条１項による監督と関連したあらゆる書類（Unterlagen）、特に蓄積されたデータ（die gespeicherten Daten）とデータ処理プログラム（Datenverarbeitungsprogramme）を閲覧すること

２ すべての執務室（Diensträume）にいつでも立ち入ること

連邦観察官は、監督の対象となった公的機関にその結果を報告することになっている（２４条５項第１文）。連邦観察官はこの報告において、データ保護の改善（Verbesserung）、特に個人データの処理または利用の際の瑕疵（Mängeln）の除去について提案することができる（２４条５項第２文）。そして、連邦観察官によるこの提案は、２５条に規定されている異議（Beanstandungen）とは独立して行われる（２４条５項第３文）。

③異議¹⁴⁵

連邦観察官は、この法律の規定またはデータ保護に関する他の法律の規定に関する違反（Verstöße）、またはその他データの処理もしくは利用に際して瑕疵を確認した場合に、次の者に対して異議を唱えることができる（２５条１項）。

１ 連邦行政については、これを所管する最上級連邦官庁（Bundesbehörde）

２ 連邦鉄道資産（Bundeseisenbahnvermögen）については、代表者（Präsidenten）

３ ドイツ連邦郵便（Deutsche Bundespost）の特別財産から、法律によって設立された企業については、郵便法に基づく排他的な権利が帰属する限りで、その取締役会（Vorständen）

４ 連邦直属の公法上の社団（Körperschaften）、施設および財団、ならびにこれら社団、施設および財団の連合（Vereinigungen）については、その理事会またはその他の代表権のある機関

連邦観察官には、このように異議を申し立てる権限があるが、問題となっている瑕疵が些細な、または一時的なものである場合、連邦観察官は異議を見合わせ、または関係機関にして、瑕疵についての態度表明（Stellungnahme）を要求するのをやめることができる

¹⁴⁵藤原・前掲注（１４１）８７頁では“Beanstandungen”という単語が「異議」と訳出されている一方で、平松・前掲注（３１）２７０頁では「警告」と訳出されている。「警告」という訳は原語と合致しないので、ここでは「異議」という訳に従う。

（25条2項）。連邦観察官による異議が申し立てられた場合には、上記の機関は当該違反や瑕疵についての見解を表明しなければならないが、25条2項は例外規定となっている。また、連邦観察官は連邦政府と連邦機関に対して、データの改善に関する勧告（Empfehlung）や、データ保護の照会に対する助言（Beratung）を行うことができる（26条3項）。

④報告

連邦観察官は、ドイツ連邦議会に2年ごとに活動報告（Tätigkeitsbericht）をしなければならない。この活動報告は、ドイツ連邦議会と一般市民（Öffentlichkeit）に対して、データ保護の重要な展開について知らせるものである（26条1項）。連邦観察官は連邦の公的機関と民営化された一部の事業について監督するが、この報告書は個人情報保護を実践・改善し、個人情報保護意識を高める手段であるという理由から、報告書では民間部門における個人情報保護の状況についても記述しなければならないとされている¹⁴⁶。

以上、連邦観察官の職務権限について概観してきた。連邦観察官は、個人情報保護の監督のために調査・立ち入り検査をしたり、異議を申し立てることができるものの、刑罰を科したり、フランスの CNIL のように違反に対して金銭制裁を科したりする権限はない。その理由は、連邦観察官はいずれの組織のもとにも属さず、他の行政組織との間に上下関係が存在しないことにある。ドイツでは、行政組織内部で刑罰を科すには、自らの組織が上級行政庁である必要があると考えられている¹⁴⁷ので、独立の存在である連邦観察官は刑罰を発動する主体たり得ないのである。

第4項 監督官庁

ドイツでは、民間機関と一部の公法上の競争企業によるデータ処理は、連邦観察官ではなく各州の監督官庁による監督の対象となる（38条1項）。州の公的機関は州のデータ保護観察官（Landesdatenschutzbeauftragte）による監督の対象となる。州の民間機関については、各州の監督官庁が監督する。

監督官庁は、この法律またはデータ保護に関する他の法律の規定に対する違反を確認した場合には、違反について本人に知らせ、訴追又は処罰する権限を有する機関に違反を告発する権限がある。そして、重大な違反の場合には、違反のあったことを営業監督官庁（Gewerbeaufsichtsbehörde）に、営業法上の措置（gewerberechtlicher Maßnahmen）の実施のために知らせる権限を有する。連邦観察官が報告を義務付けられているのと同様に、監督官庁は、定期的に、遅くとも2年ごとに活動報告書を公表しなければならない（38

¹⁴⁶Alexander Roßnagel, Handbuch Datenschutzrecht : die neuen Grundlagen für Wirtschaft und Verwaltung, C.H.Beck, 2003, S.515.

¹⁴⁷藤原静雄「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）におけるドイツの章・67頁。

URL: <http://www.caa.go.jp/seikatsu/kojin/h22report2.pdf>.

条1項第5文)。

連邦の公的機関に関する21条第1文が準用され、非公的機関による自己の個人データの収集、取扱い又は利用に際して、自己の権利を侵害されたと考える者は誰でも、監督官庁に助力を求めることができる。

続いて、38条4項によると、監督官庁によって監督を委託された者は、監督官庁に託された任務の実行に必要な限りで、営業および業務時間内に、対象となっている機関の敷地および事業所に立ち入り、そこで審査(Prüfungen)および視察(Besichtigungen)を行う権限を有する。そして、被委託者は業務上の書類、特に4g条第2項第1文による一覧表(データ処理を行う機関の名称、データ処理の目的、データ処理権限のある者等が記載されている)、ならびに蓄積されている個人データおよびデータ処理プログラムを閲覧することができる。連邦公的機関に対する連邦観察官の調査権限や立ち入り権が認められているのと同様に、民間機関も立ち入りや書類閲覧などの審査・調査の対象となっている。

そして、監督官庁はデータ保護を保障するために、個人データの収集、処理および利用について確認された違反、または技術的若しくは組織的な瑕疵(Mängel)を除去(Beseitigung)するための措置を命じることができる(38条5項第1文)。2009年の法改正前までは、監督官庁のこのような命令権には「データ保護法等の規定が、個人データの自動処理または自動化されていないデータファイル内もしくはデータファイルからの個人データの処理を規律している限り」、「9条に基づく要求の範囲内で」という条件が付されていたが、法改正によって削除された。

第5項で後述するように、この命令に従わなかった者には過料(Bußgeld)が科せられる(43条1項第11号)。重大な違反および瑕疵の場合、特に人格権への特別な危険と結びついている場合、38条5項第1文に基づく命令(Anordnung)に反し、かつ強制金(Zwangsgeldes)を科されたにもかかわらず、当該違反もしくは瑕疵が相当な期間内に除去されなかった時は、個人データの収集、処理、利用または個々の処理方式の使用を禁止(untersagen)することができる(38条5項第2文)。連邦観察官が是正命令や過料、または刑罰を発動する権限を有さない一方で、監督官庁には強い権限が法律によって認められている。

第5項 過料と刑事罰

データ保護法43条には過料規定が、44条には罰則規定が置かれている。まず、過料規定の中で特に重要なものを概観する。

(1) 過料規定

過料規定はデータ保護法43条1項と2項にあり、1項は、情報の取り扱いに必要な届け出を行わない、本人に必要な告知をしないといった、比較的単純な手続違反が秩序違反となることについて規定する。そして、38条5項第1文による監督官庁の命令に違反する行為が43条1項11号によって秩序違反となることは前述の通りである。

2 項は、手続違反を超えた、情報の不正取得等について規定しており、故意 (vorsätzlich) または過失 (fahrlässig) によって以下の行為をする者は秩序違反 (Ordnungswidrig) に問われる。

1 権限なく (unbefugt)、一般的にはアクセスできない個人データを収集または処理する行為

2 権限なく、一般的にはアクセスできない個人データを、自動処理方法を用いていつでも呼び出せるようにする行為

3 権限なく、一般的にはアクセスできない個人データを呼び出し、または、自動処理による、または自動化されていないデータファイルから自ら入手または他者に入手させる行為

4 一般的にはアクセスできない個人データの提供 (Übermittlung) を、虚偽の申告 (unrichtige Angaben) によって受ける行為

データ保護法 10 条 5 項は、「一般的にアクセス可能」という文言を、「事前の届出、許可または対価の支払いの有無にかかわらず、何人も利用できる (nutzen kann) データ」と定義しているので、43 条 2 項 1 ～ 4 号における「一般的にアクセスできないデータ」は利用が制限されているデータのことである。

5 16 条 4 項第 1 文、28 条 5 項第 1 文に反し、および 29 条 4 項、39 条 1 項第 1 文または 40 条 1 項との関連で、提供機関から提供されたデータを他の目的のために利用する行為

16 条 4 項第 1 文と 28 条 5 項第 1 文によると、データの提供を受ける第三者は提供された目的の実現のためにのみ、データを処理または利用することが認められる。39 条 1 項第 1 文は、「職業もしくは特別の職業上の秘密に服する個人データ、およびその職業上または職務上の義務を果たす際に、守秘義務のある機関の自由な使用に供された個人データについて、責任機関は当該個人データを得た目的のためにのみ処理または利用することが許される」と規定し、40 条 1 項は、「学研究目的で収集または蓄積された個人データは、学研究目的のためにのみ処理または利用することを認められる」と規定する。このように、データ保護法にはデータが当該目的のためにのみ処理・利用されるべきことが定められており、目的外の利用が秩序違反行為となる。

5b 28 条 4 項第 1 文に反して、宣伝 (Werbung) または市場調査・世論調査 (Markt- oder Meinungsforschung) の目的のためにデータを処理または利用する行為

28 条 4 項第 1 文は、「本人が責任機関に対して、宣伝または市場調査・世論調査の目的のための自己のデータの処理または利用について異議を申し立てている場合、この目的のための処理または利用は認められない」と定めており、故意または過失による違反が秩序違反となる。

7 42a 条第 1 文に反して、告知 (Mitteilung) をしないこと、不正確な、不完全な、

または遅延した通知を行うこと

4 2 a 条第 1 文は、「2 条 4 項に規定される民間機関、または 2 7 条 1 項第 1 文 2 号に規定される公的機関は、貯蔵された

- 1 特別な種類の個人データ（3 条 9 項）
- 2 職業上の秘密に関する個人データ
- 3 犯罪行為または秩序違反行為、または犯罪行為や秩序違反行為の嫌疑に関する個人データ

4 銀行またはクレジットカードに関する個人データについて、
違法に伝達されているか、またはその他の方法によって第三者の知るところとなっていて、かつ本人の権利または保護すべき利益に対して重大な障害があり、本条第 2 文から第 5 文までの規定に従って、所轄の監督官庁ならびに本人に即座に告知されなければならないことを確認する」と規定している。4 2 a 条第 1 文の 1 から 4 の個人データの漏洩による不利益が発生している場合に、データを扱う民間機関と公法上の競争企業としての公的機関には適正な告知を行う義務があり、故意または過失によって当該義務に違反した場合には過料の対象となり得る。

以下は、過料の金額についての規定である。4 3 条 3 項によると、第 1 項に規定される秩序違反には 5 0 0 0 0 ユーロ以下の過料を、第 2 項に規定される秩序違反には 3 0 0 0 0 0 ユーロ以下の過料が科される。4 3 条 1 項の秩序違反よりも 4 3 条 2 項のそれの方が重大であることが、上記の法定刑に反映されている。過料は、秩序違反による行為 (*der Täter aus der Ordnungswidrigkeit*) がもたらした経済的な利益 (*wirtschaftlichen Vorteil*) を上回らなければならない (4 3 条 3 項第 2 文)。この場合、第 1 文に規定された金額では不十分であれば、これを超えることができる (4 3 条 3 項第 3 文)。

(2) 刑罰規定

データ保護法における刑事罰規定は以下の通りである。

前述の 4 3 条 2 項の秩序違反行為を、対価を得て、または自己もしくは他人の利益を図るために、または他人を害することを意図して行った場合には、2 年以下の自由刑 (*Freiheitsstrafe*) または罰金刑に処す。(4 4 条 1 項)。

犯罪行為は告訴 (*Antrag*) によってのみ訴追される。告訴権者は本人、責任機関 (*verantwortliche Stelle*)、連邦観察官または監督官庁である (4 4 条 2 項)。

以上、データ保護法における過料・刑罰規定の概要について整理した。ドイツ連邦データ保護法では、連邦の公的機関のデータ取扱いを取り締まる連邦観察官には過料や刑罰を科す権限はないが、民間機関のそれを取り締まる監督官庁には、データの不正取得や目的外使用などの不正な取扱いに対して過料を科すことができる。一般的な個人データとは区別されたセンシティブな個人データ (特別な種類の個人データ) という概念を設けてい

る点では、イギリス1998年データ保護法とフランス1978年法と共通している。その一方でドイツ連邦データ保護法では、前述の43条2項7号によって、特別な種類の個人データの漏洩が不利益をもたらしている場合に適切な告知をしないという手続違反につき、個別の規定が存在するにとどまっている。フランス刑法とは異なり、特別な種類の個人データの入力や保存といった、手続違反を超えた不正な取り扱いは個別に規定されていない。ドイツ連邦データ保護法に「特別な種類の個人データ」という概念が導入されたのは、EUデータ指令を受けた2001年改正法からであり、2001年改正の契機となったEUデータ指令にも、センシティブなデータに対する不正取得等を特別の構成要件で処罰する規定は存在しない。このことから、ドイツ連邦データ保護法はEU指令に沿って、特別な種類の個人データについては別個の処理条件を設ければ足り、個別の過料・刑罰規定までは必要ないと解したのではないだろうか。43条2項7号に該当する行為以外は、特別な種類の個人データであるか否かにかかわらず、同一の過料・刑罰規定が予定されているといえる。

第2節 データ保護法における過料と刑罰について

第1項 過料

第1款 客観的な成立要件

第1節第5項ではデータ保護法における過料・刑罰規定の概要について触れたので、本節ではその成立要件の詳細について扱う。

データ保護法43条1項と2項は、秩序違反行為につき過料を科すことを定めている。1項は単純な法定手続違反に関する規定である一方、2項は手続違反を超えた、個人データの不正な取り扱いについて規定している。

43条2項1号は、無権限者による個人データの収集と処理を対象としており、データの抹消と利用は対象外である。データの利用は様々な行為態様を含んでいることから、過料の対象外となったものと解されている¹⁴⁸。

43条2項2号は、個人データをいつでも呼び出せるようにする行為を対象とする。実際にデータを呼び出すことは成立要件ではない。データの呼び出しは常に行われるわけではないので、場合によっては呼び出しが行われたか否かが判然としないこともあり、データ呼び出しの準備行為には、貯蔵されたデータを危険にさらす蓋然性があるので、抽象的危険犯（*abstraktes Gefährdungsdelikt*）として位置づけられる¹⁴⁹。

43条2項3号前段では、個人データを実際に呼び出す行為が対象となる。この号で保護される個人データは、呼び出すことが可能であり、自動化処理されたものに限定され、43条2項2号とは異なり、データの呼び出しのために準備されているか否かは問題とな

¹⁴⁸ Peter Gola / Christoph Klug/ Barbara Körffler, BDSG : Bundesdatenschutzgesetz : Kommentar, 10. Aufl., 2010, §43 Rn.20.

¹⁴⁹ Peter Gola et al., a.a.O., §43 Rn.21.

ならず、呼び出しが技術的に可能なデータであることが要求される¹⁵⁰。

43条2項3号後段は、自動処理により、または自動化されていないデータファイルから自らデータを入手し、または他者にデータを入手させる行為が規定されている。自己の利益のためではなく、他者のために行われた場合も本号の成立要件が満たされる¹⁵¹。

43条2項4号は、一般的にはアクセスできない個人データの提供を、虚偽の申告によって受ける行為について規定する。本号はハッカーによる情報の入手などにも適用される。ハッキングは形式的には「虚偽の申告」ではなく、有効なパスワードによってデータを入手する行為であるが、パスワードの利用によってデータを騙し取る行為として本号の規制対象となる¹⁵²。前述の通り、43条2項1～4号では、一般的にアクセスできない個人データが対象となる。

43条2項5号は、個人データの提供を受けた者が、提供された目的以外の処理と利用を行うことを対象としている。16条4項に規定されているように、データ提供機関(übermittelnde Stelle)はデータを提供する際に、目的について指示しなければならない。提供目的外のデータ処理・利用が禁止されると同時に、データ処理等の目的は明確に説明される必要があり、再三にわたってデータが伝達されるような場合には目的が明白に区別されなければならない¹⁵³。2009年の法改正以前の43条2項5号では、「第三者に譲渡することを通じて、提供されたデータを他の目的のために利用する」行為が秩序違反になっていたが、法改正によって「第三者に譲渡することを通じて」という文章が削除され、目的外のデータ利用がすべて秩序違反として構成されるようになった。

そして、43条2項5号では、①職業もしくは特別な職業上の秘密に服する個人データ、およびその職業上または職務上の義務を果たす際に、守秘義務のある機関の自由な使用に供された個人データについて、当該個人データを提供された者が、責任機関がデータを得た目的以外で個人データを利用する行為と、②学術研究目的で収集または蓄積された個人データの提供を受けて、学術研究目的以外で利用する行為も秩序違反行為となる。本号の対象となるのは、これらの秘密の保持を義務付けられている者自身ではなく、正当な方法でそのようなデータの提供を受けた者または機関である。したがって、データの提供が行われれば、医師などの特定の職務を行う者、または公職者に科せられた守秘義務とその違反行為は、本号の対象外となる¹⁵⁴。

43条2項5b号は、本人が責任機関に対して、宣伝または市場調査・世論調査の目的によるデータ処理・利用について異議を申し立てているにもかかわらず、これらの目的のためにデータ処理・利用する行為について規定しており、2009年の改正によって新設された条項である。宣伝を行う企業は調査の結果、宣伝目的でのデータの利用や処理を拒否

¹⁵⁰ Peter Gola et al., a.a.O., §43 Rn.22.

¹⁵¹ Peter Gola et al., a.a.O., §43 Rn.22.

¹⁵² Peter Gola et al., a.a.O., §43 Rn.23.

¹⁵³ Peter Gola et al., a.a.O., §43 Rn.24.

¹⁵⁴ Peter Gola et al., a.a.O., §43 Rn.24.

していない者のみについて行われることを証明 (sicherstellen) しなければならない¹⁵⁵。これまでは本人の拒否があった場合について十分に対応することができなかったが、法改正によって処罰の間隙が一部埋められた。監督官庁が宣伝を行う企業による本号の違反について訴追する場合、当該企業は入念な検査と、場合によっては企業の組織的な行為が法に適合することを要請されるものの、本号が新設されたことによって本人の拒否権と、望まない宣伝で「満杯になった郵便ポスト (überfüllten Briefkästen)」によって煩わされない権利が本当に強化されたのか否かは疑問視されている¹⁵⁶。このような問題意識により、宣伝産業における監督官庁の権限強化に向けた再検討が必要であると指摘されている¹⁵⁷。

データ保護法 4 3 条 2 項各号の秩序違反行為は、権限のない者によって所定の行為がなされることによって成立するので、この法律やデータ保護についての他の法律に適合していることが正当化事由となる。

データ保護法違反者に制裁金支払い能力がないことが確実である場合、過料を科すことは無意味なので、行政執行法 (Verwaltungs-Vollstreckungsgesetz, VwVG) 1 6 条に基づく代替強制拘留 (Ersatzzwangshaft) が用いられ得る¹⁵⁸。

また、ドイツの各州において、州のデータ保護法 (Landesdatenschutzgesetze) が施行されている。多くの州のデータ保護法では過料と刑事罰の両方が規定されているが、シュレースヴィヒ＝ホルシュタイン (Schleswig-Holstein) 州データ保護法では過料規定のみが存在する。一方、ベルリン州とラインラント＝プファルツ (Rheinland-Pfalz) 州データ保護法では刑罰規定のみが存在する。

第 2 款 主観的な成立要件

4 3 条 1 項・2 項は、故意と過失の両方を秩序違反の対象としている。故意によってデータ保護法の違反が行われることは極めて稀なことであり、過失による違反が一般的である¹⁵⁹。ドイツ刑法学における過失は、「認識ある過失 (bewusste Fahrlässigkeit)」と「認識なき過失 (unbewusste Fahrlässigkeit)」に分けられる。ドイツ刑法における「未必の故意 (bedingter Vorsatz)」は、発生し得る法益侵害に向けた決定であるのに対して、認識ある過失は、許されない危険創出 (unerlaubter Gefahrschaffung) であるにもかかわらず、行為者が結果の不発生を信じる場合であり、この 2 つは明確に区別される¹⁶⁰。一方、「認識

¹⁵⁵Coriana Holländer, Datensündern auf der Spur – Bußgeldverfahren ungeliebtes Instrument der Datenschutzaufsichtsbehörden?, RDV 2009, S.219.

¹⁵⁶Holländer, a.a.O., S. 219.

¹⁵⁷ Holländer, a.a.O., S.219.

¹⁵⁸ Holländer, a.a.O., S.222.

¹⁵⁹ Peter Gola et la, a.a.O., §43Rn.27.

¹⁶⁰Claus Roxin, Strafrecht Allgemeiner Teil, Band I Grundlagen · Der Aufbau der Verbrechenslehre 4.Aufl, C.H.Beck, 2006, S.1087. 山中敬一 (監訳) 『ロクシン刑法総論第 1 卷[基礎・犯罪論の構造]【第 4 版】【翻訳第 2 分冊】』(信山社・2009 年) 625 頁以降参照。

なき過失」は、一定の作為または不作為において、必要な注意をせず、その結果として法的な構成要件の結果を認識せずに発生させることをいう¹⁶¹。

認識ある過失と認識なき過失は理論上区別されているものの、ある行為が認識ある過失による行為であると同時に、認識なき過失による行為でもあり得ることが指摘されている¹⁶²。論者によると、ある者が結果発生の蓋然性を10%であると見積もって、結果の不発生を信じたものの、実際には結果発生は25%であったという場合に、行為者はすでに認識ある過失で行為している。同時に、より高度の危険性が認識可能だったということで認識なき過失も存在する¹⁶³。論者は、認識の有無によって法的効果が左右されないということにより、認識ある過失と認識なき過失を区別する意義が乏しい旨を指摘する¹⁶⁴が、実際の事例においても両者を截然と区別することは容易ではないだろう。

前述の通り、データ保護法43条1・2項における「過失」には、認識ある過失と認識なき過失の両方が含まれる。したがって、自己に権限のないことを認識せず、一般的には自由に利用できない個人データを収集する行為などの、単純な不注意による行為も広く過料の対象となり得る。

第2項 刑罰

データ保護法44条は、前項で扱った43条2項所定の秩序違反行為を、対価を得て、または自己もしくは他人の利益を図るために、または他人を害することを意図して行った場合には、自由刑または罰金刑が科せられることを規定する。

44条は刑罰規定であり、一般的にはアクセスできない個人データが保護法益となる。この規定の客観的構成要件は、対価を得ること、または自己利益を図ること、もしくは他害を図ることである。ここでいう「対価」とは、ドイツ刑法典(StGB)11条1項9号が規定する「財産的利益に存するすべての反対給付(jede in einem Vermögensvorteil bestehende Gegenleistung)」のことである¹⁶⁵。「反対給付」の概念は、何らかの相応する取り決め(entsprechende Vereinbarung)の存在を前提としており、その取り決めによって自己の利益を図ったり、現実に利益を得たりすることは要求されない¹⁶⁶。データ保護法の下では故意による行為のみが刑罰の対象となることは、条文の文言より明らかである。

ドイツの各州にも州データ保護法が存在するのは前述の通りである。刑罰法規の有無や内容は州ごとに異なっており、バーデン-ヴュルテンブルク州、ブランデンブルク州、ブレーメン州等のデータ保護法では未遂(Versuch)も刑事罰の対象となる。

¹⁶¹Johannes Wessels / Werner Beulke, Strafrecht Allgemeiner Teil, 42., überarb. Aufl, C.F. Müller, 2012, S.262.

¹⁶²Roxin, a.a.O., S.1089

¹⁶³ Roxin, a.a.O., S.1089.

¹⁶⁴ Roxin, a.a.O., S.1087, Wessels et al., a.a.O., S.262 も、認識ある過失と認識なき過失の区別は、量刑判断のみに必要となることを述べている。

¹⁶⁵Peter Gola et al., a.a.O., §44 Rn.5.

¹⁶⁶ Peter Gola et al., a.a.O., §44 Rn.5.

現行法の前身である1990年連邦データ保護法43条にも罰則規定があり、そこではデータ保護法によって保護され、周知のもの（*offenkundig*）となっていない個人データを無権限で蓄積、提供する行為等が処罰の対象となっていた。そして、現行法では「周知のものとなっていない」という文言から、「一般的にはアクセスできない」という文言に変更され、1990年法では過料ではなく刑罰の対象となっていたデータの無権限の呼び出しや入手などの行為が、現行法では過料の対象へと変更されている。旧法に比して、現行法では刑罰の対象となる行為が制限される。そして、現行法への法改正に伴い、データの内容が広く知られているか否かにかかわらず、アクセスにつき制限のない個人データはデータ保護法による保護の対象外とされるようになった。

1990年データ保護法において規定されていた、データが「周知のものである」という文言には、「一定数の人々に知られているか、または他の情報なしに（*ohne weiteres*）知覚可能であり、人々の間で確定的に保持されていること」という定義があるものの、インターネットや電子工学的なデータ転送によるデータの提供には地域的・時間的・量的な限界がないので、今日ではすべてのデータは「周知のもの」となり得る¹⁶⁷。また、データが「周知のもの」であるか否かは、データ処理の目的、性質、地域的・人的・時間的状況によって左右され得るという指摘もされている¹⁶⁸。

このように、データの「周知性」という概念は曖昧で、インターネット等によって情報の伝達が容易に行われる現代ではその実効性を失っているので、2001年データ保護法への改正において、保護客体が「一般的にはアクセスできない」データに変更されたことには意義がある。しかし、本来であれば一般人の自由なアクセスに供するべきではない性質の個人データであるにもかかわらず、データの責任機関等の安全措置に問題があつて、不当にも自由なアクセスができる状況になってしまっているような場合には、現行法の43条2項の条文で十分に対応できるかどうかは疑問である。安全措置の甘さが「一般的にはアクセスできない」という構成要件該当性を阻却してしまう不当な結果になることは回避すべきであろう。

第3節 監督官庁による規制の実態

前述の通り、ドイツ連邦データ保護法の枠組において、連邦データ保護観察官には他の公的機関の違反に対して過料や刑罰を科す権限がない一方、監督官庁には民間機関の命令違反やその他のデータ保護法違反に対して過料を科す権限と、犯罪について訴追をする権限が認められている。

第1項 監督官庁の位置づけ

連邦データ保護法38条に規定されている各州の「監督官庁」には、州のデータ保護観

¹⁶⁷ Thilo Weichert, Datenschutzstrafrecht-ein zahnlöser Tiger?, NStZ 1990, S.491.

¹⁶⁸ Weichert, a.a.O., S.491.

察官 (Landesdatenschutzbeauftragter) とデータ保護のための独立委員会 (Unabhängiges Datenschutzzentrum) の 2 種類がある。ドイツの 16 州のうち、ザールラント (Saarland) 州とシュレースヴィヒ=ホルシュタイン (Schleswig-Holstein) 州が独立委員会を有しており、委員会には情報の専門家である州のデータ保護観察官が存在する。

監督官庁は民間機関を管轄するとされているが、州によっては一つの監督官庁が民間機関と公的機関の両方を管轄している例もある。ベルリン州のデータ保護観察官は、元来民間機関のみを対象としていたものの、完全に独立した監督機関が民間機関と公的機関の両方を監督することを求める 1995 年 EU データ指令 28 条を受け入れる形で、両方の領域を監督するようになった。ノルトライン=ヴェストファーレン州等のデータ保護観察官と、シュレースヴィヒ=ホルシュタイン州の独立委員会も、両方の領域を監督の対象としている。

EU データ指令 28 条では、監督機関が完全な独立性を有することが求められ、ドイツ連邦憲法裁判所も、情報自己決定権の有効な保護のためには独立したデータ保護観察官の存在が必要であることを強調している¹⁶⁹。現在のドイツでは、全ての州の監督官庁が独立の地位をもって監督にあたっている。そこで、本節ではドイツの 16 州の中で、情報保護のための特別な委員会を有しているシュレースヴィヒ=ホルシュタイン州とザールラント州を取り上げて、第三者機関による取り締まりの現況を明らかにする。

第 2 項 監督官庁による過料・刑罰

第 1 款 シュレースヴィヒ=ホルシュタイン州

個人情報保護のためのシュレースヴィヒ=ホルシュタイン州独立センター (Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein. 以下、ULD) の業務は、州におけるデータ保護法違反に対する異議に基づく瑕疵の除去要求と、データ保護の問題について企業や州の市民に助言をすること、毎年の活動報告 (Tätigkeitsberichte) を行うこと等である。州における民間機関と公的機関の両方を監督する。

シュレースヴィヒ=ホルシュタイン州のデータ保護法では、44 条に以下のような過料規定がある。刑罰規定は設けられていない。

44 条 1 項 秩序違反は、この法律に違反して、周知のものとなっていない個人データを

- 1 収集、貯蔵、目的外の処理、変更、伝達、呼び出すための準備、消去した場合と、
- 2 呼び出し、閲覧、入手、または誤った事実による欺罔行為 (Vortäuschung) を通して、自己または他人に伝達させる行為について成立する。

44 条 2 項 秩序違反は、以下の場合にも成立する。

¹⁶⁹BVerfGE65,1,46;67,157,185.

1 匿名化された、または偽名化されたデータを他の情報と共に照合し、それによって一人または複数の本人を特定する場合

2 この法律に違反して、偽名化されたデータについて、与えられた権限を超えてアクセスを入手した場合、または

3 この法律の5条1項による技術的・組織的な措置を採ることを完全に (vollständig) 怠った場合

3項 秩序違反には5 0 0 0 0ユーロ以下の過料が科され得る。

そして、技術的・組織的な措置について規定した5条1項の内容は以下の通りである。

この法律の規定、またはデータ保護に関する他の規定の実行 (Ausführung) は、技術とデータ保護の必要性の観点から、必要で妥当な技術的・組織的措置を通して行われなければならない。

以下のことを保証しなければならない。

1. 手続 (Verfahren) とデータが時宜に適って自由使用に任され得る状態であり、合法的に使用され得ること (自由裁量)

2. データが破損しておらず、完全であり、分類可能であり (zurechenbar)、最新のものであること (完全性)

3. 認められた方法のみによってデータが呼び出され得ること (機密性)

4. 期待可能な出費 (Aufwand) による個人データの処理が、後付けられ (nachvollziehen)、調査され、評価され得ること (透明性)

5. 個人データが、決められた目的以外の目的のために収集され、処理され、利用され得ないこと、必要以上の出費を伴う (mit unverhältnismäßig hohem Aufwand) 場合に限りて収集、処理、利用を可能とすること (不可連鎖性 Nicht-Verkettbarkeit)、そして

6. 26条から30条までの条文で認められた本人の権利行使を有効なものにするような (情報処理の) 方法であること (異議の可能性)

26条から30条には、自己のデータを処理される目的などの告知を受ける権利、データ処理への拒否権等が規定されている。

このように、シュレースヴィヒ=ホルシュタイン州のデータ保護法では、技術的・組織的措置を採ることを怠る行為を秩序違反の対象としている。このような秩序違反規定は、シュレースヴィヒ=ホルシュタイン州と同様に独立のデータ保護委員会を有するザールラント州データ保護法にも、連邦データ保護法にも存在しない特徴的なものである。連邦データ保護法9条では必要な技術的・組織的措置を採ることを義務付けた上で、38条5項において、技術的・組織的な瑕疵の除去のための措置を命ずる権限を監督官庁に認めている。この命令に違反した場合に初めて過料の対象となり得るという構成を採っている一方で、シュレースヴィヒ=ホルシュタイン州データ保護法が「命令違反」を仲介せず、必要な技術

的・組織的措置を講じないという段階で秩序違反を構成するという点は注目に値する。個人データの目的外使用や不適切な処理などの様々な違反行為が「措置の懈怠」として扱われ、直ちに過料の対象となり得るからである。

以上の条文を前提として、本款では、ULD が発表する活動報告書から、過料に関する実務について探ることとする。

2011年3月に出された報告書では、過料の事例が次のように紹介されている。ULD の過料に対する姿勢を理解する必要上、若干長くなるが引用する。

「銀行の以前の顧客が、宣伝目的によるデータの利用について異議を唱えたにもかかわらず、当該銀行からの再三にわたる宣伝を受け取った。我々（ULD）は、過料を科さなければならなかった。

連邦データ保護法によると、何人も責任機関に対して、宣伝または市場調査・世論調査目的による自己のデータを利用または転送について異議を唱える権利を有する。前述のケースのような、宣伝目的によるデータの利用に対しても異議を唱えることが認められる。問題となった銀行の対応（**Reaktion**）は、我々に対して懸念を抱かせた。それというのも、銀行は企業の組織の内部における重大な瑕疵について認識していながら放置していたからである。当該データについての異議が完全に遵守されるか、または遵守され得るという技術的・組織的な保障もなされていなかった。このことは、本人の異議が無視されるという結果につながった。過料決定は法律上の効力のある（**rechtskräftig**）ものである」¹⁷⁰。

この事例報告からは、当該銀行には瑕疵の認識があり、違反について故意は認められなくとも、違反結果についての認識ある過失はあったであろうということがわかる。銀行による宣伝が一度ではなく再三にわたって送られたという事情も、違反の悪質性を基礎づけるだろう。このことから、ULD は結果の重大性や瑕疵の治癒の見込みなどを考慮して、悪質なケースに限定して過料決定を下しているのではないだろうか。なお、前述の通り、シュレースヴィヒ＝ホルシュタイン州のデータ保護法では刑罰規定が設けられていない。

次に、2007年3月に出された報告書では、1件の過料の事例が挙げられている。保険会社の従業員が、雇用主のレターヘッド（**Briefkopf**）を用いて、自動車の許認可の所轄官庁（**Kfz-Zulassungsstelle**）に申し立てた上で、車両所有者に試問を行った。実際には当該車両による被害について何らの届出もなされていなかったにもかかわらず、当該従業員は試問で得られる情報を全くの私的な目的で使用するために、正当な権限なく試問を行ったのである。当該従業員によるこの行為は、車両所有者についての一般的にはアクセスできない情報を故意に不正取得するという秩序違反に該当し、ULD は従業員に過料を科した¹⁷¹。報告書の記載の通り、従業員の行為は故意による不正な情報収集であり、過料決定が

¹⁷⁰ 33. Tätigkeitsbericht des ULD, S.94.

URL: <https://www.datenschutzzentrum.de/material/tb/tb33/uld-33-taetigkeitsbericht-2011.pdf>.

¹⁷¹ 29. Tätigkeitsbericht des ULD, S.90.

<https://www.datenschutzzentrum.de/material/tb/tb29/tb29.pdf>.

下されるにあたり、故意行為であることと、私的な目的のために虚偽の試問によって情報を収集したという行為の悪質性が考慮されたのではないかと思われる。

続いて、2006年3月の報告書では、「過料—それは時には不可避である」というサブタイトルが付された記述がある。本報告は、ULD による過料実務を次のように要約する。「通常、企業は ULD がデータ保護の改善のために行う要求・指示・助言には大いに譲歩し、理解を示している。しかし、違反が再三行われた場合、特に故意による重大な法律違反の場合は、個々の過料手続が必要となる」¹⁷²。

続いて、本報告書は過料の事例について以下のように詳述する¹⁷³。

「データ保護監督官庁の事情調査のためには、法律で明確に定められた情報提供 (Auskunftserteilung) 義務は無視できるものではない… (中略) …企業が我々 (ULD) の調査における照会 (Aufragen) に応じることなく、それが再三にわたる場合、ULD は過料を下さなければならない。… (中略) …複数の市民から同様の申請 (eingaben) がなされることは、過料手続が導入される根拠となる。市民たちは、ある利益団体 (Gewinnspiel) に加入するための通知を受け取った。実際には、通知を受け取った彼らのうちの誰もその団体に参加せず、企業からも告知がなかった。にもかかわらず、彼らの生年月日、口座番号、電話番号が一部、企業に提供されていた。データ管理者は、支払い不能の (insolvent) 企業から 50 万人のデータが、本人の承諾なしに、既に何年も前に提供されていたことを認めた。その間に、この企業はすべての商業活動を中止したことを通知した。したがって、一般的にアクセスできない個人データの故意による処理についての疑いは晴れていない (nicht vom Tisch)」。

このような報告書の記載からは、複数の者の個人データが違法に、そして故意によって処理された以上のケースについて、実際に過料決定が下されたのか否かということは定かではない。しかし、被害が広範であれば過料決定が選択される余地があるということを表しているだろう。

また、再三の異議 (Beanstandung) があつたにもかかわらず、明らかに分別のない家主が公道で権限なくビデオ監視を行った事例につき、ULD が過料決定を下したところ、この過料決定についての異議が区裁判所に申し立てられたことも報告されている¹⁷⁴。

以上、シュレースヴィヒ=ホルシュタイン州のデータ保護委員会によって報告された事例を通して、過料の実務の実態について検討してきた。これらの事例からは、データ保護法の違反があり、それが州のデータ保護法の過料規定に合致するとしても、直ちに過料決定が下されることはなく、実際には特に悪質なケースに限って過料が下されるということがわかる。そして、2006年の報告書にも記載されているように、州のデータ保護法の監督下にある企業等の機関は、ULD の監督や規制に対して協力的である場合が一般的であり、

¹⁷² 28. Tätigkeitsbericht des ULD, S.83.

<https://www.datenschutzzentrum.de/material/tb/tb28/tb28.pdf>.

¹⁷³ 28. Tätigkeitsbericht des ULD, a,a,O, S.83.

¹⁷⁴ 28. Tätigkeitsbericht des ULD, a,a,O, S.83.

このことも過料の事例が少ない原因の一つとなっている。このことから、第三者機関である ULD の監督は、データ保護法の違反に対する抑止力としての機能を一定程度は果たしていると考えられる。

第2款 ザールラント州

個人情報保護のためのザールラント州独立センター（Unabhängiges Datenschutzzentrum Saarland. 以下、UDS）は、ザールラント州の公的機関と民間機関の両方を監督する。シュレースヴィヒ=ホルシュタイン州とは異なり、ザールラント州データ保護法（Saarländisches Datenschutzgesetz）には過料規定と刑罰規定の両方が存在する。まず、過料規定は以下の通りである。

36条1項 秩序違反は、この法律によって保護される周知のものとなっていない個人データに対する以下の行為に対して成立する。

1. 収集、蓄積、改変、転送、閲覧または呼び出しのための準備、消去または利用
2. 呼び出し、閲覧、入手、または誤った事実の欺罔行為（Vortäuschung falscher Tatsachen）によって、自己または他人に転送させる行為

36条2項 秩序違反には、50000ユーロ以下の過料が科され得る。

続いて、刑罰規定は以下の通りである。

35条1項 この法律によって保護されている一般的にアクセスできない個人データについて、対価を得て、または自己もしくは他人の利益を図るために、または他人を害することを意図して、

1. 収集、蓄積、改変、転送、閲覧または呼び出しのための準備、消去または利用
2. 呼び出し、閲覧、入手、または誤った事実の欺罔行為（Vortäuschung falscher Tatsachen）によって、自己または他人に転送させる行為

に出た者には、2年以下の自由刑または罰金刑が科される。

これらの行為の未遂（Versuch）も可罰的である。

35条2項 当該行為が他の刑罰規定に触れない限りにおいて、1項の規定が適用される。

このように、ザールラント州データ保護法では、シュレースヴィヒ=ホルシュタイン州とは異なり、技術的・組織的措置の懈怠は過料・刑罰の対象とはなっておらず、個人データの収集や利用等の行為が客観的要件となっている。以上の条文を前提として、本款では、ULS が発表する活動報告書から、過料と刑罰に関する実務について検討する。なお、ULS では2年間で1つの報告書が提出されており、2009年・2010年までは公的機関と民間機関で別個の報告書が作成されているが、2011年・2012年からは報告書が一本化されている。

ULD のみならず ULS の報告書においても、データ保護法違反について過料や刑罰が科された事例は希少である。この傾向は、公的機関も民間機関も同様である。

公的機関についての 2009 年・2010 年の報告書では、ザールラント州の中央過料官庁（Zentrale Bußgeldbehörde）が行った、交通秩序違反行為に関する聴聞（Anhörungsbogen）における不適切なデータ収集について ULS が対応した次の事例が紹介されている¹⁷⁵。

ULS は、当該聴聞をデータ保護法に基づいて調査することについて請願を受けた。この聴聞において、請願者は、自己について聞かれた質問にはいかなる場合も完全かつ正確に応答する義務がある旨と、この義務の違反は、秩序違反法（Ordnungswidrigkeitengesetz）111 条に違反し、過料の対象となる旨を指示された。更に、この者の氏名の他に、住所、生年月日、出生地および電話番号が尋ねられた。

請願者には、自己にかけられた秩序違反の嫌疑について弁明する機会が与えられた。請願者には原則的に陳述義務はないものの、当然のこととして、全てのケースにおいて、人物の同一性確認のために必要な質問には応答しなければならなかった。秩序違反法 111 条は、応答義務を規定し、応答の拒否に対して過料を予定しているものの、電話番号という事項は応答義務の対象とはなっていない。秩序違反法 111 条では、担当官庁等に対して氏名、出生地または生年月日、配偶関係、職業、住所、国籍について不正確な応答をしたり、応答を拒否したりする行為が過料の対象となるに留まる。それにもかかわらず、聴聞では請願者の電話番号も尋ねられ、請願者はこれに応答した。

ULS は、当該電話番号のデータの収集について、ただちに聴聞の形態を変更して、本人の自発的な意思に沿うように要請している。

この事例は公的機関による不適切なデータ収集について ULS が規制を行ったものである。秩序違反法の文言に従えば、応答する必要のない電話番号を尋ねる行為は、周知のものとなっていない個人データを収集する行為にあたり、ザールラント州データ保護法 36 条 1 項および連邦データ保護法 43 条 2 項 1 号所定の秩序違反に該当し得る。しかし、上記の報告書には、ULS がこの聴聞について過料決定を下したという記述はなく、請願を受けた上での事実調査と要請に留まっている。聴聞において、本来であれば尋ねることのできない電話番号について尋ねるという行為が故意によって行われたものであるとは限らず、法律で規定された範囲を超えて尋ねたデータが電話番号のみであること、他の個人データと異なり、電話番号は自己によって変更可能であることから、ULS が軽微な法律違反であると判断したのではないだろうか。

続いて、非公的機関についての 2003 年・2004 年の報告書には、次のような過料の事例がある¹⁷⁶。

¹⁷⁵ Datenschutz im öffentlichen Bereich 23. Tätigkeitsbericht 2009/2010
<http://www.lfdi.saarland.de/images/stories/pdf/Berichte/tb23.pdf>.

¹⁷⁶ Tätigkeitsberichte der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen

ある銀行の従業員は、どの範囲で個人データを貸主 (Vermieter) に提供してもよいのかという本人の意思決定 (Entscheidung) を待つことなく、借主である複数の当事者のデータを Schufa に照会したところ、Schufa は私人に対していかなる情報も提供しないので、たとえ銀行員が相手であっても個人データの提供を受けることはできなかった。

Schufa の正式名称は、"Schutzgemeinschaft fuer allgemeine Kreditsicherung (貸主保護団体)" であり、ドイツ在住者と企業の経済力や信用について査定を行い、この査定結果である Schufa-Auskunft を家主や銀行などの貸し主に販売する事で利益を得る団体である。

そこで銀行員は、借主である当事者自身を促して、Schufa への照会をさせることによって当事者の個人データを得た。銀行員は、当事者本人がこの手続に同意しており、Schufa への照会が合法であると主張していた。しかし、当事者本人に Schufa-Auskunft について告知せずに照会を行わせたということから、本人の同意は法律上有効なものではないとされた。

本人の有効な同意を得ずに Schufa にデータ照会をさせてそのデータを得るという銀行員の行為は、連邦データ保護法 4 3 条 2 項 4 号における不正な申告による個人データの受け取りという客観的要件を満たしているとして、当該銀行の従業員には過料決定が下された¹⁷⁷。

この事件では、被害者は複数である。さらに、銀行員の行為は "Täuschungshandlung (詐欺的行為)" であると表現されていることから、銀行員が故意により、そして当事者本人を欺罔するような形でデータを収集したということに過料決定の根拠があると考えられる。

第3款 過料・刑罰に対する監督官庁の姿勢

第1款と第2款では、個人データ保護のための特別な委員会を有しているシュレースヴィヒ=ホルシュタイン州とザールラント州の実務について検討した。これら2つの州では、データ保護法の違反に対して過料・刑罰が科される例は稀であったが、この傾向はドイツ全土にもいえることである。データ保護法の違反につき、2008年に州の監督官庁が初めて高額の過料を科した代表的なケースが2つある。その一つは、ビデオ監視を行った Tönnies という食肉加工企業に対して80000ユーロの過料が科されたというものである。ノルトライン=ヴェストファーレン州のデータ保護観察官は、企業に対して過料を科した。問題となった企業は、社内の更衣用個室や食堂など、合計200以上のカメラを設置して従業員を監視していた。衛生上の必要から、食肉生産室にはカメラを設置することが認められていたものの、それ以外の場所に対するカメラ設置がデータ保護法違反として問題となったのである。Tönnies 社は州データ保護観察官による過料決定を受け入れ、食肉生

Datenschutz des Saarlandes 2. Tätigkeitsbericht 2003/04

http://www.lfdi.saarland.de/images/stories/pdf/Berichte/tbnoe_2.pdf, S.47~48.

¹⁷⁷ 2. Tätigkeitsbericht 2003/04, a, a, O, S.48.

産室以外のカメラを撤去した¹⁷⁸。

もう一つは、食料品のディスカウントショップチェーンの Lidl が盗撮によって従業員を監視していたことにつき、バーデン=ヴュルテンブルク州のデータ保護監督官庁が 1 5 0 万ユーロの過料を科したことである。Lidl が管理していた 3 5 の販売会社が調査の対象となり、ドイツの複数の州の監督官庁が携わったが、Lidl の本拠地がネッカーズルムであることから、バーデン=ヴュルテンブルク州が所管することとなった。Lidl 社は 2 1 9 の支店にカメラを設置しており、複数の労働組合員が企業による広範囲な監視について明らかにした後、Lidl 社は監督官庁による過料決定を受諾している¹⁷⁹。

この 2 つの事例では企業に高額な過料が科されているが、これまでの監督官庁の業務の中で、過料を科すことはあまり行われていなかった。2 0 0 5 年 9 月から 2 0 0 6 年 8 月までの間、ドイツ共和国全体で下された過料決定は 4 4 件であり、2 0 0 8 年にベルリン州のデータ保護観察官が下した過料決定は 3 件である¹⁸⁰。

データ保護法における秩序違反の訴迫につき、監督官庁がこれまで制限的であったのはなぜかということが問題となる。違反の数は毎年増加傾向にあるので、データ保護法が完全に遵守されているから過料決定の数が少ないと解することはできず、監督官庁の人員が定員を満たしていないことが、過料手続が実行される件数の少ない理由の一つであるとする見解がある¹⁸¹。データ保護法の秩序違反を訴迫するには、人的資源が求められるからである。過料を科すのは最後の手段 (ultimatio-Mittel) とされており、データ保護法 3 8 条 5 項による監督官庁の権限に基づいて、データ保護法違反が取り除かれた可能性が見いだせない場合、監督官庁は過料を科すことが可能である。しかし、監督官庁の人員が不足していること、不十分な管理権限、そして企業に対して過料を科すことに慎重な態度により、個人データが危険に晒され得ることが指摘されている¹⁸²。

監督官庁による実務の実態に加えて、2 0 0 9 年のデータ保護法改正後も依然として処罰の間隙がある¹⁸³。第 1 節で述べた通り、データ保護法 9 条は、個人データを収集・処理・利用する公的・民間機関に対して、データ保護のために必要な技術的かつ組織的な措置を講ずる義務を定めている。しかし、2 0 0 9 年の法改正後も、企業等の機関がこの義務に違反する行為は処罰の対象となっていない。過料の対象となる行為が法律で定められていることは、一般予防と特別予防の両方の効果を有する¹⁸⁴。しかし、秩序違反法における起

¹⁷⁸ Focus-Online v.15.09.2008;

http://www.focus.de/politik/deutschland/datenschutz-toennies-muss-wegen-videoueberwachung-bussgeld-zahlen-aid_333478.html.

¹⁷⁹ Welt-Online vom 11.09.2008;

<http://www.welt.de/wirtschaft/article2428529/Spitzelaffaere-kostet-Lidl-1-5-Millionen-Euro.html>.

¹⁸⁰ Holländer, a,a,O,S.215.

¹⁸¹ Holländer, a,a,O,S.215.

¹⁸² Holländer, a,a,O,S.215.

¹⁸³ Holländer, a,a,O,S.221.

¹⁸⁴ Holländer, a,a,O,S.222.

訴便宜主義（Opportunitätsprinzip）に依拠すれば、すべての違反に対して過料が科されることはなく、過料規定の予防効果の程度は、監督官庁が違反を訴追するか否か、そしてどの程度訴追の対象とするのかということに依存するので、監督官庁は過料を科すことを回避するのではなく、過料を法益保護の手段とみなすべきであることが指摘されている¹⁸⁵。

ドイツではデータ保護法違反に対して過料が科されるケースが少なく、刑罰規定は過料規定よりも対象となる行為が限定されているので、刑罰が科されるケースは更に希少なのが現状である。実際に過料や刑罰が下されることが少ない根拠として、人員が不十分であることを指摘する前述の見解があり、監督業務におけるそのような困難さは否定できないだろう。それに加えて、監督官庁が過料・刑罰を科すことに慎重な態度を採っていることも確かである。過料が科されるのはデータ保護法違反による被害が広範囲であったり、再三の異議を無視したりといった悪質なケースが多く、刑罰はその対象とする範囲の狭さも手伝って、刑罰が科された事例はほとんど見られない。その一方で、前述の報告書にも記載されていたように、多くの企業は監督官庁の指導・助言に対して受容的であり、監督業務に対しても協力的である。全体的な傾向として、監督官庁の指示等に従わない悪質なケースが過料の対象となっていることに鑑みれば、過料や刑罰の規定が存在することと、監督官庁による監督業務の2つが協同することが、データ保護法違反についての一定程度の抑止力になっていると考えられる。

第4節 小括

本章では、ドイツのデータ保護法におけるデータの不正な取り扱いに対する過料と刑罰の成立要件および、データ保護のための第三者機関である監督官庁等による実務の実態について検討してきた。

ドイツのデータ保護法制において、情報の不正な取り扱いに対する抑止力となり得るのは、監督官庁による監督業務と、違反に対する過料・刑罰規定である。ドイツ連邦データ保護法と州のデータ保護法では、単純な手続違反と共に個人データの不正収集・提供などの行為に対して過料が予定されており、刑罰の適用される範囲は図利または加害目的等によってデータの不正収集等を行った場合に限定される。

いわゆる情報窃盗や第三者提供などの、日本においても頻発している行為態様は連邦データ保護法43条2項各号によって規定されており、イギリス1998年データ保護法55条と、フランス刑法における諸規定（刑法226-22条を除く）とは異なり、故意のみならず過失による行為も対象となっている。ドイツ刑法学では、過失は「認識ある過失」と「認識なき過失」の両方を含むので、単純な不注意による情報漏洩も過料の対象としてカバーされる。そのような過失による情報漏洩や第三者提供によっても甚大な被害の発生する場合があることから、過失行為も対象とすることには意義がある。

ドイツでは、民間機関による情報処理に対する規制が各州に任されており、各州のデー

¹⁸⁵ Holländer, a,a,O,S.222.

タ保護法の中には、過料規定が存在せず刑罰規定のみが設けられている州や、未遂も刑罰の対象となっている州がある。ドイツは連邦国家であるので、州によって過料規定や刑罰規定に差異があることにも一定の合理性があるだろう。しかし、そのような社会実体のない日本では、刑罰や過料の規定を含んだ個人情報保護法制は統一的なものであるべきだろう。また、EU データ指令を受けて、一般的な個人データとは区別された「特別な種類の個人データ」という概念を導入している点は、イギリスデータ保護法とフランス 1978 年法と共通している。「特別な種類の個人データ」には、人種的出自・宗教的信条・健康状態などといった情報が含まれる。ドイツ連邦データ保護法においても、イギリス・フランスと同様に「特別な種類の個人データ」の取り扱いのための個別の条件を設けており、一般的な個人データのそれに比して条件が多く、内容も具体的なものになっている。しかし、一般的な個人データとは区別されるものとして規定されているにもかかわらず、特別な種類の個人データを不正取得する等の行為について個別の過料・刑罰規定が設けられていないという点についてはイギリスデータ保護法と同様である。イギリスと同様、ドイツ連邦データ保護法も「センシティブな個人データ」という概念を EU 指令からそのまま導入しており、個別の規定を設ける必要性までは検討していなかったのではないだろうか。データの取り扱いの段階で厳密な条件を設けるという事前規制によって十分な保護が図られると解したものと思われる。

第3節で述べたとおり、ドイツにおいては過料・刑罰の科される事例が希少である。その根拠について、監督官庁の人員が不十分であることによって監督業務が満足に行われていないとする指摘もあるが、多くの企業が監督官庁の実務に対して協力的であるという州の監督官庁の報告もなされている。特に企業にとっては、過料や刑罰を科されることは社会からの信用を損なうことにつながりかねないので、監督官庁による指導・助言に従う場合が多いのだと思われる。その結果、過料が科されるのは、データ保護法違反による被害が広範囲であったり、再三の違反が行われたりするような悪質なケースに限られている。刑罰にいたっては、ほとんど実例を見ない。

このように、過料・刑罰が科される事例が希少であるということになれば、過料・刑罰規定の存在意義と、将来的に刑罰規定を創設することについて疑問が呈される余地もあるだろう。しかし、過料・刑罰規定の存在には一般予防・特別予防の効果が認められるはずである。ドイツにおいても、イギリス・フランスと同様に、独立の第三者機関による取り締まりと監督に加えて、情報窃盗などの行為を直接的に処罰する規定の存在することにより、悪質な違反行為が一定程度抑制されているといえるのではないだろうか。過料・刑罰の濫用の危険については、ドイツ各州の監督官庁が慎重に過料・刑罰の実務を行うことによる予防が効果的に行われている。また、企業等は社会的信用を損なうことを危惧して、過料・刑罰の対象となり得る行為を控えることが考えられるが、一般人は必ずしもそうではないと考えられる。やはり、情報窃盗や無権限による第三者提供などの行為を予防するためには刑罰規定が必要とされる場合もあるだろう。

第6章 保護法益としての個人情報と規制方法

第3章から第5章まで、イギリス・フランス・ドイツの個人情報保護法制と、第三者機関による情報処理の取り締まりと監督実務について分析してきた。そこで本章では、ここまでの章で得られた知見に基づき、日本の個人情報保護法制における刑罰の可能性と限界について考察する。第1節では個人情報が刑法における保護法益たり得るのかということを検討し、第2節以降では個人情報保護の妥当な方法について検討する。

第1節 個人情報の法益性

第1項 現行法における他の保護法益への不可包含性

現代社会において、個人情報が一定以上の重要性を有することについては争いがないものと思われるが、個人情報という利益は現行の刑法典で保護されている他の法益の中に包含することはできないのだろうか。

まず、個人の信用情報や健康状態などといった、当該個人の社会的評価が低下し得る事実を摘示すれば刑法230条の名誉毀損罪が成立するので、個人情報という利益を独自の法益と解さなくとも、「名誉」という保護法益に包含すればよいと解することは妥当だろうか。確かに、個人情報の性質によっては当該個人の社会的評価が低下することは十分考えられるものの、個人情報には氏名、年齢、住所、生年月日といった、当該個人の同一性に関する基本的な性質のものも多く含まれる。このような基本的な情報は、それが第三者に漏らされたり売買の対象となったりすることによって、当該個人の生活に不利益がもたらされるが、必ずしも社会的評価の低下につながるとはいえない。したがって、個人情報という利益を「名誉」という従来の保護法益に包含することは不可能である。

次に、本論文第2章第1節では、秘密漏示罪が、一定程度の個人情報を個人的法益として保護する機能を有していることを述べた。刑法134条以外にも、特定の職業に就いている者に守秘義務を科し、それに違反して秘密を漏らす行為を処罰する規定は数多くあるので、秘密という枠組において、個人情報は幅広く保護されているように見える。しかし、刑事事件を起こした少年の精神鑑定につき、精神科医から少年についての秘密資料を得たジャーナリストが処罰されなかったケースのように、守秘義務者から秘密を漏示された非守秘義務者がその秘密を漏示した場合をカバーできないという問題があることは、第2章第1節で述べた通りである。このように、現行の秘密漏示罪には処罰の間隙があるが、個人情報という利益を独立の保護法益とはせず、現行の秘密漏示罪を主体の制限なく「正当な理由なく秘密を漏示する」行為を処罰するという規定に変更すれば足りるといえるのだろうか。そもそも、秘密漏示罪において、医師や弁護士などの特定の職業に就いている者に行為主体が限定されているのは、これらの者は職務によって患者や依頼人などの個人の利益を図るために当該個人の秘密を知る必要があり、職務を通して得た秘密の管理には特別の責任を有するからである。秘密漏示罪の保護法益に「当該職務への信頼」を含めるか否かは別問題としても、秘密漏示罪が保護対象とする秘密は単なる秘密ではなく、特定

の職業に就いている者または就いていた者の特別な守秘義務を前提とするものであるので、非守秘義務者による秘密漏示行為による被害が甚大であったとしても、秘密漏示罪の行為主体に対する限定を外すことはできない。そのように解すれば、秘密漏示罪における「秘密」という保護法益の中に個人情報という利益を包含することは、秘密漏示罪の性質上不可能である。

このように、現行刑法における名誉毀損罪と秘密漏示罪は個人情報を一定程度保護しているように見えるものの、各々の犯罪規定の趣旨に鑑みれば、「名誉」または「秘密」という保護法益の中に個人情報を含めることはできないということがわかる。さらに、第1章第1節で述べた通り、窃盗罪や横領罪といった財産犯の解釈によって、有体物に化体されていない個人情報そのものを保護するという理論構成を採ることも困難である。財物には移転可能性がある一方で、情報は誰かに知られたり利用されたりしても当初の保有者の手元から失われるわけではないので、情報に特有の「非移転性」「非喪失性」は情報の法益としての特殊性を示すとともに、情報を財産罪によって保護することの限界を意味している¹⁸⁶。以上のことから、個人情報という利益は特殊性・独立性を有するものとして位置づけることが可能である。

第2項 憲法上の価値から導出される保護法益としての個人情報

前項では、個人情報という利益が従来の法益に包含できない独自のものであることを明らかにした。続いて本項では、個人情報の重要性と他の法益への不可包含性により、個人情報を刑法における独自の保護法益として位置づけることが可能かということについて検討する。

第3章から第5章まで、イギリス・フランス・ドイツの個人情報保護法について検討してきた。これら三国では、個人情報の侵害に対して実際に刑罰が科されるケースは少なく、刑罰の濫用は控えられているものの、個人情報保護法の立法段階においては、個人情報の重要性や、個人情報の侵害に関するトラブルの発生という理由から、個人情報の不正収集などを直接的に処罰する規定を設けるという結論が比較的容易に導き出されているように思われる。しかし、刑法の謙抑性の原則に鑑みれば、情報の価値が高いということから直ちに刑罰的保護の強化に直結するとはいえない¹⁸⁷ので、個人情報を独自の保護法益として位置づけるためには更なる議論が必要となる。

個人情報は、科学技術の発展に伴ってその重要性が注目される新しい利益である。個人情報のほかに、現代社会が生み出した諸問題を契機として保護法益化が議論された利益には「環境」がある。「環境刑法」は大気、水、土壌などの環境を保護するために刑法を用いるという試みであり、従来の刑法が保護してきた生命、身体、財産、自由などの利益以外の新しい利益を刑法における保護法益として位置付けるという点は、本論文の問題意識と

¹⁸⁶松原芳博「情報の保護」法学教室298号（2005年）54頁。

¹⁸⁷松原・前掲注（186）54頁。

共通する。「環境刑法」には、環境が刑法における保護法益として無限定であるからこそ、環境の刑法的保護については刑法の倫理形成機能に基づく行為無価値論的理解に立脚した上で、環境倫理の維持を環境刑法の役割とする見解がある¹⁸⁸。その一方で、「環境」という概念が広範で無限定であることによって「環境」の保護法益性が否定されるものではなく、環境が汚染されれば最終的には人間に対する不利益として還元されることから、「快適な環境」という利益も重要な法益として認められるべきであり、問題となるのは「環境」という利益を保護するために刑法の発動を認めるべきか否かということであるとする見解もある¹⁸⁹。「不特定・多数人の健康およびその健康と結びつく生活環境という保護『法益』に対する侵害の危険という視点」から、環境汚染行為の処罰根拠と犯罪成立要件を理解することが可能であることも指摘されている¹⁹⁰。

「環境刑法」には前述のように多様な見解が存在するが、現在の憲法学説において「環境権」が認められていることもあり、環境を保護法益として位置付ける見解は一定の賛同を得ているものと思われる。実際に、一定程度の環境汚染行為は、水質汚濁防止法や大気汚染防止法等の法律によって罰則の対象となっている。射程範囲が広範であり、社会的法益的性格を有する「環境」が保護法益として認められるのであれば、個人に帰属する個人情報も保護法益として位置付けることにはさほどの困難はないのではないだろうか。「環境」とは異なり、個人情報はその範囲を限定することが比較的容易であるので、「情報倫理の維持」という行為無価値論的構成を採らなくとも、保護法益として位置付けることは可能だろう。

「環境権」という文言は憲法の条文には記載されていないものの、憲法学説によって権利、つまり法益として認められている。「環境権」は、健康で快適な生活を維持する条件としての良い環境を享受し、これを支配する権利であると理解されている¹⁹¹。環境権は、環境破壊を予防・排除するために提唱された権利であり、良い環境の享受を妨げられないという側面では自由権であるから、憲法13条の幸福追求権の一内容であると共に、環境権を具体化・実現するためには公権力による環境保全や改善のための施策が必要であるから、その面では社会権としても位置付けられると解されている¹⁹²。「環境権」という名称の権利を正面から認めた判例は存在せず、大阪空港付近の住民が人格権・環境権を根拠に、損害賠償と午後9時以降の飛行機の発着の禁止を求めて出訴した大阪空港公害訴訟（最決昭和56年12月16日民集35巻10号1369頁）では、過去の損害の賠償のみを認め、

¹⁸⁸伊東研祐『『環境の保護』の手段としての刑法の機能』『団藤重光博士古稀祝賀記念論文集』3巻（有斐閣・1984年）279頁。

¹⁸⁹山本輝之『『法益の保護』、『刑法の謙抑性』の原則は維持できるのか？』法学教室223号（1999年）18頁以降。

¹⁹⁰内藤謙「法益論の一考察」『団藤重光博士古稀祝賀記念論文集』3巻（有斐閣・1984年）25頁。

¹⁹¹芦部信喜（高橋和之補訂）『憲法（第5版）』（岩波書店・2011年）262頁、辻村みよ子『憲法（第4版）』（日本評論社・2012年）305頁。

¹⁹²芦部（高橋）・前掲注（191）263頁、辻村・前掲注（191）305～306頁。

環境権を根拠とした差し止め請求を却下した。しかし、その後の下級審裁判例には、道路公害訴訟において一定水準以上の大気汚染物質排出の一部差し止め請求が認められる例¹⁹³や、基地の騒音などについて高額な損害賠償の支払いが命じられる例¹⁹⁴もあり、良い環境を享受する権利が間接的に認められる方向へと変化しているようである。

このように、憲法の領域において「権利」として認められている利益には、刑法における保護法益としての地位を付与しても差し支えないのではないだろうか。刑法によって保護される生命・身体・自由・財産・名誉といった法益は当然ながら憲法によっても根拠づけられているので、これらの伝統的な利益に包含されない利益であっても、憲法の領域において保護され得る利益であれば、刑法による保護の対象とすることに何ら問題はない。

実際に、刑法における法益論の先行研究にも、憲法上の価値から法益概念を導き出す見解が複数存在する¹⁹⁵。ロクシンは、刑法の任務は、憲法的に保障されたすべての基本権の保障（Gewährleistung）に基づいて、市民の自由で平和な共同生活を保護することにあると述べている¹⁹⁶。続いてルドルフィーも、刑事立法者は人間の有益な社会生活に対する結果を考慮することなく、特定の道德違反を罰則によって禁止することは許されないという観点から、法益概念の形成においては基本法（憲法）による価値判断に従い、純粋な道德違反を刑罰威嚇の対象から除外するべきであり、あるいは個人の自由と責任に基づく有益な社会生活のための条件を侵害または危険にさらす行為のみが刑罰威嚇の対象となるべきであると解している¹⁹⁷。

そして、日本の刑法学説にも、「刑罰法規による保護の客体としての『法益』の概念は、日本国憲法を基礎とする法の全体系を考慮し、『憲法の基本原理と構造からみて刑罰法規による保護に値する生活利益』という意味での『憲法的・実質的法益概念』でなければならない」¹⁹⁸とする見解と、「法益とは、国家として憲法に従って構成される（べき）社会の内における当該社会構成員の共同生活の存立の為に必要不可欠な条件であって、且つ、純粋

¹⁹³神戸地判平成12年1月31日判時1726号20頁。

¹⁹⁴金沢地判平成14年3月6日判時1798号21頁など。

¹⁹⁵ドイツと日本の両国において、法益論が刑法解釈や刑事立法に果たす機能やその限界についての議論が活発に行われており、先行研究も数多く存在する。最近の代表的な研究としては、法益論は刑事立法に対する制約機能（立法的批判機能）を有しており、その意義を失っていないとする、嘉門優「法益論の現代的意義（1）（2・完）－環境刑法を題材にして」大阪市立大学法学雑誌50巻4号（2004年）934～972頁、51巻1号（2004年）96～132頁がある。法益論それ自体についての研究も興味深いテーマではあるが、本論文における筆者の問題意識は、個人情報刑法における法益性と妥当な規制方法であるので、法益論の沿革と、法益論の刑法学における機能についての詳細には立ち入らない。

¹⁹⁶Roxin, a, a, O, S. 16.

¹⁹⁷Hans-Joachim Rudolphi, Die verschiedenen Aspekte des Rechtsgutsbegriffs, Festschrift für Richard M. Honig, zum 80. Geburtstag, 1970, S. 160～161.

¹⁹⁸内藤・前掲注（190）15頁。

規範によって保護されている（べき）因果的に変更可能な対象である」とする見解¹⁹⁹がある。

これらの見解は刑法解釈や刑事立法を憲法という観点から制限・拘束するものであり、憲法を根拠に新しく刑罰法規を設けることを可能にするものではなく、憲法の領域で認められる権利を刑法における法益として位置付けるための根拠にはならないという批判も予想される。しかし、日本の憲法学説と判例が認めるに至った「新しい人権」の多くは、従来から存在する憲法13条の幸福追求権の解釈から導出されたものであるもので、表現の自由や生存権といった、憲法制定当時から存在する人権も、環境権やプライバシー権などの「新しい人権」も、憲法で認められた権利であることには変わりはない。したがって、個人情報という新しい利益であっても、これが憲法における権利として認められる以上、刑法における保護法益として位置付けることは可能である。そこで、ここからは、個人情報という利益の憲法上の意義を検討することによって、個人情報の刑法における保護法益性について分析を進める。

憲法上のプライバシー権は、個人情報との関連において「自己情報コントロール権」として理解されるという学説²⁰⁰が有力に主張されている。元来、プライバシーの権利はアメリカの判例において「ひとりで放っておいてもらう権利（the right to be let alone）」として理解され、日本においても「宴のあと」事件1審判決（東京地判昭和39年9月28日判時385号12頁）²⁰¹が「私生活をみだりに公開されない法的保障ないし権利」として定義した。このように、プライバシー権は、個人の私的領域に他者を無断で立ち入らせないという消極的な権利として理解されてきたが、情報化社会の発展に伴って、自己に関する情報を自らコントロールし、自己の情報とプライバシーの保護を公権力に対して請求するという積極的な権利としての側面が重視されるようになっていく²⁰²。確かに、自己についての情報公開や、誤った情報の抹消を行政に請求する権利は保障されなければならないだろう。その意味では、プライバシー権を単なる自由権として解するのではなく、請求権としての側面も加味する考え方には一定の意義がある。しかし、個人に関する知識・情報はコントロールできないものであり、他者によって知覚され得るものである²⁰³。

¹⁹⁹伊東研祐『法益概念史研究』（成文堂・1984年）414頁。

²⁰⁰芦部（高橋）・前掲注（191）121～122頁など。

²⁰¹元外務大臣で、東京都知事選に落選した有田八郎をモデルにした三島由紀夫の小説「宴のあと」において、有田とその妻との夫婦喧嘩や妻への暴力等の私生活を暴露する描写があったことから、有田は三島由紀夫と小説を出版した新潮社を相手取り、プライバシーの侵害であるとして損害賠償と謝罪広告を請求した。

²⁰²芦部（高橋）・前掲注（191）122頁。

²⁰³阪本昌成『プライバシー権論』（日本評論社・1986年）8頁。宮下紘「ビックデータの活用とプライバシー保護」法学セミナー707号（2013年）11頁においても、『自己情報コントロール権』としてのプライバシー権論については、大量のデータが世界の至る所で処理されている情報化社会において満足に自らのデータをコントロールすることなどできないため、その勢いを失いつつある」とされている。林紘一郎『「個人データ保護」

他者によって知覚される可能性があり、知覚されざるをえない場合もあることは「センシティブな知識・情報」であっても同様である²⁰⁴。この論者の主張する通り、情報の流通は本来であれば個人がコントロールできる性質のものではない。自己についての情報が他者に知覚されたとしても、自己の個人情報を手元から失われることはないものの、情報が一度でも他者に知覚されれば、情報の内容を取り返すことはできない。情報は個人に帰属するものであるが、財物とは異なり、個人がその流通を支配することはできないのである。

また、「自己情報コントロール権」という考え方は、自己に関する情報について何らかの問題が発生する前に自己解決をするという事前規制的な性格を有していると考えられるが、情報を自己によってコントロールする権利が保護されるのであれば、一度他者の知るところとなった情報は保護されないということになり、不当な結論を導くのではないだろうか。以上のことから、「自己情報コントロール権」という考え方に賛同することはできない。

このように、「自己情報コントロール権説」には幾多の問題があるものの、個人情報保護法が制定される以前から、個人情報保護されるべきことは判例によって提唱されてきた。

まず、地方自治体が弁護士の照会に応じて原告の前科情報を提供した行為につき、原告が自己の名誉・信用・プライバシーが侵害されたとして損害賠償を請求した「前科照会事件」の最高裁判決（昭和56年4月14日民集35巻3号620頁）では、「前科及び犯罪経歴は人の名誉、信用に直接かかわる事項であり、前科等のある者もこれをみだりに公開されないという法律上の保護に値する利益を有するのであって、市区町村長が、本来選挙資格の調査のために作成保管する犯罪人名簿に記載されている前科等をみだりに漏えいしてはならないことはいうまでもない」ということから、地方自治体が照会に応じた行為は違法な公権力の行使であると判断された。伊藤正己裁判官の補足意見では、「前科等は、個人のプライバシーのうちでも最も他人に知られたくないものの一つ」であるとされており、情報がみだりに提供されない権利がプライバシー権として認められるという趣旨が示されている。

続いて、大学主催の講演会に参加申し込みをした学生の氏名・住所等を記載した名簿の写しを警察署に提出した大学の行為につき、学生らがプライバシーの侵害であると主張して損害賠償を請求した「早稲田大学江沢民講演会事件」の最高裁（平成15年9月12日民集57巻8号973頁）は、「本人が、自己が欲しない他者にはみだりにこれを開示されたくないと思えることは自然なことであり、そのことへの期待は保護されるべきもので

の法益と方法の再検討:実体論から関係論へ』情報通信学会誌31号（2013年）81～82頁によると、「自己情報コントロール権説」には、次の7つの欠点がある。①コントロールは手段であって保護の内容や権利ではない、②情報と情報主体との関係は多様でパターン化しにくい、③権利内容を事前に細部まで設定できるという誤解に基づく、④技術的にコントロールできるという実効性の保証がない、⑤プライバシー侵害の防止に傾きやすく情報の円滑な利用を阻害するおそれがある、⑥実定法上の根拠が明確でない、⑦コントロールを徹底すれば財産権的色彩（排他性）が強くなり弊害が生ずる、というものである。

²⁰⁴阪本・前掲注（203）8頁。

あるから、本件個人情報、上告人らのプライバシーに係る情報として法的保護の対象となる」と判断した。この事件で問題となった個人情報は前科等のセンシティブなものではなく、氏名・住所といった基本的なものであったが、本件の最高裁は個人情報一般につき法的保護が及ぶと解している。

そして、1999年に改正された住民基本台帳法に基づいて、氏名・住所・生年月日・性別等の本人確認情報を住民基本台帳ネットワークシステムに取り込むことが、プライバシーの侵害にあたるとして、市民が居住する市に対して国家賠償請求を行った「住基ネット事件」の最高裁（平成20年3月6日民集62巻3号665頁）でも、「何人も、個人に関する情報をみだりに第三者に開示又は公表されない自由を有する」と判断された。もっとも、本件最高裁は問題となった本人確認情報のうち、氏名・生年月日・性別・住所の4つの情報は「秘匿性の高い情報とはいえない」ので、市町村が住基ネットによって情報を管理・利用する行為は「個人に関する情報をみだりに第三者に開示又は公表されない自由」を侵害するものではないと解しており、個人情報をその秘匿性・重要性によって区別している。このように、個人情報が法的に保護される利益であることが判例の蓄積によって明らかとなっている。そして、これらの判例は個人情報が保護される根拠として、「自己情報コントロール権」という概念には依拠せず、自己の意思に反して個人情報を開示されたり探知されたりすることからの自由として捕えているようである。それでは、このような自由が法的に保護される根拠はどこにあるのだろうか。

「自己情報コントロール権説」を批判しつつ、プライバシーの利益を「評価の対象となることのない生活状況または人間関係が確保される状態に対する正当な要求または主張」と定義し、このうち、「法的承認をうけるに値する利益」がプライバシー権であるとする見解²⁰⁵がある。同様に、刑法の名誉毀損罪に関する学説にも、プライバシーの保護は社会的評価から自由な領域の保護として解釈され、正しい社会的評価を受けるべき利益である名誉とは区別されるというものがある²⁰⁶。このように、プライバシーの利益を「社会的評価からの自由」として解釈する見解には、名誉とプライバシーを明確に区別することが可能になるという利点があり、本来であればコントロールできる性質のものではない情報を管理・支配可能なものとして扱う「自己情報コントロール権説」の弱点も克服しているので、本論文においても、「社会的評価からの自由という利益」の側面から個人情報保護を検討する²⁰⁷。

²⁰⁵阪本・前掲注（203）9頁。

²⁰⁶佐伯仁志「プライバシーと名誉の保護（4・完）」法学協会雑誌101巻11号（1984年）65頁。

²⁰⁷阪本・佐伯による「社会的評価からの自由」としてのプライバシー権という考え方に賛同しつつ、刑法230条の名誉毀損罪について、①社会的評価から自由であるべき私的領域におけるプライバシーと、②社会的評価を受けるべき領域において、確実な資料・根拠に基づいて論評される利益としての名誉の2つが保護法益であると再構成する論文として、佐藤結美「名誉毀損罪の再構成—プライバシー保護の観点から—（1）（2・完）」北大法学論集62巻5号（2012年）204～157頁、62巻6号（2012年）、

プライバシーの利益が「社会的評価からの自由」であると解すれば、どのような個人情報保護の対象となるのであろうか。当該個人の「社会的評価」を左右する性質の個人情報には、前科前歴、健康状態、経済状況などといった、それが漏洩・提供・探知の対象となれば当該個人の社会的評価が低下し得るものは問題なく含まれるだろう。その一方で、氏名・住所といった、基本的な本人確認情報は「社会的評価からの自由」に影響する個人情報であるといえるだろうか。「氏名、住所、電話番号、顔かたち等は、本来社会的に開かれた個人情報であって、公的またはせいぜい中立的な性質の個人情報である」という指摘²⁰⁸がなされている。確かに、氏名や住所、性別などの基本的な個人情報が他者の知るところになったとしても、それ自体によって当該個人の社会的評価が左右されるとは考え難い。しかし、住所などの基本的な情報も、使用方法によっては当該個人の生活に不利益が生じる蓋然性がある。本人の知らない間に、もしくは本人に対する情報の使用目的の告知が行われることなく、氏名・住所・電話番号の情報を収集して名簿を作成し、名簿が売買されたことによって本人に勧誘電話が頻繁にかかってくるようになったというようなケースでは、個人情報の不当な取り扱いによる生活への介入・干渉が行われているといえるだろう。このように、「社会的評価からの自由」を左右しない性質の基本的な個人情報であっても、不当に扱われたことによって何らかの損害が発生し得るのであれば、そのような個人情報も保護に値する利益であるといえる。

日本の個人情報保護法は情報の性質を区別することなく、一律に「個人情報」を保護客体としているが、刑法的保護の対象となる「個人情報」は、第一に、「社会的評価からの自由」を左右し得る性質の情報であると考えられる。このような個人情報には、医療情報、前科前歴、信用情報といったものが該当する。続いて「社会的評価からの自由」に影響しない氏名・住所といった情報であるとしても、それらの扱われ方によって個人の生活に不利益が発生する場合には、そのような情報も保護の対象となる。その意味において、個人情報を「センシティブ情報」とそれ以外の一般的な情報を区別するイギリス・フランス・ドイツの個人情報保護法制には見習うべきところがある。いずれの性質の個人情報であっても保護法益としての地位を有することには変わりないが、後者の性質の個人情報の場合は、「社会的評価からの自由」の侵害が認められない以上、処罰がなされるためには情報が不当に扱われたことによって当該個人の生活に不利益が発生したという結果が必要だろう。このように、刑法における保護の対象となり得る個人情報は2種類に分けられ、「社会的評価からの自由」または生活に対する不当な干渉・介入からの自由が保護法益として観念されるので、個人情報に対する侵害行為は精神的自由に対する罪として位置付けられる。

本節では、個人情報保護法が刑法における保護法益としての地位を有し得ることについて明らかにしたが、個人情報に法益性を付与することが直ちに「刑法の謙抑性の原則」に違反するとはいえない。どのような個人情報に対して、どのような侵害行為をすれば刑罰の対象

350～314頁。

²⁰⁸阪本昌成『プライバシーの権利』（成文堂・1982年）199頁。

となり得るのかという制裁論のレベルにおいて慎重な議論を行うことによって、法益保護と謙抑性原則の均衡を保つことは十分に可能である。

第2節 個人情報の侵害に対する妥当な規制のあり方

前節では、個人情報が刑法における保護法益としての地位を有し得るということを検討した。そこで、本節では、個人情報に対するどのような侵害行為が刑罰の対象となり得るのか、刑罰の他に妥当な規制方法はあるのかということについて、第3章から第5章までで得られた外国法の知見をもとに考察する。

第1項 第三者機関による監視の可能性

イギリス・フランス・ドイツの個人情報保護の在り方で共通しているのは、①中立的・専門的な第三者機関が個人情報の取り扱いを監督しており、第三者機関は法律違反に対して金銭制裁（ドイツの場合は過料）を科す権限を有していることと、②個人情報の不正収集、無断での第三者提供といった広範な侵害行為を間接罰ではなく、直接的に処罰する規定が多数設けられていること、③刑罰規定が多く設けられているものの、実際には第三者機関による監督や金銭制裁が功を奏しており、刑罰が科されるケースは少ないことである。日本では個人情報保護法の違反を直接的に処罰する規定は存在せず、中立的・専門的な第三者機関も存在せず、省庁のガイドラインや企業等の自主規制というレベルに留まっている一方で、イギリスにおける情報コミッショナー、フランスにおける CNIL、ドイツにおける連邦データ保護監督官・州の監督官庁が強力な権限でもって個人情報の取り扱いを監督することによって、刑罰の発動が結果的に控えられているという実態には見るべきものがある。日本においても、そのような第三者機関を設けることは可能だろうか。社会保障や税の分野を中心に、国民一人ひとりに個人番号を設ける「行政手続における特定の個人を識別するための番号の利用等に関する法律（以下、共通番号法とする）」の成立に伴って設けられた独立第三者機関である「特定個人情報保護委員会」や個人情報保護法における主務大臣制度との関係から検討する。

第1款 共通番号法成立前の第三者機関に関する議論

イギリスなどの諸外国には個人情報保護のための第三者機関が設けられている一方で、日本の個人情報保護法には主務大臣が命令を行うという制度が採られ、独立の権限を有する第三者機関が設けられることはなかった。

個人情報保護法施行後も、いくつかの審議会等で第三者機関の設置に関する議論が行われてきた。内閣府国民生活審議会個人情報保護部会（現在は消費者庁に設置されている）の2007年6月29日の「個人情報保護に関する取りまとめ（意見）」では、民間部門における個人情報の取り扱いについて、「我が国では、個人情報の取扱いは民間事業者の事業活動の一環として行われ、当該事業活動と不可分なものであるとともに、業種・業態に応

じた様々な特性を有していることから、個人情報 の適正な取扱いを十分に確保するためには、事業ごとのきめ細かい判断が不可欠であり、また、当該事業活動に関する事務と一体的に遂行することが合理的かつ実効的であると考えられる。こうしたこと等から、当面、主務大臣制を維持することが妥当であると考えられ、第三者機関の設置については、国際的な整合性も踏まえ、中長期的課題として検討することが必要である」とされた²⁰⁹。

「中長期的課題として検討する」必要性が指摘されていることから、第三者機関設置の可能性を全面的に否定する考えではないものの、2001年9月25日データ保護コミッショナー国際会議で採択された「「資格に関する委員会の基準及び規則並びに認定の原則」²¹⁰が、第三者機関として認められるために次の条件の充足を要求していることを受けて、日本の機関がこの要件を充足することは困難であるとされた。

その条件は以下の通りである。

①適切な法的根拠に基づいて設置された公的機関であること。

②所掌事務の遂行のために適切な水準の自主性・独立性が保証されていること。

自主性については、第三者機関が、法的・実務的に、第三者の許可を得ずに適切な措置を講じる権限を付与されていることが求められる。独立性については、第三者機関が政治的・行政的干渉を受けずに活動し、既得権益の影響に耐えることができるために重要である。

③所掌事務を定めている法律が、データ保護やプライバシーに関する国際的な枠組みに準拠していること。

④適切な範囲の機能を有しており、その実施が法的な権限により担保されていること。

データ保護の第三者機関は、法令順守、監督、調査、救済、指導及び公教育等の分野について、一連の機能を有する。第三者機関は、助言的な機能を有するだけでなく、法的・行政的な結果を伴う監督権限を有さなければならない。

第3章から第5章で検討してきたイギリス・フランス・ドイツの第三者機関は各々のデータ保護法にその存在が規定され、独立した監督機関として位置付けられ、命令を行ったり違反に対して金銭制裁を科したりする等の権限を有していることから、これらの条件を充足している。その一方で、この報告書では「自主性・独立性や、適切な範囲の機能及びその実施の法的な権限による担保の観点から」、日本の機関は条件を充足できない²¹¹とされているが、そのような第三者機関を設立することにつき現行法の枠組では限界があるという趣旨なのか、それとも社会的な実態として困難であると解しているのかということは定かではない。

国民生活審議会の前述の報告書は民間事業者の個人情報取り扱いに関するものであったが、公的部門における個人情報取り扱いにおいても、独立の第三者機関は設置されていな

²⁰⁹国民生活審議会個人情報保護部門「個人情報保護に関する取りまとめ（意見）」

<http://www.caa.go.jp/seikatsu/shingikai/kojin/20th/torimatome.pdf>.

²¹⁰2002年9月9日データ保護プライバシーコミッショナー国際会議で改定された。

²¹¹前掲注（209）「個人情報保護に関する取りまとめ（意見）」

い。行政機関個人情報保護法と独立行政法人等個人情報保護法では、両法を所管する総務大臣による監督が認められているものの、諸外国の第三者機関のような広範で強力な権限を有するものではない。各々の地方公共団体が保有する個人情報についてはそれぞれの個人情報保護条例が一般法として規定されているが、地方公共団体の条例では執行機関としての委員会や委員を置くことはできない（地方自治法138条の4第1項）ことから、地方公共団体にはイギリス等のような独立した第三者機関を置くことは法的に不可能であることが指摘されている²¹²。国の公的部門と民間部門について、独立第三者機関を置くことに法律上の制約はあるのか否かについては検討の余地がある。

2011年7月に公表された、消費者委員会個人情報保護専門調査会の報告書²¹³では、第三者機関について以下の3点が検討課題であるとされた。

（1）個人情報保護法制の執行に、自主性・独立性を保証された第三者機関が関与すべきとの意見については、社会保障・税番号制度の検討における議論を参照しつつも、個人情報保護法制の全体像を視野に入れた構想として、具体的な在り方や想定される効果等を検討する必要がある。

（2）社会保障・税番号に係る個人情報との関係で設置が検討されている第三者機関に、番号以外に係る個人情報についても苦情の受付や制度運用の監督を行う権限を与えるべきとの意見については、個人情報保護法制の全体像を視野に入れた構想における選択肢の一環として、検討する必要がある。

（3）個人情報保護法上の主務大臣と第三者機関との間における機能配分等の整理については、番号法における議論の進展を注視しつつ、個人情報保護法制としての全体的な整合性・実効性を確保する観点から、個人情報保護法の在り方についても検討する必要がある。

このように、2007年の国民生活審議会の報告書の段階では個人情報保護分野における第三者機関を設けることについて懐疑的な論調であったのに対して、個人情報保護専門調査会の報告書では、個人情報保護制度全体において、独立の第三者機関を設ける可能性が示唆されている。その根拠は、①個人情報保護法を改正せずに番号制度の枠組みで第三者機関がつくられるとすれば、その「番号」を特別に扱う理由が不明確であるということ、②番号制度において設置を検討されている第三者機関が、他の行政機関の個人情報保護についても監督等するのが効率的であり、公的機関以外の民間機関における個人情報・プライバシー保護についても、主務大臣制ではなく、法律と技術の専門家を十分に配置した第三者機関で一元化して苦情を受け付け、各事業者を監督したほうがよいのではないかとということなどである。この報告書では個人情報保護法における主務大臣制度についても、個人情報を取り扱う各々の事業分野の特殊性を考慮した監督を行ってきたとして一定程度の

²¹²宇賀克也「特定個人情報保護委員会について」情報公開・個人情報保護49号（2013年）68頁。

²¹³「個人情報保護法及びその運用に関する主な検討課題」

<http://www.cao.go.jp/consumer/history/01/kabusoshiki/kojin/doc/houkokusho.pdf>.

評価をしているが、情報についての専門性を有する第三者機関と主務大臣が共存することが期待されている²¹⁴。主務大臣制度のもとでは、個人情報取扱事業者の取扱う事業を管理する権限を有している大臣または国家公安委員会が「主務大臣」として勧告や命令を行うので、経済産業分野における個人情報の取り扱いに何らかの違反があれば経済産業大臣が、医療や介護の分野においては厚生労働大臣が「主務大臣」となる。このように、当該事業の個別具体的な実態について知悉している主務大臣が取り締まることには、監督業務によって各々の事業が不当に妨害されないという利点があると考えられるので、第三者機関を設けることは主務大臣制の廃止にはつながらない。

第2款 特定個人情報保護委員会

2013年5月24日に国会で成立し、5月31日に公布された共通番号法では、特定個人情報保護委員会という第三者機関が内閣府の外局の委員会として設置されることとなった。

(1) 法律の概要と「特定個人情報」について

この法律における「共通番号制度」の下では、①一人ひとりの個人（住民票を有する在留外国人も対象となる）に対して、住民票コードから生成された固有の「個人番号」が付与される。続いて、②この番号によって紐付けされた同一人の情報は、社会保障分野（年金、医療、介護保険、福祉、労働保険）、税務分野（国税、地方税）、東日本大震災後に追加された災害対策分野において利用するために、複数の府省庁や地方公共団体の間で相互に連携する。そして、③これらの機関で保有している情報について、同一人の情報であることの確認を行う。

このような共通番号制度の意義は、分散されている個人情報の名寄せ・突合せの負担を減らすことによる行政運営の効率化と、本人確認手続の簡素化による負担軽減と利便性の向上にある（共通番号法1条）。この法律では、「個人番号」の他に「特定個人情報」も保護の対象となる。特定個人情報とは、「個人番号をその内容に含む個人情報」とであるとされているので（法2条8項）、「個人情報＋個人番号」のセットを指している。共通番号法2条3項によると、「個人情報」とは「行政機関個人情報保護法第2条第2項に規定する個人情報であって行政機関が保有するもの、独立行政法人等個人情報保護法第2条第2項に規定する個人情報であって独立行政法人等が保有するもの又は個人情報の保護に関する法律第2条第1項に規定する個人情報であって行政機関及び独立行政法人以外の者が保有するもの」である。つまり、生存する個人に関する情報であって、特定の個人を識別することができるものを意味している。

共通番号制度は社会保障と税の分野を主な対象としていることから、特定個人情報は秘密性の高い情報とともに使われることになる²¹⁵という指摘があり、特定個人情報の提供・

²¹⁴前掲注（213）「個人情報保護法及びその運用に関する主な検討課題」

²¹⁵石井夏生利「個人番号制度と第三者機関」法学セミナー707号（2013年）15頁。

収集・保管が原則的に禁止されていること（１９条・２０条）は諸外国の個人情報保護法制における「センシティブ情報」の取り扱い条件と類似している部分がある。さらに、本法に設けられた第三者機関は個人情報一般ではなく特定個人情報を取り扱うものであることから、特定個人情報の要保護性は高く位置付けられているのであろうが、特定個人情報を構成する個人情報と個人番号は、そもそも性質の異なる客体である。個人番号は行政手続の効率化や本人確認の利便性向上のために導入されたものであり、その意味では国家的法益的な性格を有していると考えられる。にもかかわらず、個人的法益的な性格を有する個人情報とセットにして一つの法概念として構成するのは不合理ではないだろうか。

共通番号制度そのものに対しては、社会保障等の分野における正確な所得の把握にどの程度役に立つのかという費用対効果が不明であるとの批判があり、新聞等で報道されていることに反して、この制度が導入されたとしても個人情報を一元管理することはできない。番号制度が導入されても、個人情報は従来通り市町村、独立行政法人、健康保険組合といった各行政機関等が保有するという分散管理体制を採る。情報保有機関 A が他の機関 B の保有する個人情報を必要とする場合には、A は B に照会を行うことになっているが、その際に個人番号を直接用いるのではなく、情報照会 A 機関と情報提供 B 機関がそれぞれ保有する個人番号に割り当てられている「符号」を用いる。これを前提に、情報照会機関 A が、照会を希望する特定個人情報名と符号 A を情報提供ネットワークシステムに送信する。次に、これを受け取った情報提供システムネットワークでは符号 A を、情報提供機関 B の符号 B と変換することによって、情報提供を許可して符号 A と B を紐付ける。そして、情報提供システムネットワークから情報提供機関 B に対し、A が照会を希望する特定個人情報名と符号 B を送信する。これを受信した情報提供機関 B は当該特定個人情報を抽出し、情報照会機関 A に送信して完了するという流れである²¹⁶。このように、共通番号制度において個々の機関が作成した個々の符号が用いられているのは、個人番号を直接用いることによってどこかの機関から特定の個人番号が漏洩したような場合に、それを用いて特定個人情報すべてを取得されるおそれがあり、それを回避するためである。個人番号の不正な取り扱いによる不利益の発生が予想されることには疑問をはさむ余地はないが、個人番号は符号を媒介とするものの、情報のやり取りをするための手段であり、個人情報はその手段を用いた結果として得られる目的物である。「特定個人情報」という概念は、手段としての個人番号と結果としての個人情報という性質の異なる２つのものをセットにしているという点でやはり不合理である。個人番号と個人情報の両方が保護に値するものであるならば、

宮下紘「番号制度と個人情報保護 個人番号の利用開始に向けて」時の法令１９４３号（２０１３年）７０～７１頁は、個人番号で扱う情報の機微性ゆえに、職場・財産・収入情報に世帯や障害に関する情報が紐づけられ漏洩すれば、個人情報のみによって偏見・差別や好奇心が助長されることになり、その損害は単純な個人情報の漏洩の比ではないと述べている。

²¹⁶岡村久道『よくわかる共通番号法入門 社会保障・税番号のしくみ』（商事法務・２０１３年）５２～５３頁。

別々の概念として構成した上で法規定を設けるべきであっただろう。

「特定個人情報」という法概念に賛同することはできないが、個人情報の取り扱いを監督する独立した第三者機関の可能性を検討するにあたり、特定個人情報保護委員会については参照する意義がある。ここからは、特定個人情報保護委員会の法的位置付けとその権限について分析する。

（２）特定個人情報保護委員会の独立性と専門性

特定個人情報保護委員会は、内閣府の外局に置かれている。内閣府設置法４９条３項の規定²¹⁷に基づき設置され、内閣総理大臣の所管に基づく委員会である（共通番号法３６条）。この委員会は、国家行政組織法３条に基づく「三条委員会」であり、省庁と並ぶ行政機関として位置付けられていることから、委員会が自らの名で命令を発し、施行規則を自ら定めることができる独立性の高い機関である²¹⁸。国家行政組織法８条に基づく審議会等である「八条委員会」に比して、その権限は広範である。

特定個人情報保護委員会は、「委員会の委員長及び委員は、独立してその職権を行う」（３９条）と規定され、職務の政治的中立性が法によって担保されている。委員会は委員長及び委員６人で構成され（４０条１項）、委員長と委員は「人格が高潔で識見の高い者」から両議院の同意を得て内閣総理大臣が任命する（４０条３項）。委員長と委員は、個人情報の保護に関する学識経験のある者、情報処理技術に関する学識経験のある者、社会保障制度または税制に関する学識経験のある者、民間企業の実務に関して十分な知識と経験を有する者及び連合組織²¹⁹の推薦する者で構成される（４０条４項）。委員長と委員は、在任中は原則的にその意に反して罷免させられることはなく、身分が保障されている（４２条）²²⁰。このように、委員会の構成員は独立性・政治的中立性が法によって担保されているだけでなく、複数の分野の専門的知見を有する者から任命されることが予定されており、複数の分野の専門家による慎重な議論により適切な結論に達することが期待されている²²¹。特定個人情報保護委員会が有する独立性と専門性は、イギリス・フランス・ドイツにおける

²¹⁷内閣府設置法４９条では、「内閣府には、その外局として、委員会及び庁を置くことができる。

２ 法律で国務大臣をもってその長に充てることと定められている前項の委員会には、特に必要がある場合においては、委員会又は庁を置くことができる。

３ 前２項の委員会及び庁（以下それぞれ「委員会」及び「庁」という。）の設置及び廃止は、法律で定める」とされている。

²¹⁸石井・前掲注（２１５）１７頁、岡村・前掲注（２１６）１９０頁、水町雅子「番号法の概要」ジュリスト１４５７号（２０１３年）３９頁。

²¹⁹地方自治法２６３条の３第１項の連合組織で、同項の規定による届出をしたものをいう。

²²⁰罷免されるのは、①破産手続開始の決定を受けた場合、②共通番号法の規定に違反して刑に処せられた場合、③禁固以上の刑に処せられた場合、④委員会により、心身の故障のため職務を執行することができないと認められたとき、又は職務上の義務違反その他委員長若しくは委員たるに適しない非行があると認められた場合に限る（４２条１～４号）。

²²¹宇賀・前掲注（２１２）７３頁。

個人情報保護の第三者機関と類似している。

（３）特定個人情報保護委員会の権限

特定個人情報保護委員会の権限には、個人情報保護法における主務大臣と同様のものもあるが、全体的には主務大臣に比して広範な権限を付与されている。まず、特定個人情報保護委員会は、個人番号利用事務等実施者に対し、特定個人情報の取り扱いに関して必要な指導および助言をすることができる（５０条）。個人番号利用事務等実施者には、国の機関も含まれる（２条１０項、１２項）。助言は個人番号利用事務等実施者による自主的解決を助けるための進言である²²²。指導・助言は、本人からの苦情や主務大臣等からの情報提供を契機として特定個人情報保護委員会が問題点を認識して行う場合もあり、対象者から求められて行う場合もある²²³。

次に、委員会は、特定個人情報の取扱いに関して法令の規定に違反する行為があった場合に、必要があると認めるときには当該違反行為者に対して期限を定めて、当該違反行為の中止その他違反を是正するために必要な措置をとるべき旨を勧告することができる（５１条１項）。勧告制度は、指導・助言では自主的な問題解決が図られない場合に用いられる。法律の文言上は勧告の前に指導・助言を行うことを要求するものではないが、実際には指導・助言を経た後、その内容を踏まえて行うことが想定されている²²⁴。ここでいう「法令の規定に違反する行為」は共通番号法のみならず、個人情報保護法、行政機関個人情報保護法などの法令違反も含まれている。「当該違反行為者」とは、特定個人情報を法律に基づいて取り扱う権限のある者のみならず、権限なしに違法に特定個人情報を扱う者も対象となる。したがって、個人番号利用事務等実施者、その事務に従事する者（派遣労働者も含む）、情報提供システムネットワークの運営機関およびその事務に従事する者といった情報実務に従事する者のほか、不正取得によって特定個人情報を保有している者、不正に漏洩した特定個人情報を転得するなどして特定個人情報を保有している者、個人番号の提供を求めることができないのに求めている者といった者などの、法令違反行為を行った全ての者が含まれる²²⁵。

続いて、委員会は、勧告を受けた者が正当な理由なく勧告に係る措置をとらなかった場合には、期限を定めて勧告に係る措置をとるべきことを命令することができる（５１条２項）。正当な理由なく勧告に従わないことが命令の条件となっているので、勧告が事実誤認に基づくものであることが判明したり、大災害等の、勧告を受けた者の責に帰すことのできない理由により勧告を遵守できなかつたりした場合には命令を行うことはできない²²⁶。このように、５１条２項の命令（通常命令）は勧告を前提としているが、特定個人情報の

²²²岡村・前掲注（２１６）１９７頁。

²²³宇賀・前掲注（２１２）７７頁。

²²⁴岡村・前掲注（２１６）１９８頁。

²²⁵宇賀・前掲注（２１２）７７頁。

²²⁶宇賀・前掲注（２１２）７８頁。

取扱いに関して法令の規定に違反する行為があった場合において、個人の重大な権利利益を害する事実があるため緊急に措置をとる必要があると認めるときは、当該違反行為者に対して、期限を定めて、当該違反行為の中止その他違反を是正するために必要な措置をとるべき旨を命ずることができる（５１条３項）。これを緊急命令といい、通常命令とは異なり勧告を経る必要はなく、違反行為に対して直ちに命令することが可能である。５１条２項の通常命令や５１条３項の緊急命令に違反した者は、２年以下の懲役または５０万円以下の罰金に処せられ（７３条）、主務大臣による命令の違反と同様に間接罰の仕組みが採られている。

委員会は、この法律の施行に必要な限度において、特定個人情報を取り扱う者その他の関係者に対し、特定個人情報の取り扱いに関する必要な報告もしくは資料の提出を求め、またはその職員に、当該特定個人情報を取り扱う者その他の関係者の事務所その他必要な場所に立ち入らせ、特定個人情報の取扱いに関し質問させ、もしくは帳簿書類その他の物件を検査させることができる（５２条）。報告・資料要求と立入検査は「この法律の施行に必要な限度」で行うことができるので、特段の違反行為の存在を要件としない。この規定による報告や資料の提出をせず、もしくは虚偽の報告・資料を提出し、また当該職員の質問に対して答弁をせず、もしくは虚偽の答弁をし、もしくは検査を拒否、妨害、忌避した者は、１年以下の懲役または５０万円以下の罰金に処せられる（７４条）。

個人情報保護法における主務大臣にも、報告要求、助言、勧告・命令する権限が認められているが、特定個人情報保護委員会にはそれらに加えて立入検査を行う権限が設けられ、それを拒否等することが刑罰で禁止されていることは特徴的である。イギリス・フランス・ドイツの個人情報保護のための第三者機関には立入権限が付与されており、委員会は EU 型の第三者機関に類似した存在となっているといえる。さらに、特定個人情報保護委員会は、個人番号その他の特定個人情報の取り扱いに利用される情報提供ネットワークシステムその他の情報システムの構築および維持管理に関し、総務大臣等に対して必要な措置を実施するよう要求したり（５４条）、特定個人情報保護に関する施策の改善について内閣総理大臣に対して意見を述べたりすることができる（５５条）。

特定個人情報保護委員会について、共通番号法附則６条２項では、「政府は、この法律の施行後１年を目途として、この法律の施行の状況、個人情報の保護に関する国際的動向等を勘案し、個人番号をその内容に含む個人情報である特定個人情報以外の取扱いに関する監視または監督に関する事務を委員会の所掌事務とすることについて検討を加え、その結果に基づいて所要の措置を講ずるものとする」とされているので、「近い将来において、特定個人情報保護委員会が、個人情報保護全般を対象とする第三者機関に発展する可能性もある」²²⁷。

²²⁷宇賀・前掲注（２１２）６９頁、石井・前掲注（２１５）１９頁。

（４）主務大臣制との関係

（３）で見てきたように、特定個人情報保護委員会には様々な権限があり、その中には委員会に独自のものと、主務大臣にも付与されているものがある。具体的には、特定個人情報保護委員会の指導・助言権限、報告・資料要求権限、勧告・命令権限と、主務大臣の報告要求権限（個人情報保護法３２条）、助言権限（３３条）、勧告・命令権限（３４条）の関係が問題となる。特定個人情報保護委員会の権限は、一般的には特定個人情報の取扱いに関するものである一方で、主務大臣の権限は個人情報、個人データまたは保有個人データに関する権限であるが、その対象が重複する場合もある。個人情報保護法が主務大臣による監督の仕組みを採用したのは、主務大臣が各業界の実情についての情報を得やすい立場にあり、膨大な民間事業者を一つの機関が監督することが困難だからであるので、専ら特定個人情報保護委員会が特定個人情報について監督するわけではなく、主務大臣による監督が否定されるものではない²²⁸。

主務大臣と特定個人情報保護委員会の分業につき、３つのパターンを提示する見解²²⁹がある。この論者によると、①勧告・命令権限を第三者機関に一元化し、主務大臣が第三者機関の権限発動を求める方法、②主務大臣と第三者機関が勧告・命令権限を行使するが、主務大臣が行使する場合には第三者機関から意見聴取ないし協議する方法、③主務大臣と第三者機関が単独で勧告・命令権限を行使し、互いに通知する方法の３つの選択肢がある。これらの類型は、個人情報保護施行令の１３条１項が「個人情報取扱事業者が行う個人情報の取扱いについて、主務大臣が２以上あるときは…（中略）…主務大臣の権限は、各主務大臣がそれぞれ単独に行使することを妨げない」と規定し、１３条２項が「前項の規定によりその権限を単独に行使した主務大臣は、速やかに、その結果を他の主務大臣に通知する」と規定していることを参考として作られたものであり、論者は②と③の種類の使い分けが適切であると解している²³⁰。このように、特定個人情報保護制度においても主務大臣制を廃するのではなく、必要に応じて両者を連携させるべきであるとの見解が有力に主張されている。

前述の通り、法的にも事実的にも性質の異なる個人番号と個人情報を組み合わせて構成する「特定個人情報」という法概念には賛同できないものの、個人情報一般を対象とする第三者機関を設立するにあたり、特定個人情報保護委員会と主務大臣の関係に関する前述の議論は参考に値する。各事業における個人情報の取扱いを監督するには、個人情報の保護と事業の円滑な運営のバランスを取らなければならない。したがって、各事業の実態を把握している主務大臣と、個人情報保護について高い専門性を有する第三者機関が連携しながら指導・助言、勧告・命令といった権限を行使するのが妥当であろう。

²²⁸宇賀・前掲注（２１２）７１頁。

²²⁹宍戸常寿「パーソナルデータに関する第三者機関について」（２０１３年１０月２９日に開催された第３回パーソナルデータに関する検討会における配布資料２）

<http://www.kantei.go.jp/jp/singi/it2/pd/dai3/siryoku2.pdf>.

²³⁰宍戸・前掲注（２２９）

第3款 第三者機関による金銭制裁の可能性

特定個人情報保護委員会は将来的に個人情報一般について監督等を行う機関へと移行する可能性があり、主務大臣制よりも広範な権限を付与されているものの、違反に対して金銭制裁を科す権限までは与えられていない。イギリス・フランス・ドイツの第三者機関には金銭制裁（または過料）の権限があり、情報についての高い専門性と相俟って違反に対する抑止力となっている。特に、フランスでは裁判所による罰金刑よりも第三者機関である CNIL による金銭制裁の方が情報処理者にとって脅威となっていることは第4章で述べたとおりである。日本の個人情報保護の第三者機関に対して、このような金銭制裁権を与えることは可能だろうか。

第三者機関が何らかの違反行為に対して金銭制裁を科す例として、独占禁止法違反事件における公正取引委員会による課徴金納付命令が挙げられる。公正取引委員会は内閣府の外局に位置し、独立して職務を行う「三条委員会」として位置付けられているという点で、特定個人情報保護委員会と同様である。公正取引委員会は課徴金納付命令（7条の2）と排除措置命令（7条）を行政制裁として行うことができるが、違反行為に対して実際に処分を下すか否かの判断は委員会の裁量に委ねられているので、一部の事業者だけに制裁を課したり、制裁を課す対象行為を限定したりすることが可能である²³¹。このことは、特定個人情報保護委員会が違反に対して措置等の命令をするか否かの裁量を有していることと同様である。

このように、公正取引委員会と特定個人情報保護委員会は独立性と裁量性という点で類似しており、特定個人情報保護委員会は将来的に個人情報一般に関する第三者機関に発展することが法律上予想されているので、個人情報一般を対象とする第三者機関にも、独立性・専門性・裁量性という性質を継承させることができる。そこで、個人情報一般を取り扱う第三者機関に対して金銭制裁権を付与することができるか否かという問題を考察する前提として、公正取引委員会による課徴金納付命令という行政制裁が法的にはどのように位置づけられているのかを確認する。

当初の独占禁止法では、不当な取引制限行為に対して排除措置命令と刑罰（89条）で対処していたが、排除措置命令を受けたとしても違反事業者は将来に向かって違反行為をやめれば済むので、違反行為による利得はそのまま違反事業者の手元に残ることから、課徴金制度が導入された²³²。課徴金の金額は、違反行為期間中における当該商品等の売上額に一定率（算定率）をかけた額の2分の1であったが、平成17年と平成21年の法改正によって算定率が引き上げられた。そして、違反行為を反復した場合（7条の2第7項）や違反行為において主導的役割を果たした場合（7条の2第8項）には算定率を上乗せす

²³¹矢吹公敏「独占禁止法違反事件における審査・審判手続と課徴金制度の将来像」法律時報85巻12号（2013年）47頁。

²³²山本雅昭「諸制裁の性質—刑法の視点から」法律時報85巻12号（2013年）15頁。

ることで課徴金額が引き上げられることとなった。この法改正により、違反事業者が同一事件について課徴金と罰金を併科された場合には課徴金額から罰金額の2分の1に相当する金額が控除されることが制度化された（7条の2第19項）。課徴金と罰金の併科が二重処罰にあたるのではないかという批判を受けて導入された調整方法である。

刑罰としての罰金と課徴金（金銭制裁）の関係については第2項で改めて検討するが、課徴金はあくまでも行政制裁であって、行政罰（刑罰）ではない。刑罰ではない以上、行政機関は独自の裁量で金銭制裁を科することが可能であり、公正取引委員会と同様に、個人情報一般に関する独立の第三者機関も、一定の違反に対して金銭制裁を科することに法的な問題はない。そして、課徴金（金銭制裁）が刑罰ではないことから、同一の違反行為に対して課徴金と罰金を併科したとしても、「二重処罰」には該当しないはずである²³³。実際に、課徴金と罰金の金額を調整する独占禁止法7条の2の第19項が新設される前の判例では、「一定のカルテルによる経済的利得を国が徴収し、違反行為者がそれを保持し得ないようにすることによって、社会的公正を確保するとともに、違反行為の抑止を図り、カルテル禁止規定の実効性を確保するために執られる行政上の措置」が課徴金であるとして、カルテルの反社会性や反道徳性に対する制裁として科される刑罰とは趣旨・目的・手続等を異にするので、併科は二重処罰にあたらないと判断されている²³⁴。

しかし、併科することが「二重処罰」にあたらないとしても、併科することに積極的な意義があるか否かは別の問題である。併科の問題については第2項で検討する。

また、公正取引委員会では、制裁金額については違反による売り上げを基準として一定割合を乗じた金額を課徴金として義務的に課する制度になっているので、事件ごとの特徴を考慮した上で妥当な金額を算定するのが困難となっている²³⁵。個人情報侵害行為から発生する結果の重大性や行為態様の悪質性といった、事案ごとの個別具体的な事情を考慮しなければ、妥当な制裁金額を算定することはできない。したがって、制裁金の上限を設けた上で、上限を超えない範囲で個人情報保護の第三者機関が金額を自由に判断して決定するという方法を採用するのが望ましい。

第2項 刑事規制の可能性

第3章から第5章までで扱ってきたイギリス・フランス・ドイツの個人情報保護法制では、独立した第三者機関による金銭制裁を含む監督と共に、個人情報の侵害行為を直接処罰する規定が置かれている。本項では、第3章から第5章までで得られた刑罰規定についての知見に基づき、日本の個人情報保護法制において、どのような刑罰規定を設けるべきかということを考察する。

²³³佐伯仁志『制裁論』（有斐閣・2009年）115頁以下（初出は「二重処罰の禁止について」『刑事法学の現代的状況 内藤謙先生古稀祝賀』（1994年）275頁以下）。

²³⁴東京高判平成5年5月21日高刑集46巻2号108頁など。

²³⁵矢吹・前掲注（231）50頁。

第1款 イギリス・フランス・ドイツの刑罰規定の特徴

まず、イギリス1998年データ保護法55条1項では、データ管理者の同意なく故意または無謀によって、①個人データもしくは個人データに含まれる情報を取得もしくは開示し、または②個人データに含まれる情報について他の者に開示を斡旋してはならないと規定されている。この他に、55条4項では、1項に違反して個人データを売却する行為が処罰の対象となり、5項では1項に違反して取得した個人データの売却を申し出る行為と、売却を申し出た後に1項に違反して個人データを取得する行為が処罰の対象となっている。4項と5項の行為は1項に違反することを前提としているので、いずれも故意または無謀によって行うことが条件である。

このように、イギリスでは不正取得から売却まで、幅広い行為が直接的な処罰の対象となっているものの、イギリスの個人情報保護の第三者機関である情報コミッショナーは、報告書「プライバシーの価値とは何か？」において、55条の規定に拘禁刑が設けられていないことを批判している。イギリスでは、なりすましによって情報を入手するブラッキングや、私立探偵を用いた不正な情報収集が問題となっており、報告書ではこのような情報の不正収集等に有効に対処するためには、現行の罰金刑では不十分であり、拘禁刑を設けるべきであることが主張されている。フランス刑法にも個人データの不正収集等を処罰する規定があり、ドイツには過料規定と刑罰規定があるものの、実際に刑罰が用いられるケースは少なく、刑罰に対して慎重な態度が採られているのとは異なり、イギリスでは厳罰化に対して積極的な主張がなされていた。このように刑罰に対する考え方が異なるのは、フランスのCNILには金銭制裁権限があり、ドイツの民間機関に対しては監督官庁が違反に対して過料を科すことができるのに対して、報告書が出された段階ではイギリスの情報コミッショナーには違反に対して金銭制裁を科す権限がなかったからではないだろうか。55条とは別に、情報コミッショナーは、データ管理者がデータ保護原則に違反している場合には通知を出すことによって是正措置を命じたり、データの取り扱いの中止を命じたりすることができるが、この通知を無視した場合には金銭制裁ではなく刑罰が予定されている。このように、情報侵害に対して一定程度の抑止力のあるものが刑罰のみであるという状況であれば、刑罰に対する期待が高まり、厳罰化が主張されるのは自然なことといえる。報告書が公表された後の2010年4月から、データ管理者によるデータ保護原則の違反に対して制裁金を科す権限が情報コミッショナーに付与された。制裁金の制度が導入されてから日が浅いので、制裁金実務に関する資料は少ないものの、情報コミッショナーの年次報告書によれば、制裁金は重大な違反を対象としており、制裁金の対象となるケースの多くはセンシティブデータに関する違反の事例である。対象となるのが一般個人ではなくデータ管理者であるとはいえ、データ管理者による不正なデータの取り扱い一般に対して制裁金を科す権限が付与されたということになれば、刑罰に対して過大な期待をする必要もなくなるので、今後のイギリスの個人情報保護における制裁金制度の重要性が高まるものと思われる。

続いて、フランスでは、個人情報の侵害を処罰する規定が刑法典に多く規定されている。最も基本的な刑罰規定は、詐欺的あるいは不誠実、不正な手段で個人情報を収集する行為は処罰の対象となるというものである（226-18条）。その他には、本人の反対にもかかわらず、市場調査等のために個人情報を処理するなどの行為（226-18-1条）、利害関係者の明示的な同意なしに、人種的または民族的出自などのセンシティブ情報を入力または保存する行為（226-19条）、本人への敬意や私生活の内奥を侵害するような情報を収集した上で、本人の許可なく無資格の第三者に提供する行為（226-22条）が処罰の対象となる。イギリスデータ保護法55条と比較すると、フランス刑法における個人情報に対する犯罪は、情報の性質に着目した規定が多い。法定刑は同一であるものの、センシティブ情報や「本人の敬意や私生活の内奥」にかかわる情報に対する独立した犯罪規定を有しているのはフランスの特徴といえる。問題となった個人情報の内容によっては、226-19条のセンシティブ情報に対する犯罪と226-22条の「敬意や私生活の内奥」に関わる情報に対する犯罪の両方が成立したり、226-22条の犯罪と刑法226-13条における職業上の守秘義務違反の罪や、1881年出版自由法29条の名誉毀損罪の両方が成立したりするという指摘が判例・学説からなされている。このように別個の規定が設けられているということから、フランス刑法においては名誉、秘密、個人情報が異なる法的利益として理解されていることがわかる。このように、フランス刑法では個人情報関係の多彩な刑罰規定が設けられ、様々なケースに対応可能なものになっている。

そしてドイツでは、連邦データ保護法と州のデータ保護法によって個人情報が保護されている。連邦データ保護法43条では個人データの取り扱いについての単純な手続違反と、一般的にはアクセスできない個人データを、故意または過失により無権限で収集、処理、呼び出し等する行為が秩序違反を構成し、過料の対象となる一方で、これらの秩序違反行為を対価を得て、また自己または他人の利益を図るために、または他人を害することを意図して行った場合には自由刑または罰金刑が科される。ドイツの各州にデータ保護法が設けられており、過料規定のみが設けられている州や刑罰規定のみが設けられている州もあるが、両方設けられている州では個人データを不正に収集、提供、処理等する行為が秩序違反を構成し、これらの行為を対価を得て、自己または他人の利益のために、または他害のために行う場合に刑罰の対象となる。このように、ドイツの連邦と州では、個人データの不正な取り扱いについては原則的に過料が用いられ、その行為の中でも特に悪質なものに限って刑罰の対象としており、個人データの不正収集や提供などの行為を幅広く刑罰の対象とするイギリス・フランスとは異なっている。

また、イギリスとドイツはフランスとは異なり、センシティブ情報やそれに類する性質の情報に対する別個の犯罪類型を設けていない。センシティブ情報については、イギリス・フランス・ドイツともに一般的な個人情報よりも厳格な取り扱い要件を設けているが、本人の明示的な同意がある場合というもの以外にも、情報が取り扱われ得る状況に応じて多くの例外が設けられているという点で共通している。刑法226-19条と226-22

条の犯罪が別個に設けられているフランスはともかく、別個の犯罪規定のないイギリス・ドイツでは、このように例外を多く認めることによってセンシティブ情報という法概念の意味が希薄化している。

このように、イギリス・フランス・ドイツには個人情報の侵害行為を直接処罰する規定が設けられているが、客体となる情報の性質や主観的要件にも相違があり、日本法における妥当な刑罰規定の在り方を検討するにあたって参考に値する。

第2款 イギリス・フランス・ドイツにおける第三者機関の実務の特徴

前款では、イギリス・フランス・ドイツにおける刑罰規定の特徴と、それぞれの規定の相違について整理した。これら三国では、刑罰規定のみならず第三者機関による監督が重要な役割を果たしており、この2つが協同することで個人情報の保護が図られているといっている。第三者機関の性質と実務については前節でも述べたが、日本法において刑罰規定を新設するにあたっては第三者機関による実務の在り方も考慮する必要があるので、ここで改めて述べることにする。

まず、第三者機関は情報保護についての高い専門性を有し、独立して監督業務を行う。監督業務には指導・助言、立入検査といったものや、警告・命令（イギリスでは各種通知）、金銭制裁などがある。イギリスは金銭制裁の制度が導入されて間もないが、違反に対する予防効果を期待して設けられた制度のようである。そして、フランスの CNIL も金銭制裁を行う権限を有し、ドイツでは監督官庁が民間機関について過料を下す権限を有しているが、実際に金銭制裁や過料が下されるケースは少ない。なぜなら、フランスでは CNIL が金銭制裁を行うまでもなく、催告や警告を行えばそれに従うケースが多く、ドイツにおいても多くの企業が監督官庁の実務に協力的であり、指導や助言等がなされればそれに従うことが一般的だからである。CNIL や監督官庁の指示に従わないといった、限られた悪質なケースが金銭制裁や過料の対象となる。このように、広範な権限を有する第三者機関の独立性と専門性は企業等が第三者機関の実務に従う根拠となり、刑罰以前に金銭制裁の存在することは刑罰の発動を控えさせることになる。イギリス・フランス・ドイツにおける個人情報に関する刑罰（過料）規定は幅広い行為態様をカバーしているが、結果的にはその多くが実際に用いられることなく、「象徴規定」となっているものと思われる。

第3款 妥当な刑罰規定の在り方、金銭制裁と刑罰の役割分担

第1款と第2款で述べたように、イギリス・フランス・ドイツでは、多くの刑罰（過料）規定が存在するものの、第三者機関による金銭制裁を含めた監督が功を奏しているので、実際には用いられる機会が少ない。このことから、日本法において個人情報に対する刑罰規定を設けるに際しても、多くの行為態様をカバーする必要はなく、悪質な行為のみを刑罰で禁止すれば足りるのではないだろうか。

（１）刑法的保護の対象となる客体

本章第１節では、プライバシーを「自己情報コントロール権」ではなく、「社会的評価からの自由」と解することを述べた。前科前歴・健康状態に関する情報、信用情報といったものは、それが探知の対象となれば「社会的評価」が左右され得るので、保護の対象となる。プライバシー権を「社会的評価からの自由」であると解する刑法学説には、個人情報全般を対象とする直接罰方式の刑罰を設けるのではなく、個人情報の中でも特に保護の必要性が高いセンシティブ情報に関して、直接罰方式を含めた厚い刑法的保護を導入することを検討すべきであると主張するものもある²³⁶。しかし、氏名・住所・電話番号といった、それ自体では社会的評価を左右することはない、センシティブではない個人情報ではあっても、利用方法によっては個人の生活に不利益が生じることが考えられるので、こちらも保護の対象となる。このように、保護の対象となる個人情報は２種類に分けられるが、情報としての性質が異なるので、犯罪を構成する要件も異なったものとするのが望ましい。イギリス・フランス・ドイツの個人情報保護法制では、「センシティブ情報」を一般の個人情報より厳重な保護を要するものとして区別しつつも、センシティブ情報の取扱いを認めるための例外を多く設け、フランス以外は「センシティブ情報」もそれ以外の個人情報も同一の犯罪類型の客体としているが、「センシティブ情報」という法概念の意義が希薄化している点で妥当ではない。

（２）客観的要件

次に、具体的な刑罰規定の検討を行う。イギリス・フランス・ドイツの個人情報保護法制では、個人情報の不正収集、開示、売却、提供などが刑罰（ドイツでは主に過料）の対象とされ、日本においても情報の漏洩や、正当な権限のある者を装って情報を聞き出す行為が問題となっている。このように、個人情報を侵害する行為態様としては、窃取や欺罔による取得という財産犯型の類型と共に、それを第三者に知らせるといふ名誉毀損罪・秘密漏示罪型の類型が考えられる。したがって、「社会的評価」を左右し得る性質の個人情報であれば、それを本人の同意なく、または欺罔によって取得、開示、収集、漏洩、売買する行為は処罰の対象となると考えられる。

一方、それ以外の住所・生年月日などの基本的な個人情報の場合は、そのような行為がなされただけでは処罰の対象とはならない。第３章で述べたように、イギリスでは、ある人物がイギリスのとある地域に住んでいるという情報を他人に伝えた者が、正確な住所まで知らせなかったにもかかわらずデータ保護法違反で有罪になったという判例があるが、「個人情報」の範囲の解釈如何によって処罰範囲が不当に拡張される結果を生むだろう。

²³⁶佐伯・前掲注（８）２０５頁。また、西田典之「個人情報と刑事罰」ジュリスト１１４４号（１９９８年）５７～６１頁も、個人情報プライバシーに属する情報であり、割賦販売法や貸金業の規制等に関する法律によって、消費者のあずかり知らないところでやり取りされ、消費者は自己防衛ができない情報であるので、刑法的保護に値すると述べている。

このような基本的な個人情報是不当に取り扱われたことによって、望まない電話やメールが頻繁に送られたり、架空請求の対象とされたりといった、実際に個人の生活に不利益が生じるという結果が発生して初めて刑罰による保護の対象となる。つまり、「社会的評価」に関する個人情報に対する犯罪は抽象的危険犯的なものである一方で、それ以外の個人情報に対する犯罪は侵害犯的な構成となる。

また、犯罪の主体も重要な問題である。イギリスデータ保護法 55 条では、個人データの不正収集等が処罰の対象となる。条文の主語は‘a person’となっていることと、「データ管理者の同意を得ることなく」という文言があることから、誰もが行為主体となり得るといえる。フランス刑法の条文の文言は、「〇〇する行為は処罰される」という形式となっている。宣伝目的で個人データを処理する刑法 226-18-1 条は情報の取扱を業務とする主体を想定する規定であると思われるが、不誠実・詐欺的・不正な手段で個人データを収集する刑法 226-18 条の行為は業務者や情報処理責任者でなくとも、一般個人によっても行われ得る犯罪類型であろう。そしてドイツ連邦データ保護法 43 条 2 項では「権限なく」個人データを収集等する行為が過料の対象となり、このような秩序違反行為に更なる主観的要件が追加されたのが 44 条の刑罰規定である。「権限なく」という文言から、データを取り扱う業務者ではない一般個人も対象となっていることがわかる。

これに対して、日本の現行個人情報保護法では、「個人情報取扱事業者」に対して個人情報保護のための様々な義務を付与した上で、主務大臣の命令に反した場合に刑罰の対象となる。つまり、刑罰の主体となるのは個人情報取扱事業者のみであり、一般の個人は対象外である。しかし、権限のない一般の個人であっても、情報を不正に取り扱った場合の被害は無視できるものではなく、主体から一般個人を排除する理由はないだろう。また、個人情報保護法制定前の個人情報保護法制化専門委員会における刑罰に関する議論においても、個人情報取扱事業者のみならず、一般個人も罰則の対象としてよいとする意見が出されていた。一般個人による行為による法益侵害の方が軽微であると断言することはできないので、犯罪の主体を一般個人にまで拡張することに問題はないと思われる。

(3) 主観的要件

(2) で検討したように、社会的評価に関する情報と、それ以外の情報では犯罪となる行為態様が異なるが、主観的要件も問題となる。イギリスでは、故意または無謀による個人情報の不正取得等が犯罪となり、フランスでは原則的に故意犯のみが処罰の対象となる一方で、「本人の敬意や私生活の内奥」を侵害するような個人情報の場合は故意のみならず軽率または怠慢による行為も処罰され得る。「軽率または怠慢」は、認識ある過失と認識なき過失を意味しており、その意味では他の犯罪類型よりも処罰範囲が拡大されている。そしてドイツでは、秩序違反行為を対価を得て、または自己や他人の利益のために、あるいは他害のために行う場合のみを処罰の対象としており、主観的要件によって処罰範囲を限定する。個人情報に対する犯罪における主観的要件についての考えは三国間で相違がある

が、日本法の枠組においてはどのような主観的要件を設けるのが望ましいのだろうか。

第一に、金銭制裁や過料であれば金額の大小にかかわらず前科とはならないのに対して、刑罰であれば罰金額や懲役・禁錮の年数にかかわらず前科となり、スティグマとなることから、刑罰の発動は慎重に行われなければならない。刑罰は可能な限り謙抑的でなければならないことから、過失犯よりも非難の程度の強い故意犯のみが処罰の対象となるのが原則である。過失犯を処罰するには、当該犯罪における保護法益が重要なものでなければならない。イギリス刑法では、結果発生危険性を認識している「無謀」と、危険性を認識していない「不注意 (negligence)」が区別され、それが条文の文言にも反映されている。

一方、日本では通常の「過失」と「重大な過失」が区別され、「重大な過失」による行為は法定刑が加重されているが、日本の現行刑法典では重過失失火罪、重過失激発物破裂罪（117条の2後段）、重過失致死傷罪（211条1項後段）という3つの犯罪類型にとどまっている。判例では重大な過失は、「注意義務違反の程度が著しい場合をいい、発生した結果の重大性、結果発生の可能性が大であったことは必ずしも必要としない」²³⁷と解されており、結果そのものよりも行為に対する非難が大きいことが「重大な過失」の意義であると思われる。イギリスに倣い、故意犯と重大な過失による行為を処罰の対象とするという方法も考えられるが、日本の現行法で重過失を規定しているのは、前述の重過失失火罪などといった、生命や身体に直結し得る犯罪類型のみである²³⁸。一方、個人情報とは「社会的評価からの自由」「生活への不当な介入・干渉からの自由」という精神的な自由の利益として保護されるものである。その意味では名誉や秘密と同列であり、そのような利益に対する「重大な過失」による行為まで処罰範囲に含めるのは均衡を失するだろう。したがって、個人情報の性質が「社会的評価」を左右し得るか否かにかかわらず、故意犯のみを処罰の対象とするのが妥当である。

（４）刑罰と非刑罰的金銭制裁の使い分け

このように、刑罰の対象となる行為は故意犯に限定される。しかし、過失による個人情報の侵害行為には何らの法的責任も問われないと解するのは妥当だろうか。企業が過失によって個人情報を大量に漏洩する例も多く、そのような行為による生活への介入・干渉という結果も無視できるものではない。よって、過失による情報漏洩や開示といった行為は

²³⁷東京高判昭和57年8月10日刑月14巻7・8号603頁。

²³⁸刑法230条の2は過失名誉毀損罪について規定しているとする見解として、西田・前掲注（17）119～120頁、山口・前掲注（11）146～147頁、佐伯仁志「名誉とプライバシーに対する罪」芝原邦爾ほか（編）『刑法理論の現代的展開 各論』（日本評論社・1996年）85頁がある。しかし、故意犯と過失犯を同一の法定刑で定めるというのは考え難く、230条の2は真実性の証明に失敗した場合の法的責任について定めた規定であることから、過失名誉毀損罪という理解は妥当ではない。したがって、現行刑法において過失行為が処罰の対象となるのは過失致死傷罪、失火罪、過失激発物破裂罪、過失往来危険罪、過失建造物等浸害罪といった、やはり生命・身体に直接の被害を及ぼし得る犯罪類型に限定される。

刑罰の対象とはならないとしても、独立の第三者機関による非刑罰的な金銭制裁²³⁹の対象となるべきである。故意による犯罪については、個人情報取扱者と一般個人の両方が行為主体になり得るということを（２）で論じたが、非刑罰的な金銭制裁の対象も個人情報取扱者に限定せず、一般個人まで拡張するのが妥当であろうか。

現在の日本では、独占禁止法 7 条の 2 および 20 条の 2 から 20 条の 6 までの条文により、事業者や事業団体が不正な取引制限などの違反行為を行った場合、公正取引委員会が当該違反事業者等に対して課徴金の納付を命じることが規定されている。このように、公正取引委員会による課徴金の対象となるのは事業者等に限定されているが、そもそも独占禁止法の目的は、事業者間の公正な自由競争を確保することにより、消費者の利益を保護することであるので、一般個人による違反を観念し難いということがその根拠であろう。

一方、個人情報の過失による漏洩等の行為は個人情報取扱事業者のみならず、一般個人によるものも観念し得る。しかし、フランスの CNIL のような個人情報に関する第三者機関の業務は、個人情報の適正な取り扱いが行われているか否かを監督することであるので、個人情報取扱者による違反行為が制裁金の対象になるのは妥当であるとしても、個人情報の取り扱いを業務としない一般個人にまで対象を広げるのは制度趣旨に反するのではないだろうか。一般個人が過失で情報を漏洩するような行為によって発生する被害は少ないとは必ずしも言えないが、一般個人の過失行為に対して第三者機関が制裁を加えることを正当化する根拠は乏しいだろう。

そして、故意行為は独立第三者機関の非刑罰的な金銭制裁や主務大臣の命令を経ず刑罰の対象にすることで、刑罰と金銭制裁の使い分けをするのが望ましいのではないだろうか。現行の個人情報保護法における「主務大臣の命令違反」に対する罰則は、包括的・抽象的にすぎるので、一口に「命令違反」といってもどの程度の強い違反行為であれば処罰の対象となるのかが不明確であるが、この間接罰規定に替えて、前述の故意行為を処罰対象とすることにより、刑罰の明確性を担保することが可能となる。そして、この方法であれば、刑罰と非刑罰的な金銭制裁の併科が「二重処罰」に該当するのではないかという問題や、併科する場合には罰金額と制裁金額のバランスをどのように取ればよいのかといった困難な問題を検討する必要はなくなる。多くの行為を過料の対象としているドイツを除き、イギリス・フランスでは刑罰の対象となる行為を広く規定した上で、実際には刑罰ではなく非刑罰的な金銭制裁やそれより軽い警告や通知等を頻繁に用いているので、結果的に刑罰の濫用が控えられている。しかし、このような現象はあくまでも結果的なものにすぎず、例えば実際には用いられる機会が多くなるとも、幅広い行為をカバーする刑罰規定が存在することにより、刑罰のリスクに対する国民の必要以上の脅威となっていると考えられる。本論文で考察したように、刑罰を加えるに値する悪質な行為に限定して刑罰規定を設けるこ

²³⁹ 「金銭制裁」という用語には罰金や科料という刑罰も含まれるが、「課徴金」という用語は独占禁止法・金融証券取引法に独自の用語であるので、ここでは「非刑罰的な金銭制裁」という用語を用いる。

とにより、刑罰の謙抑性を名実ともに遵守することが可能となるのではないだろうか。

第3節 小括

本章では、個人情報が刑法における保護法益たり得るかということと、個人情報の侵害行為に対する妥当な規制方法は何かということについて検討を進めてきた。

まず、個人情報は現行刑法における名誉、秘密、財産といった保護法益には包含され得ない。個人情報には、それが漏洩等されれば当該個人の社会的評価の低下につながり得る性質のものもあるが、氏名・住所・生年月日といった、当該個人の同一性に関する基本的な性質のものもあることから、「名誉」に包含することはできない。続いて、秘密漏示罪における「秘密」は、医師や弁護士等の職業に就いている（就いていた）者の守秘義務を前提とするものである一方で、個人情報は守秘義務の有無とは切り離された概念であるので、「秘密」にも包含することはできない。そして、有体物に化体されていない情報の「非移転性」「非喪失性」という性質から、情報それ自体を財産罪によって保護することも困難である。以上のことから、個人情報という利益は従来の刑法で保護されてきた伝統的な法益には包含されない、独立した利益であるといえる。

続いて、個人情報を刑法における独自の保護法益として位置付けることが可能か否かということについて検討した。個人情報という、科学技術の発展に伴ってその重要性が主張される新しい利益の保護法益化を論じるにあたって、本章では環境という利益の法益性をめぐる議論をその契機とした。環境はその範囲の曖昧さ故に、刑法における保護法益として正面から認めてよいものか否かが議論されてきたが、環境権が憲法の領域で認められていることから、現在では環境は保護法益としての地位を有している。環境権という利益が憲法に裏付けられていることと併せて、憲法上の価値から法益概念を導出するドイツと日本の法益論の学説から、憲法の領域で保護され得る権利・利益には刑法における法益性を認めてもよいという結論を得た。

そこで、個人情報は憲法によって保護され得るという前提に立ち、憲法学説が個人情報をどのように理解しているかという議論から、個人情報が保護の対象となり得る根拠について分析した。憲法学説では個人情報との関連において、プライバシー権を「自己情報コントロール権」として理解するものが有力に主張されているが、本論文ではこの見解を採らない。そもそも、情報の流れは本来コントロールできないものであり、情報が他者の知るところとなるか否かを支配することはできないからである。情報をコントロールする権利が保護の対象となるということは、一度他者に探知された情報は保護されないということになり、不当である。したがって、本論文では「自己情報コントロール権」ではなく、「社会的評価からの自由」という側面から個人情報の保護を根拠づける。プライバシーを「社会的評価からの自由」であると解すれば、名誉とプライバシーを明確に区別することが可能であり、自己情報コントロール権説の弱点も克服することができる。

以上を前提として、「社会的評価からの自由」がプライバシーの利益であるとすれば、

どのような個人情報が保護の対象となるのかということが問題となる。まず、前科前歴・健康状態・経済状態などの情報は「社会的評価からの自由」にかかわる情報であるので、それらを収集・探知等することは不当なプライバシー侵害となる。その一方で、氏名・住所・生年月日などが収集・探知されたとしても、それ自体として社会的評価が変化するとは考え難いが、これらの情報が売買の対象となり、本人に望まない勧誘電話が頻繁にかかってくるような事態になれば、これは個人の生活への不当な介入・干渉であろう。したがって、「社会的評価からの自由」に関わる個人情報とは根拠が異なるものの、住所等の基本的な個人情報も保護法益として認められ得る。このように、刑法における保護の対象となり得る個人情報は2種類に分けられ、「社会的評価からの自由」または生活に対する不当な干渉・介入からの自由が保護法益として観念されるので、個人情報に対する侵害行為は精神的自由に対する罪として位置付けられる。

本章第1節では、個人情報が刑法における保護法益として認められ得ることを明らかにした。これを前提として第2節では、個人情報の保護のための妥当な規制のあり方について検討を行った。

第2節第1項では、個人情報の取扱いを監督する独立の第三者機関を設けることの可能性について分析した。イギリス・フランス・ドイツにはこのような独立の第三者機関があり、第三者機関が個人情報保護法の違反に対して是正命令を行ったり、場合によっては金銭制裁を科したりしている。第三者機関は情報保護に関する高い専門性と広範な権限のゆえに、個人情報保護法違反に対する抑止力となっており、その結果として刑罰が用いられるケースが少なくなっている。このような第三者機関を日本に設けることができれば、刑罰の濫用にわたらずに個人情報を保護することが可能になると考えられるからである。

現在の日本には個人情報一般に対する第三者機関は存在しないものの、2013年5月に成立した共通番号法の下で、特定個人情報保護委員会という第三者機関が設けられた。共通番号法が「個人番号」と「個人情報」という法的にも事実的にも性質の異なるものを組み合わせてひとつの法概念としていることには賛同できないが、特定個人情報保護委員会は将来的には個人情報一般を取り扱う第三者機関となる可能性のあることが共通番号法附則に定められている。そこで、本章第2節第1項では、特定個人情報保護委員会の構成や権限の内容を参照しながら、第三者機関の在り方を検討した。

特定個人情報保護委員会は、独立して職務を行う機関であり、個人情報保護などの専門的知見のある者で構成されているという点で、イギリス等の第三者機関と類似している。この独立性・中立性・専門性に基づいて、特定個人情報保護の取り扱いについて指導・助言、勧告・命令、報告・資料要求、立入検査といった職務を行う権限を有する。特定個人情報保護委員会の制度が導入された後も、個人情報保護法における主務大臣制は廃止されず、委員会と主務大臣が必要に応じて連携することが予定される。なぜなら、主務大臣は各事業の実態を把握しており、事業の円滑な運営を損なわずに情報の保護を行うためには主務大臣の存在が必要だからである。

新しく設けられた特定個人情報保護委員会は広範な権限を有しているが、違反に対して非刑罰的金銭制裁を科す権限までは有していない。イギリス等の第三者機関は、立入検査や是正命令といった職務に加えて、違反に対して非刑罰的金銭制裁を科す権限も有しており、特にフランスでは裁判所の罰金刑よりも CNIL の非刑罰的金銭制裁の方が脅威になっていることから、日本の個人情報保護のための第三者機関にも非刑罰的金銭制裁を科す権限を付与するのが望ましいのではないかということを議論した。第三者機関が非刑罰的金銭制裁を科す例として、独占禁止法における公正取引委員会を参考にしつつ、機関の独立性・中立性・専門性という点で公正取引委員会と類似している個人情報保護の第三者機関であれば、非刑罰的金銭制裁を科す権限を付与しても差し支えない。また、非刑罰的金銭制裁と刑罰の併科は「二重処罰」にはあたらないが、併科することに積極的な意義があるか否かは別問題である。

そして、第2節第2項では、イギリス・フランス・ドイツの刑罰規定についての知見に基づき、日本の個人情報保護法制において、どのような刑罰規定を設けるべきかということについて考察した。まず、イギリスでは、データ保護原則に違反したデータ管理者に対して制裁金を科す権限が情報コミッショナーに付与される前までは、情報コミッショナーは刑罰に対して過大な期待を有し、厳罰化を主張していたが、2010年に制裁金制度が設けられてからは、イギリスの個人情報保護実務における刑罰の位置づけは変化するものと考えられる。フランスでは、個人情報に対する犯罪は刑法典に規定されており、イギリス・ドイツとは異なり、センシティブ情報等の特別な性質の情報に対する罪が別個に設けられている。ドイツでは、データの不正収集などの行為の多くは刑罰ではなく過料の対象となり、これらの行為を対価を得たり、加害目的等で行ったりした場合に初めて刑罰の対象となる。イギリス・フランス・ドイツの刑罰（過料）規定には様々なものがあるが、実際には第三者機関による日常の監督業務や金銭制裁によって問題が解決されることが多く、刑罰は限られた場合にしか用いられない。そこで、日本法において刑罰規定を設ける際にも、悪質な行為のみを処罰の対象とすればよいという問題意識に基づき、具体的な刑罰の在り方を考察した。

まず、「社会的評価」を左右し得る性質の個人情報であれば、本人の同意なく収集、漏洩、開示、売買したり、欺罔による収集といった行為をしたりすること自体が犯罪を構成し得る。一方、「社会的評価」をそれ自体では左右しない氏名・生年月日・住所といった基本的な個人情報の場合は、そのような行為をすることによって、個人の生活に対する不当な介入・干渉が行われるという結果が発生することにより、刑罰の対象となる。

続いて、2つの犯罪類型における主観的要件も問題となる。故意行為のみならず、重過失による行為も処罰対象とすることも考えられたが、日本の現行刑法において重過失行為が規定されているのは失火罪や過失致死傷罪などといった、生命・身体に直結する犯罪類型に限られていることから、個人情報という精神的な自由の利益に対する犯罪の場合に重過失行為を処罰対象とするのは妥当ではないと判断した。よって、本論文では、故意行為

のみを処罰対象とする。

そして、故意行為は非刑罰的金銭制裁を経ずに刑罰の対象となり、過失行為はもっぱら非刑罰的金銭制裁の対象とすることで、刑罰（特に罰金刑）と非刑罰的金銭制裁の併科に関する解決困難な問題を克服することが可能となる。さらに、現行の個人情報保護法における「主務大臣の命令に対する違反」という包括的・抽象的な間接罰規定に替えて、故意の情報侵害行為を具体的に列挙した規定を設けることにより、刑罰の明確性を担保する。

第7章 おわりに

本論文では、個人情報そのものを刑法によって保護することが可能であるか、可能であるとすれば、刑罰の果たす役割はどの範囲までなのかということを考察した。個人情報とその保護の重要性については誰もが首肯するところであるが、妥当な法的保護の在り方についての議論は錯綜している。その背景には、個人情報という新しい利益を法的にどのように位置づけるべきなのかということが先行研究で十分に検討されず、個人情報の重要性の理解も曖昧なものに留まっているという現状があるのではないだろうか。特に、刑罰を科すことによって個人情報を保護するという方法に対しては、「刑罰は最終的な手段でなければならない」という刑法の原則に抵触することを危惧するあまり、これまでの先行研究ではそれほど活発には議論されず、今後の法改正に委ねるという姿勢が貫かれているようである。

確かに、「刑罰の謙抑性」という原則は遵守されなければならない。安易な刑事立法は厳に慎むべきであることは言うまでもない。しかし、個人情報の大量漏洩や、なりすましによる収集、売買といった、個人情報の侵害による生活への被害が実際に発生している以上、このような個人情報侵害を直接的に処罰する規定を設けることを過度に回避するのは妥当ではない。特に悪質な侵害行為に対しては刑罰を発動するのもしやむを得ないだろう。このような問題意識に基づき、本論文では個人情報の侵害を処罰するイギリス・フランス・ドイツの法律を比較対象としつつ、妥当な刑罰規定の在り方について検討した。個人情報保護の手段として、これらの国には刑罰のみならず、独立した第三者機関による非刑罰的金銭制裁を含む監督業務も存在しているので、比較法的考察において刑罰を相対化することによって、刑罰を必要以上に忌避しないと同時に刑罰に偏らない保護の在り方を分析することができた。

比較法的知見に基づき、本論文では個人情報の法益性と、妥当な規制の方法について考察した。現行の個人情報保護法の客体である「個人情報」には、氏名・住所・生年月日といった基本的なものから、健康状態・信用状況・年収といった、他人の知るところとなるのを欲しない性質のものまで広く含まれているので、個人情報の性質に即した妥当な規制を行うことができなくなっている。これに対して、本論文では個人情報を、それが他者に知られることそのものによって「社会的評価からの自由」が侵害され得る性質のものと、不当に扱われることによって生活に対する不当な介入・干渉が行われ得る性質のものに二

分した。前者の情報に対する侵害行為を抽象的危険犯として構成し、後者の情報に対するそれを侵害犯として構成することにより、現行の個人情報保護法に比して緻密な規制が可能になったと思われる。続いて、刑罰の対象となるのを故意犯に限定し、過失犯はもっぱら非刑罰的金銭制裁の対象としたことで、「二重処罰」の問題を回避すると同時に刑罰の謙抑性も維持している。

従来の先行研究では、個人情報の法益性についての議論が不十分であり、刑罰規定を設けることに対してはその濫用が危惧されていた。濫用にわたらない範囲の刑罰規定を検討することの困難性により、刑罰の発動はしばらく見送るという発想になっていたのではないだろうか。このような議論状況は、「個人情報は保護されなければならない」にもかかわらず、「個人情報の侵害に対する有効な法的規制が存在しない」という矛盾を生み出し、それにより、一般市民の側では些細な個人情報であっても、または情報提供が必要な場面であっても過度に秘匿するという「過剰反応」（一般市民の側から見れば「自力救済」とでも言うべき行為であろう）をもたらし、反対に個人情報を悪用しようとする者の側では、刑罰の存在しないことが規範意識の鈍麻につながり、さらに悪質な情報侵害の発生を招くだろう。しかし、本論文における法益論と規制論によれば、刑罰の謙抑性と法益保護のバランスを取りながら、「過剰反応」も個人情報侵害の深刻化も回避することが可能となる。

以上により、本論文は日本の個人情報保護法制における従来の問題点を明らかにしつつ、新しい提言をするものである。本論文では個人情報を対象とした上で、その妥当な規制方法について検討を行ってきたが、営業秘密などの財産的な性質を有する情報の刑罰的保護については今後の研究に委ねる。個人情報と営業秘密は非移転性・非喪失性という点で共通しているが、個人情報が侵害された場合に被害を受けるのが当該個人（または家族）に限定される一方で、営業秘密は社会的法益として位置付けられ、秘密が侵害された場合の波及する範囲が広いという点で異なっている。このように、被害の範囲やそれによる効果の違いにより、妥当な保護の在り方も異なるものとなるだろう。

また、本論文では諸外国において「センシティブ情報」に分類される前科前歴、健康状態、信用情報といった個人情報を「社会的評価を左右し得る情報」として構成し、このような個人情報については本人の同意なく収集・提供等する行為や、欺罔により収集等する行為が可罰的であると解している。そこで、「センシティブ情報」の最たるものとして挙げられるのは遺伝情報である。遺伝情報が他の情報と異なる点として、（１）同じ情報を有する者が存在する可能性はほとんどないということ、（２）生涯を通して情報がほとんど変わらないこと、（３）遺伝情報の持ち主である本人のみならず、本人と遺伝子を共有する家族の人格の基本部分にもかかわる情報であること、（４）本人の肉体的形質、精神的傾向といった様々な情報が含まれており、遺伝情報自体が本人にとって不利益情報となり得ることが指摘されている²⁴⁰。以上の特質から、漏洩等によって遺伝情報が侵害された場合には、

²⁴⁰和田幹彦（編著）『法と遺伝学』（法政大学現代法学研究所・2005年）岩橋健定「個人の遺伝子情報の保護」90頁、只木誠『刑事法学における現代的課題』（中央大学出版会・

本人の「社会的評価からの自由」としてのプライバシーは将来にわたって広範囲に侵害され続ける危険性が高い。一口に「社会的評価を左右し得る個人情報」と言っても遺伝情報と他の個人情報ではレベルに差があることから、「遺伝子例外主義」の考えに立脚した上で遺伝情報保護のための新しい法的規制を設ける必要があるのか、それとも前科前歴や他の医療情報といった、他の「社会的評価を左右し得る個人情報」と同列に扱ってさしつかえないのか、検討の余地がある²⁴¹。営業秘密や遺伝情報などについても、本論文で得られた知見をもとに、検討を進めることとしたい。

2009年) 第2章「予測的な遺伝子テストと法」26頁など。

²⁴¹遺伝情報の法的規制についての先行研究として、甲斐克則「ドイツにおける遺伝情報の法制度」早稲田法学88巻1号(2013年)1~40頁、瀬戸山晃一「遺伝学的情報と法：象徴的機能としての遺伝子差別禁止法」名古屋大学法政論集250号(2013年)393~403頁、山本龍彦『遺伝情報の法理論—憲法的視座の構築と応用』(尚学社・2008年)、甲斐克則(編著)『遺伝情報と法政策』(成文堂・2007年)、實原隆志「遺伝子情報の扱いをめぐる日独の法状況」長崎国際大学論叢8巻(2008年)1~12頁、稲葉一人「遺伝子情報を巡る倫理的・法的諸問題—本人のプライバシー権と第三者の知る権利が衝突する場面を中心として—」医療・生命と倫理・社会Vol.1 No.2(2002年)などがある。