



労働者に対するデジタル技術を活用した監視に関する規制の構築

劉, 子安

(Degree)

博士 (法学)

(Date of Degree)

2024-03-25

(Date of Publication)

2025-03-01

(Resource Type)

doctoral thesis

(Report Number)

甲第8817号

(URL)

<https://hdl.handle.net/20.500.14094/0100490042>

※ 当コンテンツは神戸大学の学術成果です。無断複製・不正使用等を禁じます。著作権法で認められている範囲内で、適切にご利用ください。



博 士 学 位 論 文

労働者に対するデジタル技術を活用した監視に関する規制 の構築

神戸大学大学院法学研究科

専攻: 法学政治学専攻

指導教員: 大内伸哉

学籍番号: 183J002J

氏名: 劉子安

提出年月日: 2024 年 1 月 9 日

論文要旨

使用者には従業員の業務状況を監視する権利があるが、その権利は無制限ではなく、監視の目的や手段などによっては、労働者のプライバシー権ないし人格権を侵害する場合がある。テクノロジーの発展に伴い、監視装置の機能は飛躍的に進化しており、単に従業員の言動を記録するだけでなく、労働者の個人データを網羅的に収集することが可能になっている。しかし、どのような場合に、使用者の監視による労働者のプライバシー権等の侵害が生じるかについては、裁判例上、明確な基準は形成されていない。また、監視の利用に関する従来の裁判例は、プライバシー侵害に関する裁判例とは異なり、監視を情報収集の一態様として捉える意識が希薄である。他方、学説においても、監視の議論に関する議論はまだ十分ではない。労使間の交渉力の格差や、労働者が新たな技術を搭載した監視装置の機能を詳細に理解することが困難であることなどを考慮し、本論文では、上記のような監視装置に対処するためには、労働者の同意を要件とするのではなく、使用者が適正な監視を行えるようにするための判断枠組みを構築する必要があるという結論を得た。

次に、このような判断枠組みをどのように構築するかという問題については、監視の適法性に関する欧州人権裁判所の判例法における判断枠組み（バルブレスク基準）とフランス法における判断枠組みを分析した結果、後者の、裁判所と個人情報保護に精通したデータ保護機関との協力によって構築された判断枠組みは日本にとって示唆に富むものではあるが、日仏の個人情報保護法の構造的相違や、フランスの裁判所が課している事前通知要件は日本の現行法ですでに実現されているとの観点から、フランス法を参考にせず、本論文では、監視の適法性を審査する明確な基準を有する欧州人権裁判所の判例法における判断枠組み（事前通知の有無、私生活に対する侵害の程度、監視を行う正当な理由の有無、代替可能性の有無、監視によって得られた結果の利用の適否、侵入的な性質を有する監視の場合、従業員に適切な保護措置が提供されたかどうかからなるバルブレスク基準）を導入すべきであるという結論を得た（本論文では、これを日本型監視の適法性に関する判断枠組みと呼ぶ）。

しかし、日本型監視の適法性に関する判断枠組みにおける各要件の具体的な内容を明確にしなければ、使用者が適正な監視を行えるようにするための判断枠組みとはいえない。この問題について、監視の利用を含む個人データの処理が複雑で流動的かつ革新的な特性を有する分野であることを踏まえると、

本論文では、新たな技術開発のペースに追いつけない国家規制と、実効性や法的拘束力のない自主規制は適切ではなく、公的機関の関与を前提に、各産業団体が自らの特性を反映し、日本型監視の適法性に関する判断枠組みの各要件の内容を自ら具体的に定める共同規制の手法を利用すべきという結論を得た。

目次

序章	8
I.問題の所在	8
II.論文の構成	13
第1章 日本における問題状況	15
第1節 序説	15
第2節 監視に関する行政解釈と個人情報保護法上の規制	16
第1款 監視に関する行政解釈	16
第2款 監視に関する個人情報保護法上の規定	18
第3款 小括	19
第3節 監視に関する裁判例上の立場と学説上の議論	19
第1款 単純な監視	19
(1) 判例の立場	20
(2) 学説上の議論	24
(3) 小括	26
第2款 機器を用いた監視に関する裁判例と学説上の議論	26
(1) 裁判例の立場	26
(i.) 序説	26
(ii.) 録音機・監視カメラの使用から生じた問題点	27
(a) 録音機の使用に関する問題	27
(b) 監視カメラの問題	28
(iii.) 電子メールとコンピュータの使用から生じる問題	32
(a) 電子メール私用と私的チャットの問題	32
(b) 業務用コンピュータに対する調査の問題	36
(iv.) GPS 機能付き装置による監視	39
(2) 学説上の議論	39
(i.) 全体的状況	39
(ii.) 電子メールの私的利用をめぐる学説上見解の対立	40
(iii.) GPS 使用による監視とテレワークの実施に伴う監視	44
第3款 小括	46
第4節 まとめ	47

第2章 職場における監視の問題に関する欧州人権裁判所の判例法	49
第1節 序説	49
第2節 使用者による監視に関する国際的・地域的文書	50
第1款 国際的法律文書	50
第2款 地域的（ヨーロッパ）法律文書	50
(1) 閣僚委員会の雇用分野に関する勧告	50
(2) 欧州連合（EU）の状況	52
第3節 欧州評議会、欧州人権条約及び欧州人権裁判所の概説	54
第1款 欧州評議会の設立	54
第2款 欧州人権条約の誕生と改革	56
第3款 欧州人権裁判所の構造と判断原則	59
第4款 積極的義務の概念	61
第5款 欧州人権条約8条の定義と運用	64
第6款 小括	65
第4節 監視に関する欧州人権裁判所の判例法の考察	66
第1款 Niemietz v. Germany 事件	66
(1) 学説上の議論	67
第2款 Halford v. United Kingdom 事件	68
(1) 学説上の議論	69
第3款 Copland v. United Kingdom 事件	70
第4款 Köpke v. Germany 事件	71
第5款 Bărbulescu v. Romania 事件	73
(1) 大法院の判断	74
(2) 反対意見	77
(3) 本判決の意義と学説上の議論	78
第6款 López Ribalda et al. v. Spain 事件	79
(1) 大法院の判断	80
(2) 反対意見	82
(3) 学説上の議論	84
第7款 Florindo de Almedia Vasconcelos Gramaxo v. Portugal 事件	85
(1) 反対意見	87
(2) 学説上の議論	88
第5節 まとめ	88

第3章 フランス法における問題状況	90
第1節 序説	90
第2節 使用者の監視に関する法規制の制定	91
第1款 1982年の法改正	91
第2款 1992年の法改正	93
第3款 1992年改正法に関する学説上の議論	97
第4款 小括	99
第3節 監視に関する破毀院の立場と学説上の議論	100
第1款 序説	100
第2款 単純な監視に関する事件	101
(1) 従業員個人用のロッカーの検査	101
(2) 所持品検査	103
(3) 尾行と調査	105
(4) 小括	109
第3款 機器を用いた監視に関する事件	110
(1) 監視カメラに関する規制	110
(i.) 事前通知義務の確立	111
(ii.) 事前通知義務の例外	113
(iii.) 監視カメラの利用目的変更	114
(iv.) CNILの立場	117
(v.) 小括	121
(2) GPS機能付き装置による監視	122
(i.) CNILの立場	122
(ii.) 破毀院の立場	124
(3) IDバッジその他の装置による監視	127
第4節 まとめ	129
第4章 共同規制方式の可能性	130
第1節 序説	130
第1款 規制手段の種類と特徴	131
第2款 共同規制の概念	133
第2節 EUデータ保護法における共同規制の具体化	135
第1款 1995年データ保護指令上の行動規範	135

第2款 GDPR上の行動規範	138
(1) 序説	138
(2) 新たな行動規範の概説	138
(3) 行動規範が批准されるまでの手続	139
(4) 新たな監視機関の認定基準	143
(5) 行動規範の策定に関するインセンティブ規定	146
(6) 学説上の議論	147
第3節 日本における認定個人情報保護団体	149
第1款 認定個人情報保護団体の経緯と趣旨	149
第2款 共同規制の概念に基づく認定個人情報保護団体	151
第3款 GDPRの行動規範との差異	153
第4節 まとめ	154
第5章 監視に関する規制の構築とその手法	156
第1節 議論のまとめ	156
第2節 共同規制の概念を用いた適正な監視を行えるようにするための判 断枠組みの構築	158
第1款 欧州人権裁判所とフランス法上の判断枠組みからの示唆	158
第2款 共同規制方式による規制内容の具体化	160
第3款 労働者の同意と日本型監視の適法性に関する判断枠組みとの関 係	162
結章	165

序章

I.問題の所在

監視という問題を論じるにあたり、ほとんどの欧米の学者は、1949年に刊行されたジョージ・オーウェルのディストピア SF 小説『1984 年』¹における最も有名なセリフである「ビッグ・ブラザーがあなたを見ている (Big brother is watching you)」を引用している²。オーウェルは、ビッグ・ブラザーを全体主義国家による監視・検閲等と指しているが、今日の監視の主体は国家に限らず、「リトル・ブラザー」³である民間企業や個人から、人工知能を搭載した装置による監視まで広がってきた⁴。また、今日の監視の実態としては、町中の至るところに無数の防犯カメラが設置されている状況に加え、監視カメラと比較して存在感が感知されにくい個人のスマートフォンやウェアラブル端末などの装置も一般化してきている。これらの装置によって、個人が監視に置かれる時間的・場所的な制限がなくなり、監視は不断に実施されることが

¹ ジョージ・オーウェル (高橋和久訳) 『一九八四年』 (早川書房, 2012 年) 8 頁。

² 日本の文献としては、砂押以久子「情報化と労働者のプライバシー—フランスの電子メールモニタリングをめぐる法的問題を中心に—」労旬 1535 号 (2002 年) 11 頁がある。外国の文献としては、C. Birsan & L-C Spătaru-Negură, *Workplace Surveillance: big brother is watching you?*, 1 (25) LESIJ (2018), F. Abdurrahimli, *Big Boss is Watching You! The Right to Privacy of Employees in the Context of Workplace Surveillance*, p. 7 (2020), available at <https://ssrn.com/abstract=3740078> などがある。他方で、オーウェルの思想を引用すること自体に疑問があるとの指摘もある。例えば、情報法学者の青柳は、オーウェルが構想した世界における監視の本質は、「共産主義や全体主義という政治体制自体に起因するものであったのであり、『監視』そのものの属性ではなかった」とし、さらに、近代立憲主義に基づいて制定された憲法を有する国家における「監視」を論ずるにあたっては、「オーウェルを引き合いに出すことがそもそもの見当違い」と指摘している。青柳武彦『サイバー監視社会—ユビキタス時代のプライバシー論—』 (廣済堂, 2006 年) 287 頁。

³ 松前恵環「個人によるカメラ監視と米国不法行為法上のプライバシー権の眼形—『ポリオプティコン』の時代におけるプライバシー—」社会情報学研究 16 巻 2 号 (2012 年) 111 頁。

⁴ 岡本裕一郎『哲学と人類ソクラテスからカント, 21 世紀の思想家まで』 (文藝春秋, 2021 年) 32-33 頁。岡本は、AI を搭載した装置による監視を、「モノプティコン」と名付けており、さらにモノプティコンの特徴について、「AI というデジタル情報機器によって、自動的に監視され、記録され、登録されることを示している。こうした収集された情報は、ビッグデータとして利用されたり、データベース化されたりする。監視にしても『モノ (機械) = AI』が担当し、人々からは監視されているという意識がますます希薄になっていく。……監視はデジタル化することによって、すでに人間の手を離れてしまった……人間がモノを使って人間を監視することから、モノが人間を使って人間を監視することへと転換した」と説明している。

可能となった。

労働の世界では、監視は労働の誕生時から存在していたが、かつては労働者の 90%以上は職人や商人の店、田舎の農場に分散しており、人々は互いに労働の状況を監視していた⁵。しかし、18 世紀半ばから行われた産業革命は、多くの人々を農村から工場に呼び寄せた⁶。すなわち、多くの労働者を同時に、同じ場所に集め、共通の業務を遂行させる労働形態を要求するものであった。これによって、産業革命は何世紀にもわたった監視の状況を変革するものとなった⁷。具体的には、工場の大量生産を可能にするために、工場主は軍事訓練のように職工に「規律」を教え、そして労働者の作業の過程を組織的に監視することが必要となった。例えば、明治・大正時代の鉱山や土木工事現場における、労働者が四六時中監視されていた奴隷制に近い飯場制度や納屋制度などの例が挙げられる⁸。このように、管理と監視の組み合わせは、19、20 世紀の生産現場で中心的な様式であった⁹。しかし、1960 年代以降、データバンク社会（情報化社会）の到来を背景としたコンピュータとネットワークの普及により、職場における監視は従来の人間による監視から、次第に機械による監視へと移行した¹⁰。我々は、いまやアルゴリズムによる監視や「バーチャルな監視」の時代に突入している¹¹。今日、AI 技術の進化に伴い、使用者は、より機能が優れた追跡装置、監視カメラ、代謝モニター、ウェアラブ

⁵ H. BOUCHET, La surveillance numérique au travail, Hermès, *La Revue* n°53, 2009, p.85.

⁶ *Ibid.*

⁷ *Ibid.*

⁸ 土工のタコ部屋（監獄部屋とも呼ばれている）や紡績工場の女工など、近代日本の過酷な労働実態については、宮本常一ほか編『日本残酷物語 5』（平凡社、1995 年）109 頁参照。もっとも、製糸女工への直接的にインタビューを通じ、女工の労働実態に関する異なる様相を呈した研究もある。シャルサンドラ「『女工哀史』言説を超えて」ソミオロジ 48 巻 2 号（2003 年）3 頁以下参照。

⁹ ディヴィッド・ライアン（田島泰彦＝小笠原みどり訳）『監視スタディーズ』（岩波書店、2011 年）53 頁。ライアンは、1759 年に設立され、世界最大級の陶磁器メーカーの一つであるウェッジウッドの工場で定められた「陶工指南書」を例として挙げている。

¹⁰ 総務省の「平成 12 年通信利用動向調査〔事業所編〕」によると、1990 年代、特に 1995 年以降のパソコン保有率は、1990 年代前半まではわずか 10%程度であったが、1995 年には OS「windows95」が販売されて以降、パソコンの普及率が急速に上昇し、2000 年にはパソコンの保有率は 82.4%に達した。一方、企業におけるインターネットの利用率を見ると、1995 年以降のパソコンの保有率の上昇に伴い、その利用率も 1996 年の 5.8%から 2000 年 89.3%に達した。

¹¹ キャシー・オニール（久保尚子訳）『あなたを支配し、社会を破壊する、AI・ビッグデータの罠』（インターシフト、2018 年）参照。

ル技術等によって構成される「不可視の電子の網（Invisible electronic web）」を利用し、業務遂行の状況を含む従業員のあらゆる側面業務を高い精度で測定し、センサーによって得られたデータを人事管理に利用できるようになっている。このような AI を活用した人事管理は、現在「ピープル・アナリティクス（People analytics）」と呼ばれている¹²。また、使用者による監視は、生産性や効率の確保・向上の観点から、労働者の業務遂行の状況を確認するだけでなく、勤務時間中の労働者の安全や使用者の財産を保護するなど、さまざまな目的を果たしている¹³。さらに、AI による分析の技術が高まっている中、労働者のあらゆる側面を分析するために大量の個人データを収集するという目的が加わった。一方、監視の実施方法については、かつての労働者への尾行や身体検査から RFID（Radio Frequency Identification）や全地球測位 GPS（Global Positioning System）まで、質的にも量的にもテクノロジーの発展とともに変化してきた。このように、現代社会では、事業場における労働者の仕事成果や他のあらゆる行動が過度に透明化されていると同時に、テクノロジーの発展に伴う監視装置の存在が不透明化されているのが特徴である¹⁴。

日本の職場では、労働者は自分自身が職場という共同体の一員であると認識する風潮はかねてより存在してきた¹⁵。このような特徴は、日本の職場レイアウトから観察することができる。周知の通り、日本で代表的な職場レイアウト様式は島型対向式である。これとは対照的に、欧米のオフィスでは半個室のレイアウトが一般的である。日本のレイアウトでは、パソコン等のツールが同じ島に属する従業員に共用され、従業員間のコミュニケーションが円滑に進み、島の端にいる上司が直接的に細やかな配慮を行うこともできるというメリットが挙げられることに対して、同じ島に属する上司及び従業員が相互的（見ることと見られることが同時に発生している）かつ不断に監視するため、従業員のプライバシーの喪失、ストレスないし心理的負荷に伴う労働意欲が低下するというデメリットも明らかである¹⁶。このように、日本の

¹² R.A Bales & K. V.W Stone, The Invisible Web at Work: Artificial Intelligence and Electronic Surveillance in the Workplace, 41(1) BJELL. 1, 3-9 (2020).

¹³ Eurofound, Employee monitoring and surveillance: The challenges of digitalisation, Publications Office of the European Union, Luxembourg, 2020, p.3.

¹⁴ *Ibid.*

¹⁵ 道幸哲也『職場における自立とプライバシー』（日本評論社、1995年）13-14頁。

¹⁶ Eurofound, *supra* note 13, p.4.

職場で行われる監視は、日本の職場特有のレイアウトによって強化されており、さらに労働者が気付かないまま常時存在している¹⁷。

もっとも、これまでの日本では、使用者による監視について、正面から論じる議論はほとんどなかったといえる。確かに、使用者による監視が労働者のプライバシー権を侵害するという観点から、使用者の監視の必要性とのバランスを図ることの重要性を指摘する見解は少なからずあった。しかし、私生活の領域ではなく、業務に関係する監視となると、通常はその必要性が認められるため、プライバシー権によっても、制限をすることは容易ではなかった。一方、2000年に労働省（現：厚生労働省）が策定した「労働者の個人情報保護に関する行動指針」に基づき、監視を情報収集の一態様と捉え、実施に際して個人情報保護の観点から労働者の同意や使用者の通知義務を必要とする見解もある。これは監視を個人情報保護という観点からみるものであり、その後の個人情報保護法の制定により、監視を制定法の解釈・適用の問題として論じる基盤ができたといえる。しかしながら、実際には、個人情報保護法を、労働者の個人情報の保護という観点からなされる研究は数少なく、ましてや監視をこうした観点から研究するものはほとんどなかった。裁判例をみても、使用者の監視によるプライバシー侵害の不法行為該当性や使用者が監視から得た証拠に基づいて行った懲戒処分の有効性を争う事件などにおいて、使用者の監視の適法性に触れたものはあるが、その数は少数にとどまっており、しかも本格的にこの論点を展開したものはなかった。このように、日本法においては、監視の適法性をめぐる議論はこれまで低調であったし、ましてや今後検討されるべきデジタル技術を活用した監視をどのように規制するかという視点からの研究は皆無に等しい。

しかし、デジタル化が進化するなかで、労働者の個人情報保護の観点から、使用者による監視を検討する必要性が高まっている。というのも、デジタル

¹⁷ 日本職場のレイアウトと監視との問題は、哲学者ミシェル・フーコー（Michel Foucault）の議論との親和性が高い。フーコーは、監獄、工場または学校といった場所で、監視者・被監視者とレイアウトの設定が、見られる側の自己規律（従順な身体になること）の効果を生み出し、その結果、見る側（使用者）と見られる側（労働者）の間に権力関係が形成されると論じている。ミシェル・フーコー（田村俊訳）『監獄の誕生－監視と処罰－』（新潮出版、1977年）198頁以下参照。さらに、フーコーは、パノプティコン（一望監視方式）の応用として、当該施設の利用が労働者の監視に役立つと指摘している（同書、207頁）。また、パノプティコンを構想したジェレミー・ベンサムは当初その弟であるサミュエルが考案した工場労働者の管理計画から着想を得たとの指摘がある。ライアン・前掲注9）52頁。

技術、特に AI が発達している現代において、使用者は高度な監視装置を通じて労働者の安全・健康上のリスクを早期に発見し、対応することができる一方で、こうした装置を用いて労働者に関する情報をこれまで以上に収集することができ、こうした情報に基づく分析が労働者の個人的利益を侵害するリスクを高める可能性があるからである。とりわけ労働関係では、その利益が侵害されやすい面があるので、いっそうこの問題は深刻なものとなる。もちろんデジタル技術の発達は、まだ進行過程であり、その危険性はまだ広く顕在化しているとはいえないが、今後の課題として優先性が高いものであり、理論的な研究を進めていく必要がある。この点では、日本よりも早く個人情報保護の問題に取り組み、使用者による監視の適法性に関する議論の蓄積のある欧州人権裁判所の判例法およびフランス法の状況が参考になる。また、使用者の監視行為を、個人情報保護という観点から制約をかけるにしても、デジタル技術を活用した監視ということになると、企業にとっても十分な知識がなく、どのようにすれば適法と判断されるかについての判断が困難となる可能性もあり、この問題を解決しなければ、法の実効性が損なわれることになる。したがって、使用者の監視行為の適法性を論じるためには、単に裁判規範となるような判断枠組みを論じるだけでは不十分で、行為準則として機能するような明確性が求められることになる。さらに、デジタル技術の急速な進展とともに監視の機能も向上しているという点に鑑みれば、監視に関する判断枠組みの内容を定める際、従来の国家による直接的規制および産業界による自主規制だけでは不十分であり、新たな技術を利用する産業界との協働による規制のあり方を検討することも不可欠となる。この点についても、EU 法やフランス法の議論が参考になる。

以上をまとめると、本論文では、従来、日本では十分に議論されてこなかった、使用者による監視の適法性について、とりわけデジタル技術の進展に伴う個人情報の保護という視点から、どのような判断枠組みを定立すべきかを、それと関係して、どのような規制手法が必要かについて、欧州人権裁判所の判例法、EU 法またはフランス法との比較法を通じて、検討することとする。

II.論文の構成

本論文の構成としては、まず、第1章の第2節で監視に関する行政解釈と個人情報保護法の関連規定を検討し、次に、第3節では職場における監視に関する問題について考察する。具体的には、監視に関する裁判例を、①単純な監視に関する判決とそれに関する学説上の議論、②機器を用いた監視に関する判決とそれに関する学説上の議論分けて検討する。最後に、監視に関する裁判例の判断と労働法学における監視に関する議論の到達点と問題点を示すこととする。

また、前述したように、監視は従業員の業務遂行をチェックし、それによって得られたデータを分析することだけでなく、職場の安全等を確保する目的を有する。このような多目的な監視を網羅的に定義することは簡単ではないため、本論文では、監視を、「形態または手段を問わず、使用者が勤務時間に（必要であれば勤務時間外においても）、労働者の業務遂行の状況を確認し、プロファイリング等を通じて業務状況を向上させる目的、または職場の安全衛生、財産を保護する等業務に関連する目的で、従業員の行動、情報を観察・収集することである」と定義しておくこととする。この定義の意図は、労働契約の締結に基づいた、監視の権限の範囲内にある事項（例えば、業務進捗のチェックや企業施設の保護など）に関する問題と、プライバシー保護や差別などの観点から処理されるべき問題（例えば、特殊な時代背景において業務と無関係な労働者の信条、思想を調査するための監視など）を区別することにある¹⁸。したがって、本論文では、使用者が上記定義に該当する監視から生じる問題のみを対象とする。

次に、第2章では、労働法学ではほとんど取り上げられない欧州人権裁判所の判例を主な対象として分析する。具体的には、第2節において、ILOやヨーロッパにおける監視に関する重要な法的文書を概観し、第3節において欧州人権裁判所の構造をよりよく理解するために、欧州評議会の発足の

¹⁸ 例えば、関西電力事件では、社内の共産党員もしくはその同調者を排除するために1960年代から1970年代にかけて講じられた「特殊対策」の一環として、共産党と疑われる従業員に対する職場内外における調査・監視、差別的待遇、社内での孤立化等の方策の違法性について争われた。最高裁は、被告会社Yの行為が「原告従業員Xらの職場における自由な人間関係を形成する自由を不当に侵害するとともに、その名誉を毀損するものであり、また、Xらに対する行為はそのプライバシーを侵害するものもあって、同人らの人格的利益を侵害するもの」とし、Yの一連の行為は不法行為に該当すると判断した。最3小判平成7・9・5労判680号28頁。

背景、欧州人権条約の変容、同条約の実効性を保障する欧州人権裁判所の構造等を紹介し、第 4 節で欧州人権裁判所のこれまでの判例法における使用者による監視に関する事件を検討する。

第 3 章では、監視の問題に古くから積極的に取り組んできたフランス法を対象として分析する。具体的には、第 2 節で監視に関するフランスの立法の内容とそれに対する学説上の議論について検討し、第 3 節で監視の問題に関する事例、学説上の議論または CNIL の見解について分析する。

第 4 章では、従来の労働法学では十分に議論されてこなかった共同規制について検討する。具体的には、第 1 節で共同規制の意義とその他の規制手法との相違について論じ、第 2 節で EU の 1995 年のデータ保護指令（Data protection Directive。以下では、データ保護指令と略称する¹⁹⁾）と 2018 年に施行された一般データ保護規則（General Data Protection Regulation。以下では、GDPR と略称する²⁰⁾）における共同規制の概念を具体化した行動規範を検討し、第 3 節で日本の個人情報保護法における共同規制の手法に最も近い認定個人情報保護団体の制度及び行動規範との相違について考察する。

第 5 章においては、まず第 1 章から第 4 章までの議論を整理し、次に、第 2 章と第 3 章における比較法的検討の結果から、使用者が適正な監視を行えるようにするための判断枠組みをどのように構築するかを検討し、最後に、第 4 章の検討に照らして、このような判断枠組みの内容をどのように明確にするかを分析する。

¹⁹⁾ European Union, Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 24 October 1995.

²⁰⁾ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

第1章 日本における問題状況

第1節 序説

日本では、監視の問題はプライバシー侵害の一類型として取り上げられることが多い。労働者のプライバシー権は、1980年代から議論されてきた。今日では、たとえ「完全なプライベート」ではない職場においても、労働者が依然としてプライバシー権を有することは、判例及び学説の双方において認められている²¹。一方、監視に関する判決や学説上の議論は、プライバシー権に関するものよりもはるかに少ない。しかし、特に2005年に個人情報保護法が施行されて以降、学説は、監視を個人情報収集の一形態と捉え、注目するようになってきた²²。それは、高度な監視装置を利用することで、従業員のあらゆる行動を把握できるだけでなく、監視から得られた画像（個人データ）をアルゴリズムで分析し、労働者の健康状態などを予測することができるからである。他方、監視の問題を扱う裁判例は、1960年代の所持品検査の適法性をめぐる問題から、録音機や監視カメラ、さらにGPS機能付き装置による監視の問題まで多岐にわたるが、所持品検査から生じる問題を除き、監視の適法性はケースバイケースで判断されており、明確な判断枠組みが確立されていない。このほか、従業員の個人情報の保護という観点から、旧労働省（現：厚生労働省）は2000年から2015年まで、監視の問題を含む労働者の個人情報保護に関するガイドライン等を策定し、2015年以降、個人情報保護に関する問題は個人情報保護委員会の所管に一元化されるようになった。現

²¹ 労働者のプライバシー権を検討する文献として、山田省三「職場における労働者のプライバシー保護」日本労働法学会誌78号（1991年）33頁、盛誠吾「雇用・職場とプライバシー」堀部政男編『ジュリ増刊情報公開・個人情報保護』（有斐閣、1994年）239頁、島田陽一「労働者の私的領域確保の法理」法時66巻9号22頁（1994年）47頁、道幸・前掲注15）1頁、山田省三「雇用関係と労働者のプライバシー」日本労働法学会編『講座21世紀の労働法第6巻—労働者の人格と平等（第4章）』（有斐閣、2000年）56頁、名古屋功「労働者のプライバシー」西谷敏ほか編『転換期労働法の課題—変容する企業社会と労働法』（旬報社、2003年）161頁、竹地潔「労働者のプライバシー保護」ジュリ増刊『労働者の争点〔第3版〕』（2004年）111頁、砂押以久子「職場のサイバー・サーベイランスと労働者のプライバシー保護」立教法学65号（2004年）320頁、長谷川聡「プライバシーと個人情報の保護」日本労働法学会編『講座労働法の再生第4巻人格・平等・家庭責任』（日本評論社、2017年）29頁、劉子安「労働者のプライバシー権」季労274号（2021年）156頁などがある。

²² 例えば、①砂押以久子「個人情報保護法の労働関係への影響」労旬1606号（2005年）17頁、②同「情報化社会における労働者の個人情報」日本労働法学会誌105号（2005年）64頁、竹地潔「新たな段階を迎えた労働者の個人情報保護と企業の対応」季労213号（2006年）78頁など。

在，個人情報保護委員会によって策定された Q&A やガイドライン（通則編）に示された監視に関する注意事項は，機器を通じた監視装置の問題に対処するための重要な基準となっている（もともと，法的拘束力はない）。

以下では，まず，従業員の個人情報保護に関する行政解釈やガイドライン等の監視に関する部分を抽出し，その変遷を紹介し，次に，職場における監視の問題を単純な監視と機器を用いた監視に区別した上で，2つの種類の監視に関するそれぞれの裁判例と学説上の議論を考察する。

第 2 節 監視に関する行政解釈と個人情報保護法上の規制

第 1 款 監視に関する行政解釈

職場における監視に関する行政解釈は，労働者の個人情報を保護する目的で，主に機器を用いた監視を対象としている。これらの行政解釈は，後述する裁判例の立場よりも厳格であり，特に西欧諸国の先進的な取組みを組み入れていることから，監視の問題を検討する学説によって頻繁に引用されているが，裁判実務に与える影響は必ずしも大きいとはいえない。

監視の問題を最初に取り上げたのは，「労働者の個人情報保護に関する行動指針」である²³。同行動指針の第 2 の 6 (4) は，法令に定めがある場合，犯罪その他の重要な不正行為があるとするに足りる相当の理由があると認められる場合を除き，「使用者は，職場において，労働者に関しビデオカメラ，コンピュータ等によりモニタリングを行う場合に，労働者に対し，実施理由，実施時間帯，収集される情報内容等を事前に通知するとともに，個人情報の保護に関する権利を侵害しないよう配慮するものとする」と定めている。さらに，同行動指針の第 2 の 6 (5) は，職場における監視の目的を「労働者の健康及び安全の確保又は業務上の財産の保全に必要な場合」に限定している。このように，同行動指針は，使用者に対し，機器を用いた監視を実施する前に従業員に通知し，その目的を労働者の健康や安全等に限定することを求めている。

上記の行動指針以後，2015 年に改正される前の個人情報保護法では，各主務大臣は，事業者ごとの実情や特性を考慮し，同法に基づく民間事業者の義務を履行するためのガイドラインを策定することができると定められていた。

²³ https://www.mhlw.go.jp/www2/kisya/daijin/20001220_01_d/20001220_01_d_shishin.html（最終アクセス日 2013 年 12 月 11 日）。

厚生労働省が策定した「雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずるべき措置に関する指針²⁴」では、監視に関する部分は明確に言及されていないが、同指針第3(9)では、「その他事業主等が雇用管理に関する個人情報の適切な取扱いを確保するための措置を行うに当たって配慮すべき事項：(1)事業者は、……保有個人データの開示に関する事項その他雇用管理に関する個人情報の取扱いに関する重要事項（下線は筆者による）を定めるときは、あらかじめ労働組合等に通知し、必要に応じて、協議を行うことが望ましいものであること」と定められている。これを受け、厚生労働大臣及び経済産業大臣が共同で策定した「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」においては、上記の「重要事項」が使用者による監視を指すことが明記されている。同ガイドラインでは、使用者が監視を実施する場合、①モニタリングの目的、すなわち取得する個人情報の利用目的をあらかじめ特定し、社内規程に定めるとともに、従業員に明示すること、②モニタリングの実施に関する責任者とその権限を定めること、③モニタリングを実施する場合には、あらかじめモニタリングの実施について定めた社内規程案を策定するものとし、事前に社内に徹底すること、④モニタリングの実施状況については、適正に行われているか監査又は確認を行うことが定められている²⁵。

現行の個人情報保護法に関するQ&Aは、基本的に上記経産省のガイドラインにおける従業員に対するモニタリングの内容とほぼ同じ内容である²⁶。すなわち、同Q&Aでは、使用者が監視に関する事項を定める場合には、従業員個人への周知と事前に労働組合等の組織に通知し、必要に応じて協議を行うことが望ましいということに加え、「①モニタリングの目的をあらかじめ特定した上で、社内規程等に定め、従業員に明示すること、②モニタリングの実施に関する責任者及びその権限を定めること、③あらかじめモニタリングの実施に関するルールを策定し、その内容を運用者に徹底すること、④モニタリングがあらかじめ定めたルールに従って適正に行われているか、確認を行うこと（番号は筆者による）」に留意すべきであると定められている（5-7）。

²⁴ 平16年7月1日厚生労働省告示第259号。

²⁵ 平21年10月9日厚生労働省・経済産業省告示第2号（2-2-3-3）。また、従業員の監視を実施するにあたって留意点は、同ガイドラインの最初のバージョン（平16年10月22日厚生労働省・経済産業省告示第4号）ですでに定められた。

²⁶ 「個人情報の保護に関する法律についてのガイドライン」に関するQ&A（令和5年12月25日更新）。

第2款 監視に関する個人情報保護法上の規定

前述の個人情報保護法では、監視装置によって得られた個人の容貌や音声などが特定の個人を識別するもの（同法2条1項1号、施行令第1条第1号ロ²⁷及び規則第2条²⁸）であれば、同法上の個人情報（場合によっては、個人データと保有個人データ）に該当するため、監視装置を利用する使用者は同法の規定を遵守しなければならないとされている。使用者は監視装置の利用に際して、事前にその装置によって得られる個人情報の利用目的を特定する必要（同法17条）があり、さらに、あらかじめ上記の利用目的を公表している場合を除き、速やかに監視の対象となる従業員に監視による情報収集の存在を通知し、または公表する必要がある（同法21条1項）²⁹。一方、監視装置を通じて個人情報を収集した後の規制としては、監視装置によって得られた情報が個人データ（同法16条3項）に該当する場合、使用者はその装置によって得られた個人データの内容を正確かつ最新の内容に保つとともに、必要ではない個人データを消去する努力義務を負い、個人データの漏えい、滅失または毀損の防止その他の個人データの安全性を確保するための必要かつ適切な措置を講じる義務がある（同法22条、23条）。さらに監視装置によって得られた情報が保有個人データ（同法16条4項）に該当する場合、使用者は当該保有個人データに関し、事業者の名称及び住所、保有個人データの利用目的または開示や訂正等を求める個人の権利について、本人の知り得る状態に置かなければならない（同法32条1項～4項）。このほか、監視の利用に関する苦情があった場合、事業者はそれに適切かつ迅速な対応に努めなければならない（同法40条）、事業者が認定個人情報保護団体に加入している場合、認定個人情報保護団体は苦情の解決に介入することができる（同法53条）。

²⁷ 同法施行令第1条1号は、「次に掲げる身体の特徴のいずれかを電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、特定の個人を識別するに足りるものとして個人情報保護委員会規則で定める基準に適合するもの。……ロ：顔の骨格及び皮膚の色並びに目、鼻、口その他の顔の部位の位置及び形状によって定まる容貌」と規定している。

²⁸ 同法の規則2条は、「個人情報の保護に関する法律施行令第1条第1号の個人情報保護委員会規則で定める基準は、特定の個人を識別することができる水準が確保されるよう、適切な範囲を適切な手法により電子計算機の用に供するために変換することとする」と規定している。

²⁹ なお、監視装置によって本人の身体障害に関する映像が記録されていたとしても、その映像は要配慮個人情報には該当しない（同法20条2項8号、同法施行令第9条）。

第3款 小括

以上のように、日本の労働法規には監視を直接規制する規定はないが、行政機関は早い段階から、監視に関する先進国の取組みを参考にして行動指針やガイドラインを策定してきた。使用者の監視に関する規定がない日本法では、これらの基準が重要な役割を果たしている。

行動指針では、監視を実施する目的（労働者の健康及び安全の確保または業務上の財産の保全に必要な場合）を厳格的に制限しており、使用者が監視に関する詳細な情報（収集される情報の内容、実施理由または実施時間帯）に従業員に提供するように求めているのに対して、個人情報保護法制定後の監視に関する行政解釈、特に現行の個人情報保護委員会によって策定された Q&A では、監視目的を特定すること、従業員に対してその目的を明示すること、監視を実施する責任者とその権限を明確に定めること、監視が定められたルールに従って実施されたかどうかを事後的に点検することが求められている。行動指針と比較して、特に通知の内容と目的限定の面では、Q&A の内容かなり緩和されている。その理由は、日本の個人情報保護情報法の構造と密接に関係している。EU の GDPR とは異なり、個人情報保護法は、データ処理の適法性根拠を求めておらず、事前に情報処理の利用目的を特定し、その目的をデータ主体に通知すれば十分である（学説では、利用目的中心主義と呼ばれている³⁰）。しかし、職場以外の場所で行われる監視、例えば、デパートや駅などでは、通常、個人が通り過ぎる際にのみ記録されるのとは異なり、職場で実施される監視は、労働者の一挙手一投足を間断なく記録するものであり、そのような監視は労働者のプライバシーその他の人格的利益を著しく侵害する性質を有している。したがって、このような職場における監視の特殊性を考慮すると、利用目的中心主義に基づく個人情報保護法では、職場で実施される監視に効果的に対処できないように思われる。

第3節 監視に関する裁判例上の立場と学説上の議論

第1款 単純な監視

³⁰ 利用目的を中心とする日本の個人情報保護法（利用目的中心主義と呼ばれている）では、AI時代におけるデータ処理の問題に対応する「有効性は期待できない」と指摘した見解がある。岡本久道『個人情報保護法〔第4版〕』（商事法務、2022年）216-217頁参照。

(1) 判例の立場

単純な監視に関して、最も典型的な例は労働者の所持品検査に関する事件である。所持品検査は、かつては使用者の目の届きにくい職場で現金を収受する機会の多い職場で多く実施されていたが、バス車内に料金箱の設置が一般になった後、この種の検査が減少し、現在では企業の財産、特に営業秘密を保全するという目的で実施されることが多い。このような検査がもたらす主な問題は、従業員による盗難や企業秘密の漏洩を摘発・防止するという使用者の正当な利益と、労働者のプライバシー権や名誉などの労働者の基本的人権とのバランスを如何にして図るかということである。したがって、広い意味で、所持品検査から生じる問題は労働者の基本的人権と使用者の利益との対立とみることができる。日本では、職場における所持品検査の問題が世間の耳目を集め始めたのは、1963年に発生した神戸市交通局で勤務していた女子車掌が身体検査された後自殺した事件³¹からである。この事件の影響を受け、法務省人権擁護局は、同年の8月に「バス乗務員に対する所持品及び服装検査等の行き過ぎによる人権侵犯について」と題する通報を労働基準局長や各地方方法務局などに発した³²。この通報に加え、司法的判断として、後述

³¹ 神戸新聞昭和38年6日4日14版。この事件は、神戸バスで勤務した従業員が所持品と身体検査を受けた際に、売上金以外にポケットに500円入っていたことが判明し、その後、当該従業員は身の潔白を証明するために自殺したというものである。補足であるが、当時の公共運輸機関は、金銭着服（チャージの問題）の問題を防止するため、従業員に対する所持品又は身体検査を一般的に行なっていた。さらに、当時の検査は、現在ではありえないほどの方法で実施されており、具体的には、バスの女子車掌を全裸にさせ、ゴム手袋と検査棒で、徹底的に性器と肛門を突き回して検査していた。しかも、通常の検査の時間は3時間以上かかるようである。神戸バス従業員が自殺した事件後の日本弁護士連合会人権擁護委員会の「要望」や国会での議論については、柏崎洋美「所持品検査について―問題の背景と現状―」京都先端科学大学経済経営学部論集3号（2021年）14頁以下参照。

³² 昭和38年8月27日法務省人権第381号法務省人権擁護局。当該通達の抜粋では、「この趣旨から服務規定、就業規則などに、乗車券売上金についての不正行為防止に関する規定が設けられ、その方法として、多くの場合、乗務員の所持品および服装等の検査が行なわれているのであります。しかしながらかかる検査の実施は、人権に対する制約を伴う場合が多く、その程度、方法のいかんによっては、憲法に定める人権保障の趣旨に反する場合も少なくないのであります。したがって、このような乗務員の不正防止措置については、企業管理方式などについて十分検討を加え、人権の制約を伴わない他の方法を採り得るならば、これによることが望ましい……やむを得ない措置として乗務員の所持品および服装等検査の方法をとる場合においては、その方法、程度が行き過ぎにならないよう必要最小限度に止め、いやしくも乗務員の人権侵害となるような検査が行なわれてはならないことは申すまでもありません」としている。

する 1968 年の西日本鉄道事件最高裁判決³³によって所持品検査の適法性に関する重要な判断基準が確立され、現在もこの基準は同種の事案において用いられている。また、厳密に言えば、労働者が所持品検査を拒否した問題に関して、その判断は 2 つの段階に大別されている。第 1 段階では、所持品検査自体の適法性をどのように評価すべきであるかという問題である。この段階においては、上述の最高裁判決が確立している判断基準に照らして判断される。次に、第 2 段階では、労働者が所持品検査を拒否したことを理由になされた解雇を含む懲戒処分の有効性をいかに判断されるべきかとの問題である。この段階においては、労契法 15 条（懲戒権濫用）と 16 条（解雇権濫用）に基づいて判断される。以下では、職場の監視との関連で、上記第 1 段階の問題に限定して検討する。

まず、上記の西日本鉄道事件最高裁判決に先立ち、4 ないし 5 部赤旗新聞を所持した労働者 X が所持品検査を拒否したことを理由に懲戒解雇されたことが争われた神戸製鋼所入門拒否事件³⁴において、裁判所は、従業員の携帯品に対する検査が可能な状況は、「現実の就労の際にその職場規律をみだし、秩序維持を妨害する蓋然性が強い」場合、「工場施設や従業員の就労中の安全危険防止を妨害する蓋然性が強い具体的な理由がある」場合に限られるとし、X が所持していた新聞は 4 ないし 5 部に過ぎず、外見から新聞であることが明らかであることを総合考慮すると、本件所持品検査は違法であると判断した。控訴審の大阪高判は、一審判決の判断を支持し、所持品検査の適法性を判断する際の要素について、「携帯物件の形状、数量その他諸般の状況から見て持込の許されない物品を所持していることを疑うに足りる相当な事由がある場合に限り、……単なる会社側の見込だけによって所持品検査をすることは、思想信条の調査にもつながり、人の自由を制限する虞のあるものとして許すべきではない」と判断した³⁵。控訴審の判決は西日本鉄道事件最高裁判決の

³³ 最 2 小判昭 43・8・2 判時 528 号 82 頁。

³⁴ 灘簡易判昭 40・3・27 労民集 16 卷 2 号 179 頁。また、筆者が調べた限りにおいては、本判決はプライバシー権という用語を労働事件で初めて用いたものである。この点について、本判決は、「被告会社の従業員には被告会社の事業所内にいる間にも自由に社会生活が行なえる時間があり、且つ更衣室のロッカーに私物を保管しておくことも出来るのに、就業規則第 30 条は従業員の出入門の際にその所持品の規制を行なってしまうとする点、事業所内での従業員の自由であるべき社会生活をも規制する結果になるし、その条項上の規制の方法としても従業員の所持品の点検をしようとするものだから、各従業員が個人として有するプライバシーの権利を不当に侵害するものであってはならない」と判断した。

³⁵ 大阪高判昭 50・3・2 労判 226 号 48 頁。

後に下されたものであるが、この判決は同最高裁が示した判断基準を用いておらず、その代わりに所持品検査の適法性を諸要件から総合的に判断するアプローチを採用している。このようなアプローチは、後述する最高裁の判断基準に比べ、明確性に欠け、予測可能性が低いように見える。

次に、所持品検査の問題に関して、最も重要な判例である 1968 年に下された西日本鉄道事件最高裁判決は、同事件で争われた脱靴検査の性質について、「いわゆる所持品検査は、被検査者の基本的人権に関する問題であって、その性質上つねに人権侵害のおそれを伴うものであるから、たとえ、それが企業の経営・維持にとって必要かつ効果的な措置であり、他の同種の企業において多く行なわれるところであるとしても、また、それが労働基準法所定の手続を経て作成・変更された就業規則の条項に基づいて行なわれ、これについて従業員組合または当該職場従業員の過半数の同意があるとしても、そのことの故をもって、当然に適法視されうるものではない」とし、このような検査を正当化するためには、「①合理的理由に基づいて、②一般的に妥当な方法と程度で、しかも③制度として職場従業員に対して画一的に実施されるものでなければならない。そして、このようなものとしての所持品検査が、④就業規則その他、明示の根拠に基づいて行なわれる（番号は筆者による）」ことが必要であると判じ、上記の 4 要件を満たした検査について、「他にそれに代わるべき措置をとりうる余地が絶無でないとしても、従業員は、……特段の事情がないかぎり、検査を受忍すべき義務があ（る）」と判示した³⁶。本判決が確立した上記 4 要件からなる判断基準は、直接的または間接的に、その後の同種または類似の事件において使用されている³⁷。また、同最高裁判決が用いた「基本的人権」という用語は、具体的に何を指すかは明らかではないが、同判決以降の下級審の判断からすると、その意味は労働者の「私的領域ないしプライバシー」と理解することができそうである。例えば、使用者

³⁶ 最 2 小判昭 43・8・2 前掲注 33。

³⁷ 東陶機器事件（福岡地小倉支判昭 46・2・12 判タ 264 号 325 頁〔地位保全仮処分申請事件〕）、芸陽バス事件（広島地判昭 47・4・18 判時 674 号 104 頁）、帝国通信工業懲戒解雇事件（横浜地川崎支判昭 50・3・3 労民事集 26 巻 2 号 107 頁）、後述のコスモアークコーポレーション事件（大阪地判平 25・6・6 労判 1082 号 81 頁）、国・法務大臣（陸上自衛隊）事件（前橋地判平 29・11・29 LEX/DB 25549217）がある。また、身体検査を伴う所持品検査の事件においても、同基準を援用した事件として、日立物流事件（浦和地判平 3・11・22 労判 624 号 78 頁）がある。このほか、後述のサンデン交通事件（山口地下関支判昭 54・10・8 労判 330 号 99 頁）において、裁判所は西日本鉄道事件最高裁判決が提示した 4 要件を明確に引用していないが、実質的にこれらの基準に基づいて判断されたことは明らかである。

が被検査者のポケットに手を突っ込んだり、あるいは被検査者にポケットの中袋を裏返しさせる等の検査の違法性が争われたサンデン交通事件において、裁判所は、たとえ所持品検査の実施に具体的な事由があり、かつ警察等の捜査を待ったのでは時機を失するという緊急の必要性が認められる場合でも、「プライバシー保護との関連でなしうる検査の範囲というものが存するのであって、例えば被検査者のロッカーや自家用車内等の検査はプライバシーに対する侵害の可能性が極めて高く、特段の事情なき限り許されない」とし、所持品検査を実施する際に、労働者のプライバシーを考慮することの重要性を示している³⁸。また、労働者の財布および通帳の中身を点検したことの違法性が争われたコスモアークコーポレーション事件において、裁判所は、「財布と通帳の点検、運転免許証や携帯電話の取上げといった私的領域への介入あるいは生活への支障を伴う財産権侵害行為は、原告〔筆者注：労働者〕に対し相応の精神的苦痛を与えたことは明らかである」と判断している³⁹。

また、使用者が所持品検査をする前に、検査対象者の同意を得たと主張する場合、その同意の有効性について争われた上記のコスモアークコーポレーション事件において、裁判所は、所持品検査に対する労働者の同意の有効性について、「(労使間に)職場の上司と部下という以外に私的な人間関係があるとは認められず、そのような雇用契約上の上下関係を背景に、財布や通帳の点検をすると言われた場合、抵抗することなく点検に応じたからといって、真摯な同意があったと認めることは相当でない」とした⁴⁰。この判決は、所持品検査に対する労働者の同意を厳格に解釈し、その同意が真摯なものであることを求めている。これに対し、労働者の同意の有効性を緩やかに判断した判決も存在している。原告自衛隊隊員 X の衣室内の個人用ロッカーと X が所有している自動車を対象とし、違法薬物の所持を検査することの適法性が争われた国・法務大臣（陸上自衛隊）事件において、裁判所は、「X は、本件点検 1（筆者注：一回目の検査）に当たり、小隊長から営内更衣室のロッカー及び X の私有自動車を点検する旨を告げられた上で、自らロッカーの扉並びに自動車のドア及びトランクを開けて、本件点検 1 の実施に協力しており、X がその場で異議等を述べたことはなかったというのであるから、X は、本件点検 1 の実施に対し、少なくとも黙示的に同意していたというべきである。

³⁸ 山口地下関支判昭 54・10・8 前掲注 37。

³⁹ 大阪地判平 25・6・6 前掲 37。同旨、前掲芸陽バス事件（広島地判昭 47・4・18 前掲 37）。

⁴⁰ 大阪地判平 25・6・6 前掲 37。

また、Xは、本件点検2（筆者注：二回目の検査）に当たり、一旦は、所持品点検がプライバシー侵害に当たることを理由に拒否したものの、その後、…自らロッカー、自動車等から収納物等取出して、本件点検2の実施に協力しているのであるから、Xは、本件点検2の実施に対しても、同意するに至ったというべきである」とし、所持品検査に対する同意の有効性を緩やかに捉えている⁴¹。上記Xの自衛隊員としての特殊な地位が、所持品検査の同意の有効性の判断に一定の影響を及ぼしたと考えられる。すなわち、前掲の国・法務大臣（陸上自衛隊）事件判決は、自衛隊の任務や規律の厳正さの必要性は一般の労働者のそれよりも高く、したがって、自衛隊員による違法薬物の使用・所持を防止するために所持品検査を行う必要性は高い、としたのである。しかし、この点については、前述のコスモアーコーポレーション事件を参考にすると、従属関係にある労働者が所持品検査を拒否することは事実上不可能に近いと、労働者の同意はできる限り厳格に判断すべきである。このことは、自衛隊隊員の特殊性（特別職公務員の身分や一般的な仕事よりも厳正な規律が求められていること）を考慮したとしても、異にするべきではない。

（2）学説上の議論

監視の問題に関して最も早い段階で議論されるようになったのは、所持品検査の適法性である。当時は、前述の西日本鉄道事件最高裁判決が確立した所持品検査に関する判断基準の妥当性が議論の対象となっており、一部の学説はこれに懐疑的な見解を示した。例えば、同判決は、所持品検査を当然には適法視しないと判示したが、「一旦違法と考えられている所持品検査が、何故に適法となるのかその法理論は十分とはいえない」との疑問を呈した見解⁴²、同判決は検査を受けた労働者の意思を無視し、当該検査に了承を示していた労働組合の意思のみを考慮しただけでは不十分とする見解⁴³、同判決が提示した判断基準は、「制度として職場従業員に対して画一的に実施すべき」との要件を除き、不明確かつ抽象的な部分が多いという見解⁴⁴がある。また、所持品検査を命じられた労働者は、その検査を承諾するか懲戒解雇を甘受する

⁴¹ 前橋地判平 29・11・29 前掲注 37。

⁴² 阿久沢亀夫「判批」法學研究 42 巻 4 号（1969 年）93 頁

⁴³ 平野毅「判批」萩澤清彦編『労働判例百選〔第 3 版〕』（1974 年）91 頁。

⁴⁴ 平野毅「判批」萩澤清彦編『労働判例百選〔第 3 版〕』（1981 年）79 頁。

かの二者択一の状況に追い込まれるとの観点から、「所持品検査は憲法の自由保障の趣旨（憲法 11 条, 12 条, 13 条, 31 条, 35 条）に照らし、公序良俗に違反し、所持品検査の規定はどのような方法によろうと、また就業規則あるいは労働協約で協定しようとする無効であると言わねばならない」とし、上記最高裁判決を全面的に批判した見解⁴⁵もあったが、一般的に、所持品検査を「必要悪」として捉えた上で、その許容される範囲を厳格に解釈すべきであるとする見解が多い⁴⁶。最後に、上記同判決の判断枠組み（4 要件審査）を満たしていない所持品検査の効力はどうなるかとの問題について、所持品検査が 4 要件を満たして初めて労働者の所持品検査を受忍する義務が生じるという同判決の判断からして、上記要件が満たされていない違法な所持品検査に対して労働者にそれを受忍する義務がないと解する見解がある⁴⁷。このほか、同判決の判断基準を、機械的にあらゆる所持品検査のケースに適用することは必ずしも妥当ではなく、緊急時の身体検査と定期に行われる所持品検査を区別する必要があるとの見解がある⁴⁸。この見解によれば、顧客の苦情を対応するために臨時的に行われる所持品検査は、通常所持品検査の形態とは異なり、就業規則にそのような検査に関する規定が定められていない場合であっても、従業員は労働契約上の調査協力義務に基づき、使用者の質問に答える程度の義務は有するが、所持品検査が身体検査に及ぶような場合には、労働者と使用者との間に身体検査に関する個別の合意がない限り、労働者はそれを拒否することができる」とされている。近時、所持品検査の態様を区別すべきとする見解に近く、上記所持品検査に関する判断枠組みが適用されるか否かは、所持品検査の形態によって区別されるべきとする見解がある⁴⁹。所持品検査を、身体的接触を伴う検査とそうではない検査に区別し、前者の場合には西日本鉄道事件最高裁判決の判断基準が適用され、後者の場合には、上記判断基準は適用されないものの、所持品検査の適法性は労契法 7 条にお

⁴⁵ 浅井清信「判批」民商 60 巻 4 号（1969 年）554 頁。

⁴⁶ 例えば、可部恒雄「判解」曹時 21 巻 4 号（1969 年）99 頁、安枝英紳「所持品検査とその拒否」労判 370 号（1981 年）10 頁、名古屋功「判批」労働判例百選＜第 5 版＞別冊ジュリ 101 号（1989 年）73 頁など。

⁴⁷ 山本吉人「所持品検査の方法と限界」法教 2 号（1973 年）155 頁。

⁴⁸ 吉田淑子「所持品検査と労働者の名誉・プライバシー」労旬 1303-4 号（1993 年）17 頁以下。

⁴⁹ 大内伸哉「キーワードからみた労働法 188 回所持品検査」ビジネスガイド 931 号（2023 年）76 頁。

ける労働条件の合理性審査を受けなければならないと解する見解もある⁵⁰。この見解では、使用者が後者の身体的接触を伴わないような所持品検査を実施する場合であっても、労働者に対して実施の理由や必要性を十分に説明し、納得同意を得るよう努力することが望ましいとしている⁵¹。

(3) 小括

所持品検査の適法性に関して、前述の西日本鉄道最高裁判決がそのような検査の適法性に関する 4 要件からなる判断枠組みを定立して以降、この所持品検査に関する判断枠組みは同種の事件において直接的または間接的に踏襲されている。近時では従来見られなかった所持品検査の実施に関する労働者の同意をどのように認定するかという新たな問題が現れた。この点について、労使間の交渉力の違いという観点から、労働者の同意を安易に認めた前掲の国・法務大臣（陸上自衛隊）事件の判断は適切ではなく、所持品検査の実施に対する同意は慎重に判断されるべきである。一方、所持品検査に関する学説上の議論は、上記最高裁判決によって定立された判断枠組みを中心に展開されてきた。初期の議論の多くは、同判断枠組みを批判的に検討するものが多かったが、現在ではそのような見解はほとんど見られず、代わりに当該枠組みの適用範囲を区別する必要があるという見解が多い。

以上のように、後述する他の監視形態とは異なり、所持品検査には明白な判断枠組みが存在するため、使用者は違法な所持品検査となる場合を予測することができ、法的に適切な検査を実施することが容易となる。

第 2 款 機器を用いた監視に関する裁判例と学説上の議論

(1) 裁判例の立場

(i.) 序説

パソコンとインターネットが職場で普及することに伴い、労働者は過去に比べてより効率的に業務を遂行することができるようになった一方、使用者による、労働者が使用する業務用コンピュータの運用状況の監視も容易になった。以下では、今日ではすでに「アナログ」と考えられている録音機および監視カメラによる監視に関する事件を取り上げた上で、職場 OA 化に伴って

⁵⁰ 同上注，85 頁。

⁵¹ 同上注，85 頁。

普及したパソコンの利用や電子メールへの監視に関する事件を検討し、最後に、労働者の位置情報をリアルタイムで取得できる GPS 機能付き装置とテレワークによる監視に関する問題を考察する。

(ii.) 録音機・監視カメラの使用から生じた問題点

(a) 録音機の使用に関する問題

録音機の使用に関する事案は、職場における労働者のプライバシー権が確立される前からあった。労働者のプライバシー権が確立されるまでに、裁判例では、監視によって侵害された労働者の利益を扱う際には、労働者の同意や人格権保護といった概念が用いられていた。例えば、被告である学校 Y が、原告教師 X の授業内容に「独善性ないし偏向」があったかどうかを調査するため、隠しマイクで全授業内容を録音し、その録音の内容に基づいて X を解雇したことについて争われた目黒高校事件において、裁判所は、「校長は X の授業内容を検討せんとしたのであるが、校長、同僚又は父兄による授業参観、生徒よりノート等の借用、X とその同僚又は校長との意見交換等他にみるべき手段によることなく、直ちに X の同意なしにその全授業を録音したのである。かかる行為は X に対し、その授業内容について、有益な援助ないし助成をなすその前提としての授業内容の確知方法において適正な手段とはいえない」とした⁵²。この判決は、労働者に無断で録音されたことによって労働者のどの利益が侵害されたかを明示していないものの、使用者が合法的に録音を行うためには、①録音以外の代替手段がなく（上記判旨：意見交換等の手段）、②手段と追及される目的（上記判旨：X の授業内容に対して有益な援助をなす目的）との間に関連性があること、という条件を満たさなければならないと述べている。もっとも、本判決は使用者が監視を実施する場合、従業員の同意を得なければならないとしているわけではない。むしろ、同様の目的が達成できる場合には、より侵入性の少ない手段を用いるという要件を使用者に課していると解することができる。次に、広沢自動車学校事件⁵³においては、被告 Y 社は、原告労働者 X（教習指導員）の技能教習をチェックする目的で教習車内に録音装置を設置していたが、X は、Y 社が設置した録音装置のある同車両の乗車を拒否したことを理由に懲戒解雇された。裁判所は、「学校管理者が指導員の教習を録音して聞くというのは、教習指導員が教習

⁵² 東京地判昭 47・3・31 労民集 23 巻 2 号 155 頁。

⁵³ 徳島地決昭 61・11・17 労判 488 号 46 頁。

態度を監視されているかのように感じて心理的圧迫を受けるのは無理からぬところで、録音される指導員及び教習生の自由な同意なしにこれをする場合には、教習生も含め録音される側の人格権の侵害にもなりうることは否定できない」とし、使用者が録音機を導入する際に、「教習指導員らに対し、あらかじめその事情を話し、それに対する意見を十分に聞き、反対者の理由に対する意見を述べて説得し、例えば教習生のプライバシーの問題もあるとすれば、その同意を得るかどうかなど等実施の方法などにつき十分協議してその納得を得るよう努力すべき」と判断した⁵⁴。本判決では、監視下に置かれる労働者の同意を重視している点は、前述の目黒高校事件とは異なっている。また、本判決は、監視が労働者の心理的圧迫をもたらすという問題を指摘し、さらに使用者は監視を行う前に、監視方法等の説明及び十分な協議を通じて労働者の納得を得るよう努力すべきであると指摘した点で注目されている⁵⁵。このほか、使用者が労働組合の情報を収集する目的で、従業員の控室に盗聴器を設置したことが、従業員のプライバシー侵害にあたるとして慰謝料が請求された岡山電気軌道事件において、裁判所は、「労働者らは私的な会話等をすることもあったというのであるから、労働者らがこのような会話を他人に聞かれていることを容認していたものとは考えられず、本件従業員控室に盗聴器を設置し会話を傍受することは、労働者らのプライバシーを侵害するものであって違法なもの」としたが、本件問題となった控室が「完全たる」私的場所ではないため、そこでの会話は「いわゆる私的な場所における会話と比べて、プライバシーとして保護されるべき程度が低い」とし、慰謝料の認定額を減額した⁵⁶。本判決が、上記監視カメラが従業員のプライバシー権を侵害したことを理由に不法行為に基づく損害賠償を認めたことは重要な意義を持つが、監視カメラ利用に関する適法要件の基準は示されていない。

(b) 監視カメラの問題

使用者Yが労働組合Xの組合員らの使用する事務室に音声モニターと監視カメラを設置したことが、労働組合に対する支配介入（労組法7条3号）および同組合員のプライバシー侵害に該当することが争われた奥道後温泉観光バス（配車差別等）事件において、裁判所は、労働組合に対する支配介入に関

⁵⁴ 徳島地決昭61・11・17前掲注53。

⁵⁵ 竹地潔「ネットワーク時代における労働者の個人情報保護」季労187号（1998年）36頁。

⁵⁶ 岡山地判平3・12・17労判606号50頁。

しては、監視カメラの目的（組合員による業務妨害を防止すること）と態様（Xの組合員が上記事務室に通過するたびに、監視カメラに撮影された）に照らし、「本件事務室における毀棄的行為等を防止するのであれば、監視カメラによる抑止効果で十分であり、新たに本件音声モニター装置を設置する必要性は乏しいと思われる上、監視カメラを設置するにしても、毀棄的行為やY事務室の使用を防止するためには、Y事務室への立ち入り自体を抑止する必要があるから、むしろY事務室の入り口につながる階段を登ってくる者に見えるように、監視カメラを同入り口の外に階段の方を向けて設置する方が合理的と思われ、Y事務室内部に本件監視カメラを設置し続ける合理性は乏しいといわざるを得ない」とし、したがって、「本件監視カメラ等の設置等は、X組合に対し心理的圧力を加えて組合活動を弱体化させるものとして、X組合に対する支配介入に当たり、労働組合法7条3号に該当する不当労働行為であると認められる」と判断したが、プライバシー侵害の判断に関しては、「本件監視カメラは、事務室内を撮影するものではあるが、事務室は就業場所であって、いわゆる私的な場所ではなく、従業員が労務から解放される休憩室は本件監視カメラの撮影対象とはなっていない」とし、プライバシー侵害の請求を退けた⁵⁷。本判決は、上記の監視カメラがX組合の組合員らのプライバシーを侵害したという主張を退けたが、労働組合に対する支配介入があったことを認めた点に特徴がある。さらに、本判決のもう一つの特徴は、録音機による監視に関する事件には見られない、監視装置そのものの必要性和相当性を審査した点である。しかし、事務室は私的な場所ではないという理由で、プライバシー侵害を否定した本判決の判断には疑問が残る。厳密に言えば、判決で言及された休憩室も事務室も企業が管理する場所であり、私的な場所ではない。そのため、監視カメラがプライバシーを侵害するか否かは、場所の性質よりも、支配介入の成立に関する判断と同様、監視装置その

⁵⁷ 松山地判平21・3・25労判983号5頁。また、本件原告組合は、平成16年7月16日、配車方針の差別及び本件監視カメラ等の設置が不当労働行為に当たるとして、愛媛県労働委員会に対し、救済命令を求める申立てをした。愛媛県労働委員会は、平成17年8月19日、被告会社に対し、①組合員の被告事務室での勤務時等における本件監視カメラ等の作動の禁止、②貸切バス運転者に対する配車における組合員と非組合員との公平な取扱い、③組合員の平成16年4月以降分の賃金月額の見直し及び差額の支払及び④文書掲示を命じた、愛媛県労委平17・8・19（平成16年（不）3号）公刊物未登載。

自体の必要性和相当性を判断するほうが適切であろう⁵⁸。

また、東起業事件では、被告 Y 社が、女性従業員一人に留守番をさせることを恐れ、事務所全体を俯瞰できる監視カメラを設置したところ、原告労働者 X がプライバシー権を侵害されたと主張した。裁判所は、本件監視カメラを設置した必要性（セキュリティの向上）と設置された場所に合理性があり、「事務所内のカメラは、X の動静をつぶさに観察できるものであり、X が、前年の本件減給処分による精神的圧迫の中、更なる圧迫感を感じたことは理解し得ないでもないが、事務所内のカメラは、事務所内全体を俯瞰することができるものであり、X の座席のみを撮影するものではないし、……X の上司が（X が利用した）パソコンで X の動静を終始観察していたこと（下線は筆者による）を認めるに足りる証拠もない」とし、X の上記の請求を退けた⁵⁹。本判決が監視カメラそのものの適法性を正面から審査した点は適切であるが、監視の利用が労働者のプライバシー権や人格権にもたらす脅威に鑑みれば、同じ目的を達成できる、監視カメラよりも侵入性の低い手段があったかどうか（手段の代替可能性の審査）や、使用者が監視カメラを設置する前に労働者に十分な情報を提供していたかなどを考慮に入れるべきである。また、同判決は、上記判旨の下線部、つまり、使用者が特定の従業員の動静を絶えず監視している場合、そのような監視が直ちに違法であってプライバシー侵害等が生じるかどうかを明らかにしていない。学説上も、本件監視カメラの目的が従業員の業務自体を監視するものではないとしても、従業員の行動を監視する機能を有していたのであるから、監視の適法性について積極的に検討

⁵⁸ プライバシー侵害の成立が成立するかどうかは場所の性質に左右されとする本判決の見解は、裁判例では必ずしも一般的ではない。民事事件では、単に撮影された場所が不特定多数の者が通行するであるということだけで、プライバシーや肖像権の侵害を否定するのは相当ではなく、監視が特定の個人に対して継続的に行われていたかどうか、または個人が当該監視を予測できたかどうかが考慮されるべきであるとした判決が多く存在している。例えば、大阪地判平 6・4・27 判時 1515 号 116 頁や、東京地判平 21・5・11 判時 2055 号 85 頁などがある。前者の大阪地判は、「公道においても、通常は、偶然かつ一過性の視線にさらされるだけであり、特別の事情もないのに、継続的に監視されたり、尾行されることを予測して行動しているものではないのであって、その意味で、人は一歩外に出るとすべてのプライバシーを放棄したと考えるのは相当でない。……公共の場所にいるという一事によってプライバシーの利益が全く失われると解するのは相当でなく、もとより当該個人が一切のプライバシーの利益を放棄しているとみなすこともできない」と判断した。

⁵⁹ 東京地判平 24・5・31 労判 1056 号 19 頁。

されるべきであるとの指摘がある⁶⁰。また、上記判断に続き、「事務所にカメラを設置することに防犯上の必要性、合理性が認められる上、……X の上司が本件カメラを事務所に設置することを X に内密にしていたからといって、直ちに本件監視システム設置に係る不法行為が認められるわけではない」とも判断された。しかし、本件監視カメラの設置に正当な目的があったとしても、それは使用者が労働者に通知することなく監視カメラを導入したことの適法性の問題とは無関係であると理解すべきであるからである。これはまさに、監視に関する裁判例において、どのように監視を適正に行うかという判断枠組みが欠如していること示している。

このほか、被告 Y 病院が、原告労働者 X の使用する部屋のドア上部に一台の監視カメラを設置したことが、X のプライバシーないし人格権を侵害したか否かが争われた F 病院事件において、裁判所は、上記カメラは、階段及びエレベーター乗降口を出入りする人の姿を映してはいるものの、X の部屋のドアや当該部屋を出入りする人の姿を映してはいないこと、同病院に X の使用していた部屋のドア上部のものとほぼ同じカメラがあるからすれば、「Y が X の行動を監視するために防犯カメラを設置したとは到底認められない。さらに、X の部屋のドア上部の防犯カメラが映す範囲からすれば X に何らかの損害が生じているものとも認められない。したがって、Y による上記防犯カメラの設置が X に対するパワーハラスメントに当たり、X のプライバシー権及び人格権を侵害したとは認められない」と判断した。しかし、監視カメラが従業員を直接監視していないとはいえ、監視カメラに映った場所（階段やエレベーターの乗降口）から従業員の動向を把握することは十分可能であるため、上記判断には疑問が残る。

近時、監視の実施に先立つ使用者による通知義務の重要性を明示した判決が現れた。所持品検査の様子が監視カメラの撮影範囲に入ったことが原告労働者 X のプライバシー権を侵害したかどうか争われたセコム事件において、裁判所は、まず、本件監視の目的について、「現金などの貴重品を扱う機会の多い業務に従事する従業員が、貴重品の紛失、盗難等の事案が発生した場合に、身の潔白を証明する機会を保障する」とし、次に、本件監視の態様について、「所持品検査の様子が、設置されている防犯カメラの撮影範囲に入ってしまうことがあるとしても、防犯カメラの設置目的も鍵保管庫や回収物の送

⁶⁰ 大内伸哉「キーワードからみた労働法（156）従業員のモニタリング」ビジネスガイド 888 号（2020 年）82 頁。

達準備を行う作業場を撮影・記録するといった正当なものであることからすると、やむを得ないもの」と判断し、最後に、本件監視を行う前に使用者からの従業員への通知の有無について、「X は、入社時の新人社員研修や、勤務開始時の点呼の際に、所持品検査に関する説明を受けていたのであるから、このような所持品検査が行われることを理解し、これを受容して業務に従事していた」とし、本件監視は適法であり、プライバシー侵害には該当しないと判断した⁶¹。

(iii.) 電子メールとコンピュータの使用から生じる問題

(a) 電子メール私用と私的チャットの問題

電子メールの私的利用の問題に関しては、比較的多くの裁判例が蓄積されている。まず、日本において初めてこの問題に判断を下した F 社 Z 事業部事件を検討する。この事件では、原告労働者 X に対するセクハラ疑惑があった被告使用者 Y は、監視に関する何らの規定（就業規則等）もない下で、原告労働者 X の電子メールを監視し、さらに X が監視を察知した後、パスワードを変更した後も、IT 部門の担当者に依頼し、X の電子メールの送受信に対する監視を続けていた。X は、上記 Y の行為がプライバシー侵害に当たるとして、訴訟を提起した。裁判所は、まず、従業員による電子メールの私的利用にプライバシーがあるか否かという点について、「勤労者として社会生活を送る以上、日常の社会生活を営む上で通常必要な外部との連絡の着信先として会社の電話装置を用いることが許容されるのはもちろんのこと、さらに、会社における職務の遂行の妨げとならず、会社の経済的負担も極めて軽微なものである場合には、これらの外部からの連絡に適宜即応するために必要かつ合理的な限度の範囲内において、会社の電話装置を発信に用いることも社会通念上許容されていると解するべきであり、……社員の電子メールの私的使用が前記の範囲に止まるものである限り、その使用について社員に一切のプライバシー権がないとはいえない」と判示した⁶²。そして、これに続いて、電子メールの私的利用と業務用の電話の私的利用は基本的に同一視することができるが、電話の保守点検が原則として法的な守秘義務を負う電気通信事業者によって行われ、事前に特別な措置を講じない限り会話の内容そのものは即時に失われるという観点から、使用者のネットワークシステムを通じて

⁶¹ 東京地判平 28・5・19 労経速 2285 号 21 頁

⁶² 東京地判平 13・12・3 労判 826 号 76 頁。

送受信する電子メールの私的利用は、「電話装置の場合と全く同程度のプライバシー保護を期待することはできず、当該システムの具体的状況に応じた合理的な範囲での保護を期待し得るに止まるものというべきである」とした。最後に、従業員による電子メールの私的利用が使用者が監視する必要性と、労働者のプライバシー権との間のバランスを如何にして図るかについて、「①職務上従業員の電子メールの私的使用を監視するような責任ある立場にない者が監視した場合、あるいは、②責任ある立場にある者でも、これを監視する職務上の合理的必要性が全くないのに専ら個人的な好奇心等から監視した場合、あるいは、③社内の管理部署その他の社内の第三者に対して監視の事実を秘匿したまま個人の恣意に基づく手段方法により監視した場合など、監視の目的、手段及びその態様等を総合考慮し、監視される側に生じた不利益と比較衡量の上、社会通念上相当な範囲を逸脱した監視がなされた場合に限り、プライバシー権の侵害となると解するのが相当である」と判断し、結論として、プライバシー侵害は成立しないとした。一方、学説では、電子メールの私的利用に対して労働者のプライバシーの存在を認めたこの判決の判断を支持する見解は多いが、次の 3 点、すなわち、①電子メールの私的利用に対するプライバシー保護への期待が、私用電話のそれよりも低いとされている点、②上記 X の電子メールを監視したことは、セクハラが疑われた使用者 Y 本人である点、③使用者が正当に監視できる基準を示した本件判旨に照らせば、本件における電子メールの私的利用の監視は Y の個人的行為と評価されるべきであるため、そもそも本件監視には合理性と必要性がなかった点に

対しては批判的意見も存在している⁶³。

また、F 社 Z 事業部事件から 1 年後の日経クイック情報事件では、被告会社 Y が電子メールを用いた誹謗中傷事件の調査過程で、原告労働者 X のメールボックスを調査したこと（本件調査）が、プライバシー侵害にあたるかどうか争われた。裁判所は、まず、「（本件の）調査や命令も、それが企業の円滑な運営上必要かつ合理的なものであること、その方法態様が労働者の人格や自由に対する行きすぎた支配や拘束ではないことを要し、調査等の必要性を欠いたり、調査の態様等が社会的に許容しうる限界を超えていると認められる場合には労働者の精神的自由を侵害した違法な行為として不法行為を構成することがある」との原則を示した上で、本件調査の必要性について、「私用メールは、送信者が文書を考え作成し送信することにより、送信者がその間職務専念義務に違反し、かつ、私用で会社の施設を使用するという企業秩序違反行為を行うことになることはもちろん、受信者に私用メールを読ませることにより受信者の就労を阻害することにもなる。このような行為は、…懲戒処分の対象となりうる行為である。そして、業務外の私用メールであるか否かは、その題名だけからの確に判断することはできず、その内容から判断する必要がある」とし、本件調査の相当性について、「業務に何らかの関連を有する情報が保存されていると判断されるから、ファイルの内容を含めて調査の必要が存する以上、その調査が社会的に許容しうる限界を超えて X の精神的自由を侵害した違法な行為であるとはいえない」とし、X が本件調

⁶³ 砂押以久子「判批」労判 827 号（2002 年）31-32 頁、永野仁美「判批」ジュリ 1243 号（2003 年）155-156 頁、竹地潔「判批」ジュリ 1246 号（2003 年）206-207 頁、藤内和公「会社内の私用電子メールに対する使用者による監視の可否」法時 75 巻 5 号（2003 年）103 頁、西谷敏『人権としてディーセント・ワークー働きがいのある人間らしい仕事』（旬報社、2011 年）284-285 頁。上記藤内論文では、私用電話が行われた態様により、プライバシー保護に対する合理的期待が異なり、すなわち、「私用電話は労働者が大部屋事務室で就労しているか、それとも個室で就労しているかにより、保護の合理的期待は大きく異なる」と指摘されている（102 頁）。①に関しては、日本の職場のレイアウト（島型対向式）に関する特殊性に照らして、「隣の隣の島での電話や話も筒抜けてある。そのため、電話の私用は自然に必要最低限に抑制される。ここでは、仕事をしているふりをして静かに私的に利用しやすい E メールの方に、社員はむしろ電話よりも高いプライバシーを期待しがちである」との指摘がある。真嶋理恵子「判批」NBL734 号（2002 年）7 頁参照。なお、今後 AI による監視は、本件でセクハラ疑惑の対象となった上司による直接の監視よりも、監視実施の恣意性を軽減できる可能性があるとの指摘もある。尾崎愛美「モニタリングと HR デクのロジー」山本龍彦＝大島義則編『人事データ保護法入門』（勁草書房、2023 年）67 頁。

査について事前に知らされていなかった点について、「まず、X に調査することを事前に告知しなかったことは、事前の継続的な監視とは異なり、既を送受信されたメールを特定の目的で事後に調査するものであること、X が誹謗中傷メールと私用メールという秩序違反行為を行ったと疑われる状況があり、事前の告知による調査への影響を考慮せざるを得ないことからすると、不当なこととはいえない」と判断した⁶⁴。この判決に対しては、学説上、疑義を呈する見解が多く存在している。たとえば、本判決が労働者のプライバシー権に言及しなかったことは、労働者のプライバシー保護の観点から、前掲 F 社 Z 事業部事件判決よりも後退しているとの見解⁶⁵、労働者の職務専念義務を本判決のように厳格に捉えると、いかなる私用メールも違法なものになりかねず、さらに私用メールに関する労働者のプライバシー権等の人格的利益が無に帰するそれもあるとの懸念を示した見解⁶⁶、労働者に証拠隠滅行為を行わないよう業務命令を発した上で私用メールを調査することが可能であったにもかかわらず、本判決が事前告知の欠如を認めた点に疑問があるとの見解がある⁶⁷。

上記両事件以降の電子メールの私的利用に関する事件の大半は、使用者が従業員の電子メールの利用状況を監視することが従業員のプライバシー権を侵害するか否かの事件ではなく、職務専念義務違反による懲戒処分や解雇の事件である。これらの事件では、私用メールの量、私用禁止を定めた規程の有無、使用者による事前の注意や警告の有無に照らして、労働者が職務専念義務に違反したかどうか、使用者に懲戒権と解雇権の濫用があったかどうかを

⁶⁴ 東京地判平 14・2・26 労判 825 号 50 頁。

⁶⁵ 砂押・前掲注 2) 10 頁、龔敏「判批」法政研究 69 巻 4 号（2003 年）193 頁、荒木尚志「判批」堀部政男＝長谷部恭夫編『メディア判例百選』（2005 年）235 頁、原昌登「判批」村中孝史＝荒木尚志『労働判例百選（第 8 版）』（2009 年）61 頁。

⁶⁶ 砂押・前掲注 63) 34 頁、竹地・前掲注 63) 206 頁。

⁶⁷ 砂押・前掲注 63) 34 頁。しかし一方で、「嫌がらせメールの犯人を捜すという具体的な業務上の必要性があったことから、本人に閲読を事前に知らせないことの必要性があった」という見解もある、藤内・前掲注 63) 103 頁。

判断する傾向が見られた⁶⁸。

(b) 業務用コンピュータに対する調査の問題

使用者が労働者の業務用コンピュータが私的に利用されたか否かを調査する事案において使用される判断基準は、私用電子メールの場合に使用される基準とほぼ同じである。ここでは、この問題に関するいくつかの裁判例を取り上げて検討する。

まず、この問題に関する最初の判決として、職員の内部告発による批判記事を調査するため、被告会社 Y が、原告労働者 X が使用していた業務用コンピュータを調査したことが、X のプライバシー権を侵害したかどうか争われた労働政策研究・研修機構事件において、裁判所は、本件調査は X に無断で行われたため、調査によって得られた証拠はプライバシー侵害を理由に訴訟から排除されるべきであるとの X の主張に対し、「使用者の行為がプライバシー権の侵害にあたる場合であっても、そのようにして収集された証拠が証拠能力を欠くものとして証拠排除の対象となるのは、その侵害の程度が著しい場合に限られるというべきである」という原則を示し、業務用のコンピュータの使用履歴を調査したことがプライバシー侵害にあたるという X の主張に対し、「本件パソコンに関する調査は、Y が本件記事に関する事実関係を明らかにして監督官庁への説明をするなどの目的で行われたものであり、その態様は、リース元への返却に伴い X から回収した後で、調査項目をパソコン作業の対象となった電子ファイルの保存場所、ファイル名、作業開始日時、継続期間等に限って調査するというものであって、調査目的が正当である上、調査態様も妥当であり、X の被る不利益も大きくないから、プライバシー権の侵害にあたるということはできない」と判断した⁶⁹。本判決では、使用者がプライバシー侵害にあたる手段で収集した証拠を排除すべきか否かという

⁶⁸ 例えば、従業員懲戒処分及び解雇を有効した事件としては、K 工業技術専門学校（私用メール）事件（福岡地判久留米支部平 16・12・17 労判 888 号 57 頁、福岡高判平 17・9・14 労判 903 号 68 頁）、ドリームエクスチェンジ事件（東京地判平 28・12・28 労判 1161 号 66 頁）があるのに対し、懲戒処分等を無効とした事件としては、グレイワールドワイド事件判決（東京地判平 15・9・22 労判 870 号 83 頁）、全国建設工事業国民健康保険組合北海道東支部事件（札幌地判平 17・5・26 労判 929 号 66 頁）、トランスシステム事件（東京地判平 19・6・22 労経速 1984 号 3 頁）、北沢産業事件（東京地判平 19・9・18 労判 947 号 23 頁）、ノーリツ事件（神戸地判令 1・11・27 LEX/DB 25564452）がある。

⁶⁹ 東京地判平 16・9・13 労判 882 号 50 頁、控訴審（東京高判平 17・3・23 労判 893 号 42 頁）は一審のプライバシー侵害に関する判断を支持した。

問題が正面から判断された点において特徴がある。また、結論として、本件で証拠排除が否定されたが、「プライバシー侵害の程度が著しい」場合に証拠排除の可能性を肯定した意義は大きいと考えられる⁷⁰。

また、原告労働者 X が、職場でパワーハラスメントや暴行を受けた後、業務用コンピュータを利用し、検察官及び公平委員会への上申書と新聞社に記事の掲載を依頼する文書を作成したことを知った被告 Y1 村の職員 Y2 と Y3 が、X 立会い下で X が利用した上記パソコンの内容を開示したことが、X のプライバシー侵害にあたるかについて争われた美浦村・美浦村職員組合事件において、裁判所は、「Y2 と Y3 が内容の確認の対象としたのは、X が使用していたとはいえ Y1 所有のパソコンであって、もともと私的な使用を禁じられた私的文書の保管が予定されていない物品であり、Y2 と Y3 の調査の目的も X が勤務時間中に職務専念義務に違反して文書の作成をしていたことを確認するという正当なものである。なるほど、労働者といえども個人として生活を送っている以上、就業時間中に外部との連絡を取ることが一切許されない訳ではなく、使用者に過度の経済的な負担をかけないなど社会通念上相当と認められる限度で使用者のパソコンを利用して私用メールを送信する様な行為が職務専念義務に違反しないと解する余地がないではない」という原則を示し、「Y1 の情報セキュリティポリシーにおいては、そのような場合についても、Y1 側において端末の利用状況の調査を行うことができる場合を定めている。

⁷⁰ また、民事訴訟法には、刑事訴訟法のように捜査機関による違法な捜査手法を抑制する目的はないが、一方当事者が違法に収集した証拠を利用し、当事者の公平や武器対等原則を侵害することを防止するために、一定の場合において違法に収集した証拠の証拠能力を制限する議論が展開されてきた。下級審では、本人に無断で提出された録音テープの証拠能力をめぐる争われた事件が多く見られる。例えば、非公開とされたハラスメント防止委員会に出席していた原告が、自分を侮辱する委員の発言を無断で録音し、その録音の証拠能力が争われた学校法人関東学院事件（東京高判平 28・5・19 LEX/DB25542758）がある。同判決は、「非公開とされる防止委員会の審議は、何者かによって無断で録音されたものであり、違法に収集された証拠といえる。民事訴訟法は、自由心証主義を採用し（同法 247 条）、一般的に証拠能力を制限する規定を設けていないことからすれば、違法収集証拠であっても、それだけで直ちに証拠能力が否定されることはない……が、いかなる違法収集証拠もその証拠能力を否定されることはないとすると、私人による違法行為を助長し、法秩序の維持を目的とする裁判制度の趣旨に悖る結果ともなりかねないのであり、民事訴訟における公正性の要請、当事者の信義誠実義務に照らすと、当該証拠の収集の方法及び態様、違法な証拠収集によって侵害される権利利益の要保護性、当該証拠の訴訟における証拠としての重要性等の諸般の事情〔下線は筆者による〕を総合考慮し、当該証拠を採用することが訴訟上の信義則（民事訴訟法 2 条）に反するといえる場合には、例外として、当該違法収集証拠の証拠能力が否定される」とし、結論として、証拠としての録音を訴訟から排除すると判示した。

そうすると、Y1 は、職員に対し、利用を許しているパソコンについてその利用状況の調査がされる場合があることを周知していたといえることができる。以上に照らすと、私的利用の許されていなかったパソコン内に職務専念義務に違反して違法に作成・保管した文書データの開示を拒む理由としてプライバシー権を主張する X の主張は採用できない」と判示した⁷¹。この事件には、2 つの特徴がある。一つは、本件で X が請求したのは、前述の F 社 Z 事業部事件のように、使用者による調査が労働者のプライバシーを侵害したかという点が争われたという点、もう一つは、F 社 Z 事業部事件とは異なり、Y1 には、使用者が業務用のコンピュータを調査できることを定めるセキュリティ・ポリシーがある点である。しかし、X の職務専念義務違反を根拠に、Y2 と Y3 が業務用コンピュータ内の X の私的な内容を開示したことを適法とした上記判断には疑問がある。というのも、本件では、X は事前に業務用パソコンに保存された私的なファイルが調査される可能性があることを認識していたため、本件調査は正当であるとされたが、調査自体は正当であっても、使用者が従業員の私的なファイルを開封できるかどうかは別個の問題だからである。すなわち、労働者が業務用のコンピュータで作成した私的なファイルの私的性質は、職務専念義務違反の有無に関わらず、変わらないと理解されるべきである。そのため、使用者が労働者の私的なファイルにアクセスすることが正当化されるには、より労働者のプライバシーと調和できるような判断枠組みが必要であると考えられる。

このほか、被告会社 Y が、秘密裏に監視ソフトを導入し、原告労働者 X の勤務時間中のインターネット閲覧を監視した結果、X が業務と関係のないウェブサイトを閲覧していたことを理由に解雇された公益財団法人ブルーシー・アンド・グリーンランド財団事件において、裁判所は、「就業時間中のインターネット閲覧に関する Y の証拠収集方法は相当ではないと考えるが、さりとて、X の行動が正当化されるわけではないので、本件解雇の判断には影響しない」とした⁷²。本判決は、使用者が従業員に通知しなかった（秘密裏に）監視ソフトを利用したこと自体は相当ではないと認識しつつも、X が職務専念義務に違反したことを考慮した上で、上記監視ソフトを適法とした。しかし、本判決が従業員の上記義務違反をもって「相当ではない」監視装置を正

⁷¹ 水戸地判平 24・9・14 判例地方自治 380 号 39 頁。控訴審（東京高判平 25・3・13 LEX/DB 25500342）も同じ判断を下した。

⁷² 東京地判平 27・3・27 労働判例ジャーナル 41 号 67 頁。

当化する点には疑問がある。というのも、本件は重大な犯罪を犯した従業員を特定するような事件ではなく、上記監視ソフトの存在を従業員に事前に通知することにより、むしろ従業員が私的な目的で業務用パソコンの使用を控えるインセンティブを与える可能性があるからである。

(iv.) GPS 機能付き装置による監視

公判判例集上、使用者がGPS装置を使用して労働者の居場所を監視する事件は一件のみである。上記監視カメラの箇所で検討した東起業事件では、原告労働者 X の緊急連絡や業務状況を把握する目的で、被告 Y 社が導入したナビシステムが、X のプライバシー侵害や X に対するハラスメントとして不法行為を構成するか否かが争われた。この事件において、裁判所は、GPS システムの導入の目的、すなわち、従業員の勤務状況を把握し、緊急時に対応するための必要性を認めたが、「早朝、深夜、休日、退職後のように、従業員に労務提供義務がない時間帯、期間において本件ナビシステムを利用して原告の居場所確認をすることは、特段の必要性のない限り、許されない」とし、勤務時間外の GPS による監視を違法と判断した⁷³。

(2) 学説上の議論

(i.) 全体的状況

職場における監視の議論は、労働者のプライバシー権に関する豊富な議論に比べ、全体的に低調である。日本での監視に関する学説上の議論は早い段階から始まっており、所持品検査のような使用者による直接的な監視については、すでに1960年代後半から議論されていた。1980年代後半に日本に先行して情報化社会に突入したドイツ等の職場で生じた電子機器による監視の問題を紹介し、警鐘を鳴らす学説⁷⁴は存在したものの、そのような状況は「近未来」の問題であると捉えられていたため、大きな注目を受けることはなかった。その後、1990年代後半、電子メールの利用が普及したことで、主にプライバシー保護の観点から電子メールの監視の問題に関する議論が一時的に活発になったものの、前述の F 社 Z 事業部事件判決と、それをめぐる議論がある程度蓄積された後は、電子メールの監視についての議論は沈静化すること

⁷³ 東京地判平 24・5・31 前掲注 59。

⁷⁴ 角田邦重「西ドイツにおける人格権の保障」横井芳弘編『現代労使関係と法の変容』（勁草書房、1988年）376頁と400-402頁。

となった。その後、学説の関心は、個人情報保護法と労働法が交錯する領域の問題と移行した。特に、2005年に施行された前述の個人情報保護法を契機として、一部の学説は、同法の規定や前述の行政解釈等（第1章第2節）を参考にし、使用者は監視を実施する前に、監視の目的を事前に特定し、労働者に監視装置の存在を通知する必要があると主張した⁷⁵。近時、監視に関する学説の関心は、GPS機能付き装置、RFID（Radio Frequency Identification）による新たな監視またはテレワークの実施がもたらす監視の問題へと移行した。

以下では、電子メールの私的利用の監視をめぐる問題やGPS機能付き装置による監視等の問題に関する学説上の議論を検討する。

（ii）電子メールの私的利用をめぐる学説上見解の対立

学説上、職場における私用電子メールの監視がプライバシー侵害にあたるかどうかを最初に判断した前掲のF社Z事業部事件を契機として、電子メールの利用について議論が巻き起こった。そのなかで、就業規則等においてあらかじめ電子メールの監視・閲読の規程が設けられている場合に、使用者がそれを合法的に監視・閲読することができるのか、言い換えれば、労働者が業務とは関係ないメールに関するプライバシーを主張できなくなるのかについては、学説上の議論は大きく2つの見解に大別できる。一つは、使用者が就業規則等で事前に私用メール禁止に関する規程を定めている場合、このようなメールに対する労働者のプライバシー保護への期待はそもそも生じないとする見解⁷⁶と、もう一つは、たとえ電子メールの私用を禁止する規程があっても、プライバシー保護の観点から、使用者の監視権限に何らかの制限を加える必要があるとする見解⁷⁷である。前者の見解を最初に提示したのは、電子メールをめぐるアメリカ法上の議論を紹介した竹地（1997年）の論文である⁷⁸。ここでは、上記竹地の見解をよりよく理解するため、同論文で紹介さ

⁷⁵ ②砂押・前掲注22）67頁。

⁷⁶ 竹地潔「電子メールのモニタリングと嫌がらせメール」学会誌90号（1997年）56頁、原・前掲注65）61頁、荒木尚志「判批」長谷部恭男ほか編『メディア判例百選（第2版）』（2018年）235頁、菅野和夫『労働法〔第12版〕』（弘文堂、2019年）695頁、川口美貴『労働法〔第6版〕』（信山社、2022年）183頁。

⁷⁷ 砂押・前掲注63）37頁、藤内・前掲注63）100頁、永野・前掲注63）155-156頁、弘田彩加＝土田道夫「業務用パソコンを用いた就業時間内の私的メール交信等を理由とする懲戒処分の効力」同志社法學60巻8号（2009年）486-487頁。

⁷⁸ 竹地潔「電子メールのモニタリングと嫌がらせルール」日本労働法学会誌90号（1997年）56頁。

れたアメリカ法におけるプライバシーの合理的期待（Reasonable expectation of privacy）の法理とその後の労働事件への転用について、簡潔に紹介する⁷⁹。アメリカ法において、プライバシー保護に対する合理的期待を確立した判決は、連邦捜査局（FBI）による公衆電話の傍受が、アメリカ憲法修正 4 条⁸⁰におけるプライバシー侵害に当たるかどうかアメリカ連邦最高裁で争われた Katz 事件⁸¹である。この判決の補足意見において、Harlan 判事（John Marshall Harlan II）は、プライバシー権がアメリカ憲法修正 4 条の保護を受けるためには、「第 1 に、個人がプライバシーに対する期待を示していること（プライバシー保護に関する主観的要件）、第 2 に、その期待が客観的に合理的であると承認されていること（プライバシー保護に関する客観的要件）」という要件を満たす必要があると述べた⁸²。これは、言い換えれば、アメリカ憲法修正 4 条によって保護されているプライバシー権は、まず主観的期待を有し、さらにその期待が社会的（客観的）に合理的なものと認められるものでなければならないということである。この法理は、その後、労働事件の O'Connor 事件⁸³においても転用された。この事件で、アメリカ連邦最高裁は、従業員が使用していたオフィス内にある机及び書類箱に対する捜査がプライバシーを侵害すると認めるためには、①従業員が、上記物品に対して「社会通念上合理的であると認められるプライバシー保護への合理的期待」を有し、次に②「諸般の状況に照らした合理性」もあることが必要であると判示した。この判断を

⁷⁹ Katz 事件の詳細については、石井夏利生『個人情報保護法の理念と現代的課題－プライバシー権の歴史と国際的視点－』（勁草書房、2008 年）128-130 頁参照。

⁸⁰ 不合理な搜索及び逮捕押収に対し、身体、住居、書類及び所有物の安全を保障される人民の権利は、これを侵害してはならない。令状はすべて、宣誓又は確約によって支持される相当な根拠に基づいていない限り、また搜索する場所及び逮捕押収する人又は物が明示されていない限り、これを発してはならない。

⁸¹ Katz v. United States, 389 U.S. 347 (1967).

⁸² *Id.* 389 U.S. 361 (1967).

⁸³ O'Connor v. Ortega, 480 U.S. 709(1987).この事件では、カリフォルニア州立病院 Y が、同病院によって雇用されていた精神科医である原告労働者 X での職務上の不正の嫌疑（セクハラ等）を抱き、その後の懲戒処分で用いられる証拠を収集するために原告労働者のオフィス（机やファイル・キャビネット）を捜査し、証拠となるものを押収した後、原告労働者を解雇した。アメリカ連邦最高裁は、オフィス内の机とファイル・キャビネットは 17 年間 X が排他的に占有していたことから、「X は机とファイル・キャビネットにはプライバシーの合理的な期待を有していた」とした。事件の詳細については、高井裕之「職場におけるプライバシーと修正四案」判タ 675 号（1988 年）43 頁参照。

受け、従業員の私的なメールの開封に関するその後の判決も、O'Connor 事件判決で示された基準に照らして判断してきた⁸⁴。このように、従業員の私的なメールの開封について、アメリカ法においては、一般的には、従業員は私的な電子メールに対して主観的なプライバシー保護への期待を有するが、企業が事前に電子メールを監視する規程を設けている場合、その期待は客観的に合理的を欠くものとされている⁸⁵。しかし、私的な電子メールに対する従業員の主観的期待が、客観的にも合理的であることを従業員が証明することは困難であるため、アメリカ法では私的な電子メールに対するプライバシー保護は非常に限定的であり、使用者による監視が広く認められている。上記の竹地の見解は、前述したアメリカ法のプライバシー保護に対する合理的期待の法理を踏まえ、使用者が就業規則等で事前に私用メール禁止に関する規程を定めている場合、当該メールに対する労働者のプライバシー保護への期待はそもそも生じないと主張したのである。

これに対して、後者の見解を最初に主張した砂押は、フランス法を参考にし、労働者のプライバシー権は、制限されることはあっても、否定されることはないため、使用者が従業員の私的な電子メールの禁止に関する規程等を事前に定めていたとしても、従業員の私的な電子メールの調査・監視を行う際には、依然として労働者のプライバシーに配慮する必要があると主張した⁸⁶。この見解を支持する見解として、たとえ私用メールが企業のサーバーに保存されていたとしても、電子メールの利用権限が個々従業員に割り当てられた時点で、その使用から生じる私的領域があることから、使用者による監視・調査活動が当然に正当化されるわけではないというものがある⁸⁷。

このほか、私用メールの禁止と私用メールの内容の閲覧を区別することを強調した藤内の見解がある⁸⁸。藤内は、就業規則等に電子メールの私用を禁止する規定があったとしても、労働者がそれに違反したというだけで、使用者

⁸⁴ 竹地・前掲注 76) 45 頁。

⁸⁵ 竹地・前掲注 76) 46-47 頁参照。

⁸⁶ 砂押以久子「労働者のプライバシー保護」ジュリ増刊（2014 年）21 頁。

⁸⁷ 永野・前掲注 63) 155 頁。この見解によれば、監視の目的・手段等を総合的に考慮する必要があるとした F 社 Z 事業部事件判決の判断基準は、「ほぼ妥当といってよい」が、前掲西日本鉄道事件判決の判断基準に照らせば、監視の対象となる労働者への通知と当該監視を制度として画一的に実施する必要があることが指摘された（156 頁）。

⁸⁸ 藤内・前掲注 63) 100 頁。

が従業員の私的な電子メールの内容を閲読することはできず、使用者がそれを閲覧しようとする場合には、労働者の真意に基づく同意を得る必要があると主張している⁸⁹。ただし、労働者から上記同意を得ることができない場合でも、例外的に使用者によるメール調査が適法と判断されることがあるとする⁹⁰。その際の判断要素は、①労働者が電子メールについて合理的なプライバシー保護への期待を抱いていたかどうか（使用者が電子メールの私用を禁止していたか、私用メールに対して使用者が閲覧する可能性があることが周知されていたか、他の労働者のメールも閲読をしていたか、同僚の電子メールに他人がアクセスすることが容易であったか否か）、②使用者が従業員の私的な電子メールを閲読する業務上の必要性の有無、その程度、閲読の方法が適切かどうか（労働者が電子メールを使用することで企業秘密が漏洩するリスクがある場合、または、閲覧が無断で行われた場合、使用者が事前に労働者にその旨を通知できない事情が存在したかどうか）、③監視による労働者の利益に対する侵害が比例しているかどうか（侵害手段が目的達成に必要な程度、方法であったか、実施された監視が一回限り、あるいは継続的に行われたのか、閲読された内容は、センシティブなものであったか）である。以上の議論から理解できるように、従業員の私的な電子メールの監視の問題に関しては、私的なメールの禁止に関する規定があった場合でも、労働者には依然としてプライバシー保護の期待があるかどうか学説上の議論の中心となっているが、電子メールの監視それ自体の適法性をどのように判断すべきかについては十分な議論がなされていないように思われる。また、使用者が労働者の私的な電子メールを閲読することの適法性を判断する際に、第 1 段階として労働者の真意に基づく同意を求めるとする藤内の見解があるが、労使間の交渉力の格差や情報量の非対称性を考慮すると、労働者が使用者による監視を拒否できるとは考えにくい。そのため、結局、使用者による私的な電子メールの閲読の適法性の判断は、第 2 段階である前述の 3 要素（事前通知の有無等を含むプライバシー保護への合理的期待の有無、必要性、比例性の審査）を中心に行われることとなる。このように、労働者の同意を第 1 段階で求めること自体には意義が乏しく、第 2 段階における私的な電子メールの閲読の適法性を審査するため前述 3 要素からなる基準を、第 1 段階に移動す

⁸⁹ 同上注 102 頁。

⁹⁰ 同上注 102-103 頁。

る方が適切であろう⁹¹。さらに、藤内説の第2段階の審査は要件ではなく、要素からなるものであるが、ますます高度化する監視装置の適法性に対する審査に際しては不十分である。そのため、要素ではなく、明確な要件からなる監視の適法性を審査する判断枠組みを構築する必要があると思われる。

(iii.) GPS 使用による監視とテレワークの実施に伴う監視

使用者が労働者の位置を監視するために GPS 装置を利用することについては、下記の竹地の論文を除き、学説上ではほとんど議論されていない。ここでは、竹地の論文の要点を整理する⁹²。まず、竹地は、GPS機能付き装置はその他の監視装置とは異なり、従業員の位置を精確かつ継続的にリアルタイムで特定・把握できる特徴があり、その利用によって従業員が地理的奴隷（Geo-slavery⁹³）とされる可能性があるとは指摘した⁹⁴。次に、GPS 機能付き装置の利用がもたらす問題は、使用者が収集した位置情報の分析を通じて労働者の行動履歴を取得し、その行動履歴を「その他の個人情報等とを紐付けることにより、労働者の人物像を明らかにする」ことができるという点にあると強調された⁹⁵。さらに、竹地は、GPS機能付き装置の使用を勤務時間中に使用される場合と勤務時間外に使用される場合に分けて、それぞれに制限を加

⁹¹ 監視の適法性の判断における同意の位置付けに関しては、第5章第2節3款参照。

⁹² ①竹地潔「スマホとともに、ジオスレイバリーがやって来る！—GPSに基づく労働監視 vs 労働者のプライバシー・人格権—」富山大学紀要・富大経済論集 58 巻 2, 3 号（2013 年）、②同「スマート化する職場と労働者のプライバシー」日本労働研究雑誌 663 号（2015 年）。

⁹³ J. E. Dobson & P. F. Fisher, *Geoslavery*, IEEE TECH. & SOC'Y MAG. 47, 51 (2003). この論文では、ジョージ・オーウェルのビッグ・ブラザー（Big Brother）と Geo-slavery との違いについて、「第 1 に、LBS（位置情報サービス）はオーウェルのテレスクリーンを幼稚なものにしている。オーウェルが構想した技術は、人間の監視者が他の人間を監視し、その行動をコントロールするものである。これに対して、LBS は、1 人ひとりの個人を監視し、モデルやルールに基づいて無数の経路を評価し、自動的に指示や制裁を与えるようにプログラムすることができる。人間の視覚システムでは、1 人の観察者が 20 人、多くて 50 人の人間を監視することができるが、LBS を使用する場合は、一人の人間が無数の人間を監視でき、そのうちの一人が数センチでも道を踏み外すとすぐ発見することができるのである。第 2 に、オーウェルの警告は、いつか政府がテクノロジーを使って個人をコントロールするようになるとの警鐘を鳴らしたが、我々は、個人がテクノロジーを使用し、他の個人やグループをコントロールすることができるようになるという警告を発している。奴隷制度は好例である。というのも、歴史上、奴隷の大半は政府ではなく個人が所有していたからである」と指摘した。

⁹⁴ ①竹地・前掲注 92) 83 頁。

⁹⁵ 同上注 79 頁。

えるべきであると主張している。すなわち、勤務時間中の使用については、GPS 機能付きの携帯電話・端末等を通じて、位置情報の取得を行おうとする場合は、少なくとも、労働者本人への十分な情報提供・説明を行ったうえで、書面等で明確な同意を得なければ、適法とされないとし、他方で、勤務時間外の使用については、GPS 機能付き装置の使用は業務上の必要性はほとんどなく、その必要性があったとしてもごく稀なケースに限られるため、勤務時間外における位置情報の取扱いが適法と認められるためには、業務との関連で特別な必要があること、その必要性の旨を含め位置情報の取得・利用について十分な情報提供・説明を行ったうえで、書面等で従業員の明確な同意を得る場合に限定されるべきであり。これらの手続を履行せずに使用者が GPS 機能付き装置を利用することは、労働者のプライバシー権または人格権を侵害すると主張した⁹⁶。この見解は、GPS 機能付き装置が労働者の位置情報を継続的に収集することにより、労働者のプライバシー権を著しく侵害することを考慮し、このような装置を使用する前に使用者は労働者に通知し、労働者の同意を得ることが厳格に求められているという点で注目される。もっとも、従業員の同意を、GPS 機能を搭載した装置の適法性の要件としている点には疑問がある。まず、労使間の交渉力の不均衡を考慮すると、同意が有効であるか否かを判断することは必ずしも容易ではない⁹⁷。さらに、GPS を含めた新たなテクノロジーを搭載した監視装置の具体的な機能に関する十分な情報と知識を有しない労働者が与えた同意は、単に形式的なものになりかねず、有効な同意として認められない可能性が高い。最後に、たとえ使用者が監視装置の利用について労働者の同意を得た場合でも、労働者は事後的に同意に瑕疵があったと争う可能性があることを考慮すると、同意を監視の適法性の要件とすることの不確実性は高い。したがって、監視から労働者の人格的利益を保護するためには、同意とは別の方法で対処していく必要があると思われる（第5章第2節3款を参照）。

⁹⁶ ①竹地・前掲注92) 92頁。

⁹⁷ 山梨県民信用組合事件（最2小判平28・2・19民集70巻2号123頁）参照。

テレワーク⁹⁸の実施と監視の問題に関しては、テレワークの実施に伴って利用される Web カメラは、本人の在席をチェックするだけでなく、従業員の離席期間も自動保存するという点で、従来の人間による監視よりも高度な監視が可能となる⁹⁹。そのため、テレワークを導入する際に、「形式的には同意が取得されていたとしても、他によりプライバシー侵害の程度が低い手段があるか否かも踏まえて、モニタリングの適法性を検討すべきである」との見解もある¹⁰⁰。このほか、前述の個人情報保護法 Q&A5-7 の内容を参照し、使用者がテレワークを実施する前に、監視の目的（例えば、労働時間の適切な把握）と適切なルールを事前に就業規則等に策定する重要性を指摘した見解もある¹⁰¹。

第3款 小括

以上の検討から、裁判例において、特に機器を用いた監視に関する明確な判断枠組みが定立されておらず、それぞれの事件で審査される要件が一致していない状況が見られる。録音装置の利用について、プライバシー侵害の少ない代替手段があったかどうかを考慮した裁判例もあれば、使用者による事前の労働者への説明と協議を重視したものがあるし、監視装置の利用について従業員に通知する義務があるかどうかに関しても、裁判例の立場はまだ一致していない。さらに、監視の実施に関する裁判例は、監視の実施を個人情報処理の一形態として意識していないことが多く、個人情報処理の適法性という事情を踏まえて、監視装置の適法性を検討したものは見られない。この点は、早い段階から、監視の必要性だけでなく、それによって取得された画像の保存期間と、その録画にアクセスできた者の資格等を審査する、次章で検討する欧州の人権裁判所の立場とは大きく異なっている。

⁹⁸ テレワークの定義について、総務省は当該技術を、「ICT（情報通信技術）を活用した時間や場所を有効に活用できる柔軟な働き方」と定義している。
<https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h27/pdf/n4300000.pdf>（最終アクセス日 2023 年 11 月 27 日）。また、「パソコン、スマートフォン、タブレット端末等ネットワークに接続可能な ICT を利用して行う、所属事業場以外の場所での労働」と定義する学説もある。山川和義「サテライト・モバイルワークー雇用型テレワークと労働法上の課題」ジュリ 1522 号（2018 年）8 頁。

⁹⁹ 山川・同上注 85 頁。

¹⁰⁰ 石崎由希子「『新しい日常』としてのテレワーク」ジュリ 1548 号（2020 年）52 頁。

¹⁰¹ 松尾剛行「テレワークにおけるプライバシーの法的問題」季労 274 号（2021 年）31 頁。

一方、監視の問題に関する学説をみると、プライバシー保護の観点と上記行動指針の内容から監視の問題を検討する見解が多い。従業員の私的な電子メールの監視の問題に関しては、私的な電子メールの禁止に関する規定がある場合、労働者にプライバシー保護の期待があるかどうか議論の中心となっており、電子メールの監視それ自体の適法性をどのように判断すべきかについては十分な議論がなされていない。また、GPS 機能付き装置による監視に関しては、当該装置の利用を勤務時間中の場合と勤務時間外の場合を区別し、前者の場合には、従業員の同意と使用者による情報提供が必要であり、後者の場合には、上記同意と情報提供に加え、当該装置を使用する業務との関連で特別な必要性が求められるとの見解があった。この見解は、GPS 機能付き装置が労働者の位置情報を継続的に収集することにより、労働者のプライバシー権を著しく侵害することを考慮し、このような装置を使用する前に使用者は労働者に通知し、労働者の同意を得ることが厳格に求められているという点に注目される。ただし、従業員の同意があれば、GPS 機能を搭載した装置を適法としている点には疑問がある。というのも、労使間の交渉力の不均衡を考慮すると、労働者の同意を重視すぎることは、適切ではないからである。

最後に、テレワークの実施が自宅というプライバシーを強く要求される領域を侵害することを考慮し、使用者はテレワークの実施に伴う監視を実施する前に、よりプライバシー侵害の少ない手段の有無を検討すべきという見解もある。

第4節 まとめ

日本における監視の実施に関する法状況をまとめると、以下のようになる。まず、学説の状況をみると、2000年の労働者の個人情報保護に関する行動指針を参考にして、使用者が監視を実施する前に労働者に監視の存在を通知すべきであるとの見解と、GPS 機能付き装置による監視を実施する際に、使用者は従業員に事前に通知し、労働者の同意を得る必要があるとの見解を除き、監視の問題について本格的な研究はなされておらず、全体的に議論は低調であった。一方、使用者による監視をめぐる従来の裁判例からは、限られた事案で、ケースバイケースの判断にとどまっているという点から、監視の適法性に関する一般的な判断基準を導き出すことができない。さらに、明確な判断枠組みが欠如している問題に加え、監視に関する従来の裁判例では、監視

を情報収集の一態様として捉える意識が希薄であるという問題もある。他方、個人情報保護法及び個人情報保護委員会が策定したガイドライン等は、職場で実施される監視の特殊性には対応できないという問題もある。このように、日本では、労働者の監視の適法性について、明確な法的ルールがない状況にあった。

その結果、デジタル技術が発展するなか、使用者は明確な行為準則がないまま、ますます高度化する監視を行うことになる。しかし、不適正な監視の実施が労働者のプライバシー権等の権利を著しく侵害する可能性があることを考慮すると、こうした状況を放置することは適切ではない。すなわち、ここで求められるのは、使用者による労働者の監視がどのような場合に適法とされるのかについての明確性の高いルールが設けられ、それが使用者への行為準則として機能することである。

以上のような問題意識に基づき、第2章以下では、この問題について参考となる議論の蓄積のある欧州人権裁判所の判例とフランス法の状況を紹介し、考察することとする。

第2章 職場における監視の問題に関する欧州人権裁判所の判例法

第1節 序説

本章では、欧州人権裁判所（以下、人権裁判所と呼ぶ）の判例法における職場の監視問題を分析の対象とする。わずかな判例評釈¹⁰²を除き、人権裁判所とその判例法は、日本の労働法学においてほとんど取り上げられてこなかった。しかし、人権裁判所の判例法は、欧州人権条約（欧州人権条約はヨーロッパにおける人権および基本的自由の保護のための条約である、以下では、ECHR と略称する¹⁰³）の締約国の判例法理の変更、法制定ないし改正に大きな影響を与えるだけでなく、かねてよりドイツやフランスを主な比較法検討の対象としてきた日本にとっても重要である。人権裁判所は当初、締約国間の紛争、及び個人対国家の紛争といった締約国の消極的義務にかかる紛争しか判断の対象としていなかった¹⁰⁴。しかし、締約国の消極的義務だけでは、ECHR において保護される人権を十分に保護できず、また、公権力に比肩する私的企業等による個人の人権を侵害する可能性が高まっていることから、締約国の消極的義務と公権力対個人の伝統的な図式を超え、ECHR1 条の「人権を尊重する義務」を根拠に、締約国が私人による人権侵害を防止する積極的義務を有することも認めている¹⁰⁵。そのため、人権裁判所は、雇用関係における使用者の行為が、労働者の ECHR 上の諸権利を侵害することを防止するために、締約国が適切かつ十分な法規定または判例法理を整備しているかどうかを審査する権限を有する。とりわけ、人権裁判所は、使用者の監視と労働者の私生活保護との比較衡量の判断基準を確立したという点で、締約国に大いに影響を与えている。

以下では、まず、監視に関する国際的文書と地域的（ヨーロッパ）文書を

¹⁰² 山田省三「イギリス/職場での電話傍聴と労働者のプライバシー保護」労旬 1425 号（1998 年）26 頁、中村和夫「人権保障とクローズド・ショップ協定の効力」労旬 1049 号（1982 年）9 頁。

¹⁰³ Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 005).

¹⁰⁴ 中井伊都子「私人による人権侵害への国家の義務の拡大」法学論叢 139 巻 3 号 43 頁。

¹⁰⁵ 人権裁判所は、Marckx 事件（Marckx v. Belgium App no. 6833/74, 13 June 1979, Series A No. 31 (1979-80) 2 EHRR 330）において、締約国の積極的義務を初めて明示し、X and Y 事件（X and Y v. The Netherlands App no. 8978/80, 26 March 1985, Series A No 91, (1986) 8 EHRR 235）において、締約国は私人間の紛争における ECHR 上の権利を積極的に保護する義務があると初めて判示した。

概観し、次に、欧州評議会設立の背景と ECHR の特徴、特に ECHR8 条の「私生活等の尊重を受ける権利」、及び ECHR の制定とともに創立された人権裁判所の変容を検討し、最後に、人権裁判所が使用者による監視と労働者の私生活保護のバランスをどのようにとっているかについて、具体的な判例を抽出して考察することとする。

第 2 節 使用者による監視に関する国際的・地域的文書

第 1 款 国際的法律文書

1919 年に設立され、1946 年に国連の最初の専門機関となった国際労働機関 (International Labour Organization, ILO) によって作成された前述の労働者の個人データ保護に関する行動準則 (Code of practice on the protection of workers' personal data¹⁰⁶) は、その前言において、「コンピュータによる検索技術、自動化された人事情報システム、電子監視、遺伝子検査、薬物検査から、労働者の尊厳とプライバシーを保護し、誰がどのような目的でどのような条件の下で個人データを使用するかを決定する基本的権利を保障する」ことを目的としている。同準則は、使用者が適切に監視を実施するためには、監視の理由、実施時間、使用される方法および技術、収集されるデータについて労働者に事前に通知し、労働者のプライバシーへの侵入を最小限に抑える必要があると定めている (6-14-1)。さらに、使用者は (a) 国内法に準拠している場合、(b) 犯罪行為またはその他の重大な不正行為を疑う合理的な理由がある場合にのみ、秘密の監視を実施することができる (6-14-2)。最後に、(3) 安全衛生または財産の保護のために必要な場合にのみ、間断ない監視が許可されるべきであるとも規定している (6-14-3)。

第 2 款 地域的 (ヨーロッパ) 法律文書

(1) 閣僚委員会の雇用分野に関する勧告

欧州評議会の閣僚委員会は 1989 年に初めて労働者の個人データ保護に関す

¹⁰⁶ https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf, last visited 23 Dec. 2023.

る勧告を出した¹⁰⁷。この勧告は、雇用の目的のための情報収集と利用において、労働者のプライバシーと人間としての尊厳が十分に尊重されなければならない、特に職場における労働者の社会的・個人的関係の発展の可能性を尊重する必要があると指摘し¹⁰⁸、さらに、使用者が労働者の個人情報を収集・利用するための監視装置を導入または変更する際に、事前に従業員代表等に十分な通知または協議しなければならないとした¹⁰⁹。

その後、2015年、閣僚委員会はICTの発展がもたらす脅威に対処するために89年勧告を改訂し、締約国に対して新たな雇用関係におけるデータ処理の勧告を出した¹¹⁰。まず、使用者が電子メールの監視を行う場合、閣僚委員会は、データ処理の透明性や適法性などの原則、特に労働者に事前に通知する必要性を遵守しなければならないとし¹¹¹、さらに、使用者は業務用の電子メールにアクセスする前に、労働者による特定の操作を防止するフィルタのようなソフトウェアなどの予防措置を講じることが期待されている¹¹²とし、業務用の電子メールとは異なり、使用者はいかなる場合においても労働者の私的な電子通信の内容や送受信を監視してはならないとしている¹¹³。一方、監視カメラの利用に関しては、労働者の業務状況を直接監視する技術の導入や使用は、許されるべきではなく、監視カメラの設置が許される場合は、使用者が生産性・安全衛生または組織の効率的な運営を確保する場合のみである¹¹⁴。このような場合であっても、使用者は、監視カメラから得られた情報の保存期間や利用目的について、労働者に事前に通知し、従業員代表と協議するな

¹⁰⁷ Recommendation No.R(89)2 of the Committee of Ministers to Member States on the Protection of Personal Data Used for Employment Purposes, 18 January 1989.この勧告に言及した文献として、砂押以久子「労働者のプライバシー権の保護について（2）－フランスの現代と課題－」季労185号（1998年）189-190頁や盛誠吾「フランスにおける雇用とプライバシー・個人情報保護」堀部正男編『情報公開・プライバシーの比較法』（日本評論社、1996年）203-204頁がある。

¹⁰⁸ *Id.* (2).

¹⁰⁹ *Id.* (3-1).

¹¹⁰ Recommendation CM/Rec (2015) 5 of the Committee of Ministers to member States on the processing of personal data in the context of employment, Adopted by the Committee of Ministers on 1 April 2015.

¹¹¹ *Id.* 14.1 and 14.4.

¹¹² *Id.* 14.2.

¹¹³ *Id.* 14.4.

¹¹⁴ *Id.* 15.1

どの追加的な保護措置を講じなければならない¹¹⁵。

また、欧州評議会の諮問組織であるヴェニス委員会（Venice commission）が、2007年に職場を含む場所における監視カメラの設置に関する意見を採択した¹¹⁶。まず、同意見は、職場において従業員の私的領域が含まれ、職場内での監視カメラの使用は、労働者の私生活保護に関する法的問題が提起された¹¹⁷。監視カメラの設置は、労働者による不正行為や窃盗を防止するため、あるいは犯罪者を特定するためなど、十分な根拠がある疑いがある場合に許可されるが、特段な事情がない限り、トイレ、シャワー、休憩室、更衣室、喫煙所、従業員ラウンジなど、従業員が完全な私生活を享受できると考える場所に監視カメラを設置することは許されない¹¹⁸。さらに、従業員または従業員への事前通知なしに一時的な秘密監視を行うことは、適切な代替手段がないことが証明された場合にのみ許可される¹¹⁹。また、一般に公開されている店舗に関しては、監視カメラは、その設置が必要かつ比例的であることが証明された場合、例えば企業の財産を保護するために正当化されることができるとは、この場合においては、監視カメラは必要以上の期間を録画してはならない¹²⁰。

（2）欧州連合（EU）の状況

1995年のEUデータ保護指令¹²¹の29条により、WP29作業部会（以下では、作業部会と省略する）が設置された。作業部会は、2001年に、最初の雇用関係における個人情報の処理に関する一連の意見書（WP48）において、監視は

¹¹⁵ *Id.* 21.

¹¹⁶ Opinion on video surveillance by private operators in the public and private spheres and by public authorities in the private sphere and human rights protection, CAL-AD 027(2007) of 8 June 2007.

¹¹⁷ *Id.* §18.

¹¹⁸ *Id.* §53.

¹¹⁹ *Id.* §54.

¹²⁰ *Id.* §57.

¹²¹ 「指令」とは、加盟国にある目的を達成させるために、方法や趣旨のみを定めており、加盟国は当該目的を達成するために指令の趣旨を現存している国内法に置き換えたり立法したりする必要があるものである。もっとも、加盟国は、国内法に置き換えたり新設したりする指令に従う場合に、一定の裁量権を有する。一方で、「規則」とは、各加盟国間の法令を統一するために、制定されるものである。そこで、加盟国は規則の規定を直接国内に適用させる必要があり、仮に国内法と衝突する場合においては、国内法に優先する必要がある。直接作用性について、EUで定められる規則は、EU市民に直接に権利ないし義務を与えることができるので、直接作用性を有するものである。

従来の人格権ないしプライバシー権に係るだけでなく、前述のデータ保護指令上の諸規定も適用されると強調した¹²²。その後、2002年に作業部会は、職場における電子コミュニケーションの監視に関する意見書（WP55）を策定した¹²³。同報告書では、まず、使用者が監視を実施するためには、「透明性、必要性、公正性、比例性」の要件を満たさなければならないと指摘され、インターネットが従業員の日常生活にどの程度役立っているかを考慮せず、労働者のインターネットの使用を全面的に禁止することは非現実であり、労働者による不法行為の検出よりも技術的な予防措置を講じることが現実的であることが強調されている¹²⁴。その上で作業部会は、一定の例外状況を除き、使用者は監視を実施する前に個別労働者に十分な通知を行うだけでなく、労働組合や従業員代表にその導入をめぐって諮問・協議する必要もあると指摘された¹²⁵。また、通知の具体的な内容に関して、作業部会は、第1に、社内の電子メール／インターネットに関する方針において、会社が所有する通信設備を労働者が私的な通信に使用できる範囲を詳細に定めること（利用期間等）、第2に、監視を行う理由と目的、第3に、「いつ、誰が、何を、どのように監視を実施するか」に関する情報、第4に、労働者が就業規定に違反した場合の通知とそれに反論する際の詳細な手続を定めることを指摘している¹²⁶。なお、個別労働者や従業員代表等に通知しない秘密監視の実施に関して、作業部会は上記のILOが策定した行動準則を参考にし、加盟国の法律に適合している場合と犯罪行為またはその他の重大な不正行為の疑いが合理的な根拠をもって存在する場合に限定されている¹²⁷。

また、監視を実施する際に、従業員の同意をデータ処理の適法性の根拠として用いることが可能であるかどうかに関して、GDPRが施行された後に作業部会の任務を引き継いだ欧州データ保護会議（European Data Protection Board、以下では、EDPBと略称する）は、従来の作業部会の同意に関する解釈¹²⁸を

¹²² Article 29 Working Party, Opinion 8/2001 on the processing of personal data in the employment context, (WP48,2001), p.24.

¹²³ Article 29 Working Party, Working document on the surveillance of electronic communications in the workplace, (WP55, 2002).

¹²⁴ *Id.* pp.14-15.

¹²⁵ *Id.* p.15.

¹²⁶ *Id.* pp.14-15.

¹²⁷ *Id.* p.10.

¹²⁸ 例えば、Article 29 Working Party, Opinion 2/2017 on data processing at work(WP 249, 2017), pp.6-7.

踏襲し、「労働者の従属関係を考慮すると、……使用者が労働者にカメラ監視などの監視装置の導入や評価用紙（assessment forms）の記入を求める場合、労働者が自由意志に基づいてそれに同意するとは考えられない。したがって、労働者の同意をデータ処理の適法性の根拠とすることはできず、またそうあるべきではない」との見解を示した¹²⁹。

以上の監視に関する上記の法的文書から、次のようにまとめることができる。第1に、ILO、欧州評議会の閣僚委員会またはEUは、早い段階から監視を個人データ処理の一形態と捉えており、監視の実施はデータ処理の諸原則、すなわち透明性、必要性、公正性、比例性を満たなければならないと解釈してきた。とりわけ、透明性原則を遵守する上で、情報提供（通知義務）の重要性が強調されている。従業員への事前通知なく秘密裏に監視することは、犯罪行為を疑う合理的な理由がある場合に限って例外的に認められている。第2に、監視の通知義務だけでなく、監視実施の目的とその手段も制限されている。前述の法的文書によれば、監視の目的は、使用者が生産性・安全衛生または企業の効率的な運営を確保する場合に限られ、監視の手段は労働者のプライバシー権に配慮する必要がある、使用者に、同様の目的を達成できるプライバシー権への侵害がより少ない手段を選択する義務を課すことが求められている。最後に、監視の実施に対する労働者の同意をデータ処理の適法性の根拠とすることができるか否かについては、EUはかねてより、労使間における交渉力の格差から、労働者の同意をデータ処理の適法性の根拠とすべきではないとの立場をとってきた。

第3節 欧州評議会、欧州人権条約及び欧州人権裁判所の概説

第1款 欧州評議会の設立

1929年、フランスの外務大臣アリスティッド・ブリアン（Aristide Briand）が、演説の中で、ヨーロッパ諸国が共通の問題を解決するために「連邦連合（Federal Union）」という構想を打ち出したものの、1929年にアメリカを皮切りに世界的に深刻な経済恐慌が起こったため、その構想は実現に至らなかった。第二次世界大戦の終結から1年後の1946年9月19日、一時的に下野していたイギリス首相であったウィンストン・チャーチル（Winston Leonard Spencer Churchill）は、著名なチューリッヒ演説において欧州評議会設立の重

¹²⁹ Guidelines 05/2020 on consent under Regulation 2016/679 (adopted on 4 May 2020) p. 9.

要性を強調した¹³⁰。1949年5月5日、ようやく、欧州評議会はフランスやイギリスを含む10か国がロンドンにおいてロンドン条約（欧州評議会規程¹³¹）を署名し、欧州評議会が正式に発足した¹³²。

欧州評議会はヨーロッパで最も長い歴史をもつ政治組織であり、現在（2023年）カザフスタン、バチカン、ベラルーシとロシア¹³³を除く46か国が加盟している¹³⁴。欧州評議会が擁護する共通価値は、人権（Droits de l'homme）、民主主義（Démocratie）、法の支配（État de droit）という当初から変わらないものである。まず、同評議会の目的については、上記の欧州評議会規程において、「欧州評議会の目的は、締約国の共同の世襲財産たる理想及び主義を保護実現し、ならびに締約国の経済的・社会的進歩を促進するために、締約国間に一層緊密な統合を達成することである」（第1条（a））と謳われている。次に、同評議会の運営は、以下の機関を通じて行われている。第1は、各締約

¹³⁰ この演説の背景と詳細について、川崎晴朗「『チューリッヒ演説』の一解釈－チャーチルと戦後の欧州統合運動－」外務省調査月報1号（2004年）66頁以下。

¹³¹ Statute of the Council of Europe (ETS No. 001).

¹³² 斉藤千紘＝小島秀亮『〔人権の保護者〕欧州評議会入門』（信山社、2020年）7頁。

¹³³ ロシアによるウクライナ侵攻に関する欧州評議会の対応について、まず侵略当日の2月24日、閣僚委員会が侵略自体を批判し、翌日に評議会規程8条〔8条：第3条に著しく違反した欧州評議会の締約国は、その代表権を停止され、第7条に基づき閣僚委員会から脱退を要請されることがある。当該締約国がこの要請に従わない場合、閣僚委員会は、当該締約国の資格を喪失したことを決定することができる〕に基づき、ロシアの代表権を停止することを決定した。その後、ロシアは同規程7条に基づき、欧州評議会から脱退およびECHR廃棄を評議会事務局長に通知したが、同条に基づく手続は進行せず、結局のところ、閣僚委員会は2022年3月16日にロシアを即時除名した。Resolution CM/Res (2022) 2 on the cessation of the membership of the Russian Federation to the Council of Europe (CM/Res (2022)2) 16 Mar. 2022. 一方、人権裁判所との関係について、人権裁判所は3月1日にウクライナに関するロシアの軍事行動が、生命権（2条）、虐待の禁止（3条）及び家族生活・私生活の尊重を受ける権利（8条）等に違反したものであるとして、暫定措置（interim measures）を指示した。また、ロシアを被告とした未解決事件について、ロシアが欧州評議会によって除名されたにもかかわらず、人権裁判所は、9月16日までに発生するロシアに対するECHRの違反によって生じた作為または不作為に関する申立について、引き続き審理を行う権限を有するとの決議を発した。Resolution of the European Court of Human Rights on the consequences of the cessation of membership of the Russian Federation to the Council of Europe in light of Article 58 of the European Convention on Human Rights, 22 Mar. 2022. より詳細な紹介については、小畑郁「ロシアによるウクライナ侵略とヨーロッパ評議会・ヨーロッパ人権条約」人権判例報4号（2022年）4-5頁参照。

¹³⁴ 欧州評議会と協力関係を有するオブザーバー国として、教皇庁（1970年）、アメリカ合衆国（1995年）、日本（1996年）、カナダ（1996年）、メキシコ（1999年）がある。

国の外務大臣からなる欧州評議会における最高意思決定機関である閣僚委員会 (Committee of ministers), 第 2 は, 締約国の国会議員からなる諮問機関である議員会議 (Parliamentary assembly), 第 3 は, 1994 年に新設された締約国の地方代表議員で構成される諮問機関である地方自治体会議 (Local and regional authorities of Europe) である。最後に, これらの機関を支援するための事務局 (Secretariat) も設置された。なお, 欧州評議会は常に欧州連合 (EU) と混同されることが多い。両組織は完全に独立している組織であり, 民主主義, 法の支配, 人権という共通価値を擁護する上で補完的な役割を果たしている¹³⁵。

第 2 款 欧州人権条約の誕生と改革¹³⁶

ECHR は, 1950 年 11 月 4 日にローマで調印され, 1953 年 9 月 3 日に発効された¹³⁷。欧州評議会は, 主に 2 つの理由から, ECHR の作成を決定した。第 1 は, 第二次世界大戦中に起こった最も深刻な人権侵害を将来にわたって回避することができる手段を提供すること, もう一つは, 締約国が共産主義国家になることを防止することである¹³⁸。また, ECHR の締結は, 欧州評議会の加盟国に限定されているため, 欧州評議会のメンバーの地位を失った加盟国

¹³⁵ 両組織の異同について, 欧州評議会の HP を参照されたい。 <https://www.coe.int/en/web/portal/european-union> (最終アクセス日 2023 年 6 月 27 日)。

¹³⁶ EU の欧州連合基本条約 (Treaty on European Union) 6 条 3 項は, 「基本的人権は, 人権および基本的自由の保護に関する欧州条約 (ECHR) によって保障され, 加盟国に共通する憲法的伝統に由来するものであり, EU 法の一般原則を構成する」と明記している。また, 欧州基本権憲章 (Charter of fundamental rights of the European Union) 52 条 3 項は, 「本憲章が, ECHR が保障する権利に対応する権利を含む限りにおいて, それらの権利の意味および範囲は, ECHR が定める権利と同一とする。本条は, EU 法がより広範な保護を提供することを妨げるものではない」と規定している。このように, EU では, 欧州基本権憲章と ECHR が人権保護の基礎となっている。学説では, 「このように, EU 構成国 (そのすべてが欧州人権条約の締約国である) にとって欧州人権条約と基本権憲章という, いずれも法的拘束力を有し, かつ規定の対象と内容においてほぼ重なる国際人権文書が並存し, その解釈適用を, これも互いに優位劣位の関係になく並存する欧州司法裁判所と人権裁判所が別々に行う状況が生じている」と指摘されている。戸田五郎「欧州司法裁判所と欧州人権裁判所の併存と相互関係」産大法学 50 巻 1・2 号 (2017 年) 89 頁。

¹³⁷ 当初 ECHR を署名した国は, ベルギー, デンマーク, フランス, ドイツ, アイスランド, アイルランド, イタリア, ルクセンブルグ, オランダ, ノルウェー, トルコ, イギリスの計 12 国であった。

¹³⁸ Rainey et al., The European Convention on Human Rights, 3-4 (8th ed. 2020).

は、ECHR の締約資格も自動的に中止される (ECHR58 条 3 項)。なお、欧州評議会の加盟国は ECHR を批准する義務はないが、現在ではすべての加盟国が ECHR を批准している。

ECHR の内容は絶えずテクノロジーや社会環境の変化に照らして解釈されなければならない、調印時 (1950 年) には想定されていなかった権利を議定書の制定を通じて追加したり、ECHR それ自体の構造を変更したりしている。このことから、ECHR は「生きている条約」あるいは「変化し続ける法」と呼ばれる所以である¹³⁹。また、ECHR が発効した当初は、現在の内容とかなり異なっており、個人が人権裁判所に申立を行うことができるかどうか (旧 ECHR25 条)、人権裁判所の管轄権を受諾するか否か (旧 ECHR46 条) は ECHR の締約国の裁量に委ねられていたため、その実効性は非常に弱かった¹⁴⁰。しかし、1990 年 11 月にハンガリーが欧州評議会に加盟したことを皮切りに、人権裁判所の管轄権と人権裁判所に対する個人の申立権を受諾することが欧州評議会の加盟条件となった¹⁴¹。

人権裁判所が下した判決の執行に関しては、被告国が判決を確実に執行したか否かを確認する権限は、かねてより閣僚委員会に委ねられている。閣僚委員会は被告国が提出した判決執行計画書 (Action report) に基づき、言い渡された義務執行の完成が認められるまで監督する義務がある (現 ECHR46 条 2 項)。確定判決の執行を閣僚委員会に委ねる最も重要な理由は、前述の通り、閣僚委員会が欧州評議会の全締約国の外務大臣で構成される組織であり、このような特殊性を通じて、締約国同士のパワーバランスによって確定判決の執行を確保することができるからである¹⁴²。また、被告国が閣僚委員会の要請に従わない場合、閣僚委員会は「判決遵守義務を怠っている」ことを確認する不履行確認訴訟 (Infringement proceedings) を別途人権裁判所に提起することができる (現 ECHR46 条 4 項)。この要請を受けた人権裁判所は、被告国が継続的に判決の執行を怠っていると判断した場合、元の判決とは別に判決

¹³⁹ Tyrer v. United Kingdom (App. 5856/72) 25 April 1978, Series A No. 26 (1979-80) 2 EHRR 1. 「ECHR は、現在の状況に照らして解釈されるべき生きた文書である」 (§31)。

¹⁴⁰ 小畑郁「ヨーロッパ人権条約実施システムの歩みと展望」小畑郁ほか編『ヨーロッパ人権裁判所の判例 I』(信山社、2008 年) 3 頁。

¹⁴¹ 同上注、6 頁。

¹⁴² 斉藤千紘=小島秀亮・前掲注 131) 75 頁。

遵守義務違反という判決を下すことができる¹⁴³。もっとも、被告国がこの義務に違反したとしても、課徴金の支払いに関する規定は設けられていない。この不履行確認訴訟を導入した後述する第 14 号議定書は、被告国以外の締約国からの政治的圧力によって、被告国が人権裁判所の確定判決を遵守する効果が得られることを想定していた¹⁴⁴。

前述したように、個人が ECHR 上の権利に基づき人権裁判所に対して直接訴訟を申し立てることは想定されていなかった。1998 年 11 月 1 日に第 11 号議定書が発効される前、人権裁判所に事件を付託できるのは、欧州人権委員会（European commission of human rights, 以下、人権委員会という）と締約国であった。人権委員会は、各締約国の法学者 1 名で構成される準司法機関であり、同委員会の最も重要な役割は、申立をふるい落とすことである。具体的には、人権委員会は、個人等による申立が受理可能性の基準を満たしているかどうかを審査（旧 ECHR25 条）し、仮に当該申立に受理可能性（Admissibility）がある場合、人権委員会は公的機関ないし私人が ECHR に違反するかどうかを判断し、その結論を報告書の形で作成（旧 ECHR 31 条 1 項）し、被告国と閣僚委員会に送付する義務がある（旧 ECHR 31 条 2 項）。さらに、報告書が送付されてから 3 カ月以内に、一定の状況において、被告国と人権委員会は当該申立を人権裁判所に付託することができる（旧 ECHR 47 条）。当然、被告国が人権裁判所の管轄権を受諾することが前提条件である。

しかしその後、人権委員会への申立件数と人権裁判所への付託の急増、ソ連崩壊後の中東欧諸国の相次いだ加盟、人権委員会と人権裁判所の仕組みの複雑さと重複が考慮され、1950 年に制定された ECHR を改革する重要性が 1980 年代から次第に認識されるようになった¹⁴⁵。ECHR の一連の改革として、まず、1994 年 1 月 1 日の第 9 号議定書が発効される前、人権裁判所への申立て可能なのは人権委員会及び被告国のみであったが（旧 ECHR44 条）、同議定

¹⁴³ 同上注、76 頁。現時点までのところ、判決遵守義務違反が認められたのは、*Ilgar Mammadov v. Azerbaijan* 事件（*Ilgar Mammadov v. Azerbaijan* (App. 15172/13), 29 May 2019 [GC]）だけである。

¹⁴⁴ 小畑郁「第 14 議定書によるヨーロッパ人権条約実施規定等の改正」法政論集 205 号（2004 年）278-279 頁。ECHR の仕組み上、被告国による確定判決の履行は、閣僚委員会の監視だけでなく、メディア、すなわち国内的・国際的世論の圧力によっても期待されている。ジャン・ポール・コスタ「ヨーロッパ人権裁判所－ヨーロッパおよびヨーロッパ以外の地域におけるその影響力について－」小畑郁ほか編『ヨーロッパ人権裁判所の判例 II』（信山社、2019 年）xxiv。

¹⁴⁵ 江島晶子「ヨーロッパにおける人権保障システムの発展－ヨーロッパ人権条約第 11 議定書調印を契機として－」明治大学短期大学紀要 57 号（1995 年）37-38 頁。

書の発効後は、個人も直接人権裁判所に訴訟を提起する権利を有するようになった¹⁴⁶。さらに、4年後の1998年、ECHRの中核を改革する最も重要な上記の第11号議定書が発効した¹⁴⁷。この議定書は、閣僚委員会の事件の実質的審理権限を廃止し、個人の申立権と人権裁判所の管轄権を任意承認の方式から、自動的に承認する方式に変更し、さらに人権委員会と人権裁判所の機能を新（現在の）人権裁判所に統合した。新人権裁判所は、旧人権裁判所と同じ名称であるが、ECHR違反申立の受理可能性とECHRの違反の有無を実質的に審査する権限を有している点で異なっている。なお、近時、2018年8月11日に発効した第16号議定書は、ECHRそのものの改革ではなく、人権裁判所と締約国の最高裁判所との対話をより促進する目的として制定された¹⁴⁸。同議定書は、上記目的のもとで、締約国の最上級審（Highest courts and tribunals）が、ECHRまたは議定書の権利と自由に関連する解釈上の問題について裁判所に勧告的意見を求めることを認めている（同議定書1条）が、この要請は完全に任意であり、また人権裁判所の回答には法的拘束力もない（同議定書5条）。もっとも、人権裁判所の回答はある意味で締約国の国内裁判所にとって「指針」のようなものであり、これを通じて、国内裁判所は、当該申立が人権裁判所に持ち込まれた場合、どのような判断がなされるかを予測することができ、国内裁判所の段階において事件が解決する効果が期待されている¹⁴⁹。

第3款 欧州人権裁判所の構造と判断原則

人権裁判所は人権保護の分野における最も古い国際裁判所であり、かねてより締約国がECHRおよびその議定書を遵守しているかどうかを確保するために設置された機関である（現ECHR19条）。このことから、人権裁判所は、常にECHRの保護者（Gardienne）と称されている¹⁵⁰。前述のように、第11号議

¹⁴⁶ Protocol No. 9 to the Convention for the Protection of Human Rights and Fundamental Freedoms, CTS n°140. 同議定書は1994年1月1日に発効したが、第11号議定書の発効に伴って廃止された。

¹⁴⁷ Protocol No. 11 To the Convention for the retention of human rights and fundamental freedoms, restructuring the control machinery established thereby CTS n°155. 和訳と紹介については、江島・前掲注145）33-69頁。

¹⁴⁸ Protocol No. 16 amending the Convention on the Protection of Human Rights and Fundamental Freedoms, ETS n°214.

¹⁴⁹ 伊藤洋一「ヨーロッパ人権条約第16議定書と裁判官対話」法時93巻4号（2021年）57頁

¹⁵⁰ J-P COSTA, La Cour Européenne des Droits de l'Homme, *Rev. Quebec Droit Int'l* 33 (21), 2020, p.23.

定書発効後は、現在の人権裁判所は申立の受理可能性から申立に対する実質的審理までを行うようになった。特段の事情¹⁵¹を除き、人権裁判所の判決は被告国のみを拘束するもの（ECHR46条1項）であり、被告国以外の国に対しては、既判力は有さずが、解釈既判力しか持たない¹⁵²。しかし、この解釈既判力により、実質的にすべての締約国は人権裁判所の判決の効力に拘束されている。

ECHR に対する人権裁判所の解釈方法に関しては、学説は、人権裁判所の ECHR に対する解釈方法を、①目的論解釈（Purposive interpretation）、②実効的解釈（Effective interpretation）、③発展的解釈ないしダイナミックな解釈（Evolutive interpretation, dynamic Interpretation）、④自律的解釈（Autonomous interpretation）、⑤評価の余地の理論（Doctrine of the margin of appreciation）及び⑥比例性原理（Principle of proportionality）に分類している¹⁵³。まず、最初の4つの方法に関して、①目的論解釈とは、人権裁判所が ECHR の趣旨（個人の権利と自由の保護）に従って解釈しなければならないことを意味する。②実効的解釈とは、人権裁判所が ECHR 上の諸権利を実際的で効果的なものにするように解釈し、適用しなければならないことを意味する。この実効的解釈という方法は、後述するような人権裁判所が認める締約国の「積極的義務」と密接な関係がある。③発展的解釈とは、人権裁判所が ECHR 起草時の状況に拘束されることなく、社会の変化と発展に照らして ECHR を解釈しなければならないことを意味する¹⁵⁴。④自律的解釈とは、人権裁判所は締約国の主観的解釈に拘束されず、国内法上の概念を自律的に解釈する必要があることをいう。この解釈は、締約国が恣意的な解釈によって ECHR の適用を回避することを防止するためのものである¹⁵⁵。⑤評価の余地の理論は、フラン

¹⁵¹ 例えば、パイロット判決手続を用いた判決である。パイロット判決手続とは、被告国の国内法制度または国内慣行に存する構造的問題に起因する同種事案が、実体審理に付される申立のほとんどであることに着目し、この種の申立のうち、同一被告国の申立から特徴的な一事件を取り上げ、それを通して、当該問題を解決することを目指す手続を意味する。コスタ・前掲注 144）xxiii 参照。

¹⁵² 同上注 xxiv。

¹⁵³ RAINEY ET AL., *Supra* note 138, p.63.

¹⁵⁴ この解釈を最初に明示したのは、1978 年の Tyrer 事件、*See case supra* note 139.

¹⁵⁵ たとえば、Engel and others 事件（Engel and others v. Netherlands 8 June 1976, Series A no.22）において、人権裁判所は、軍隊における懲戒手続は ECHR6 条の「刑事上の罪」に該当しないとする被告国であるオランダの主張を退けた。同事件の評釈について、坂元茂樹「判批」小畑郁ほか編『ヨーロッパ人権裁判所の判例 I』（2008 年、信山社）139-143 頁。

スのコンセイユ・デタの原理に基づく理論¹⁵⁶であり、この理論は人権裁判所の大原則である補完性の原則（Principle of subsidiarity）¹⁵⁷と密接に関係している¹⁵⁸。文化的多様性に富む欧州大陸において、基本的権利の制限の解釈に際して画一的な判断アプローチをとることは、各国法の多様性を喪失させるという逆効果をもたらす¹⁵⁹。さらに実際には、人権裁判所の管轄範囲は現在 8 億人以上に及んでいるため、人権裁判所がすべての事件を判断することは不可能である。そのため、締約国は人権裁判所よりも、基本的権利を制限する必要があるかどうかを実際の状況に基づいて判断できる立場にある¹⁶⁰。しかし、締約国に与えられる裁量は無制限ではない。人権裁判所は、問題となった ECHR 上の権利の侵害に関して締約国間でコンセンサスが存在しているかどうかを審査し、コンセンサスがある場合には、被告国の評価の余地を狭く解釈しているのに対し、コンセンサスがない場合には、被告国の評価の余地を広く捉えている¹⁶¹。最後に、⑥比例性原理とは、人権裁判所が、私的機関と公的機関によって干渉された個人の ECHR 上の権利と、その干渉行為との適切なバランスを審査することを意味する。比例性の判断は、後述する ECHR8 条（私生活等の保護を受ける権利）の侵害があるかどうかを審査する上で重要な役割を果たしている。通常、この審査は、同条 2 項の権利への干渉が「民主的社会において必要なもの」に該当するかどうかとの段階において行われる¹⁶²。

第 4 款 積極的義務の概念

¹⁵⁶ 北村泰三「ヨーロッパ人権条約と国家の裁量--評価の余地に関する人権裁判所判例を契機として」法学新報 88 巻 7 号=8 号（1981 年）37 頁。

¹⁵⁷ 補完性の原則とは、締約国の国内裁判所は人権条約の権利が尊重されること確保しなければならないこと。人権裁判所は、国内裁判所が人権条約上の権利を保護できない場合にのみ介入することを意味する。

¹⁵⁸ RAINEY ET AL., *Supra* note 138, p.374.

¹⁵⁹ R. ERGEC, *Protection européenne et internationale des droits de l'homme*, 2^e éd., 2006, p.125.

¹⁶⁰ *Handyside v. United Kingdom*, (App.5493/72) 7 December 1976, Series A No 24, (1979-80) 1 EHRR 737, §48; *Sunday Times v. the United Kingdom* (App. 6539/74) 26 April 1979, Series A No 30, (1979-80) 2 EHRR 245, §59.

¹⁶¹ N.A. Moreham, *The Right to Respect for Private Life in the European Convention on Human Rights: A Re-examination*, 1 E.H.R.L.R. 44, 47-48 (2008).

¹⁶² 江島晶子「ヨーロッパ人権裁判所の解釈の特徴」小畑郁ほか編『ヨーロッパ人権裁判所の判例 I』（2008 年、信山社）31 頁。

前述したように、人権裁判所の審査対象は当初、締約国が個人の ECHR 上の権利を侵害した場合であると構想されていた¹⁶³。つまり、締約国は人権侵害を行わないという古典的かつ消極的義務しか負わず、私人間による ECHR 上の権利侵害に関する紛争を積極的に介入する義務はなかった。しかし、1960 年代以降、公的機関に匹敵する私的団体等が個人の ECHR における権利と自由を侵害する問題が急増し、締約国にはこのような侵害を積極的に排除し予防する義務があるかどうかという疑問が提起されるようになった¹⁶⁴。この背景を踏まえ、人権裁判所は、上記 ECHR の「実効的解釈」を通じて、締約国には、私人間による ECHR 上の権利侵害を積極的に排除し予防する義務があるという解釈を発展させてきた¹⁶⁵。このことは、ECHR の私人間効力ないし ECHR の水平的効力（仏：Applicabilité horizontale, 独：Drittwirkung）とも呼ばれている。

人権裁判所が締約国の積極的義務を最初に言及したのは、ECHR8 条（私生活等の尊重を受ける権利）に違反したかが争われた 1979 の Marckx 事件¹⁶⁶であった。この事件において、人権裁判所は「(ECHR8 条)の目的は、公的機関による恣意的な干渉から個人を保護するという『本質的な』ものである。この消極的な義務に加え、家族生活の効果的な『尊重』に固有の積極的な義務も存在する」と判示した¹⁶⁷。その後、2007 年の Dickson 事件において、大法廷は締約国の消極的義務と積極的義務の関係について、「ECHR8 条の目的は基本的に公的機関による恣意的な干渉から個人を保護することであるが、単にそのような干渉を禁止するという消極的義務を課すわけではない。この消極的義務に加え、締約国には個人の私生活と家族生活を効果的に尊重する積極的義務もある。これらの義務は、私人間の関係の領域においても、私的および家族的生活の尊重を確保するための措置の採用を含む場合がある。ECHR8 条に基づく締約国の積極的義務と消極的義務の間の境界は、正確な定

¹⁶³ 中井伊都子は、ECHR 起草時の経緯からすれば、「ECHR の締約国の人権が確保されるようにすべき義務を認める意図がなかった」と指摘した。中井・前掲注 104) 40 頁。同旨、谷口洋幸「プライバシーの権利と私生活・私的生活の尊重—国際法の視点—」国際人権 17 号（2006 年）48 頁。

¹⁶⁴ ERGEC, *supra* note 155, pp.127-128.

¹⁶⁵ M. OTTO, THE RIGHT TO PRIVACY IN EMPLOYMENT, 69 (2019).

¹⁶⁶ Case *Supra* note 105. この事件は、当時のベルギー法において嫡出子と比べて、非嫡出子がさまざまな不利益取扱いを受けていたことを理由に 8 条（私生活等の尊重を受ける権利）等の違反に関するものである。この事件の詳細については、中井・前掲注 104) 43-48 頁参照。

¹⁶⁷ *Id.* § 31.

義に適さないものであるが、両義務が適用される原則は類似している。特に、いずれの場合にも、競合する利益の間で公平なバランスをとるべきであることに留意しなければならない」と整理した¹⁶⁸。また、たとえ締約国が個人の ECHR 上の権利を効果的に保護する積極的義務を負っているといえども、私人間による権利侵害に対して締約国が常に責任を負うことを意味するわけではない。このような責任が生じるのは、あくまでも「他者による侵害から個人を保護する上で、被告国の法規定の欠如または不十分さに起因する場合」に限定されている¹⁶⁹。なお、人権裁判所は、締約国に積極的義務を課している一方で、それらの義務を果たす手段の選択において、締約国の消極的義務よりも広い裁量権（前述の評価の余地）を締約国に与えることに留意しなければならない¹⁷⁰。

一方、締約国の積極的義務は一般的に 2 種類に大別される¹⁷¹。すなわち、締約国の保護的措置を講じる義務（Duty to regulate）と、締約国の効果的な規制を実施する方法を定める義務（Duty to act）である。前者の義務に関しては、例えば、使用者による監視の場合において、人権裁判所は締約国に対し、労働者のプライバシー権を保護するための規範的規制の導入（判例法理や法律など）を求めることを意味する。具体的にどのような規制を導入するかは締約国に委ねられているが、個人のプライバシーを侵害する可能性が高い場合、人権裁判所は、法律のような形で規制を設けるべきであるとの見解を示している¹⁷²。一方、後者の義務に関しては、人権裁判所は締約国に対し、個人のプライバシーを保護するために効果的かつ必要な手段を講じるよう求めている

¹⁶⁸ Dickson v. United Kingdom, (App. 44362/04), 4 December 2007 [GC], (2008) 46 EHRR 927, ECHR 2008-XIII, §70.

¹⁶⁹ Abdurrahimli, *supra* note 2, p. 36.

¹⁷⁰ 締約国の積極的義務は ECHR 8 条だけでなく、ECHR 上の他の規定にも適用されることになった。例えば、労働組合とクローズド・ショップ協を締結していた英国国有鉄道に雇用されていた 3 人の労働者が、協定によって指定された労働組合に加入しなかったことを理由に解雇され、当該解雇が ECHR 11 条（集会・結社の自由）に違反したかが争われた 1981 年 Yong et al. 事件（Yong, James, and Webster v. United Kingdom, (Apps. 7601/76 and 7801/77), 13 August 1981, Series A No.44(1982) 4 EHRR 38）もある。この事件を詳細に検討する文献として、中村・前掲注 102）9 頁以下参照。

¹⁷¹ E. Sychenko, International protection of employee's privacy under the European convention on human rights, 67 (5) ZBORNIK PFZ. 757, 775 (2017).

¹⁷² *Ibid.*

る¹⁷³。例えば、原告労働者が HIV に感染した事実がセキュリティの不備により同僚に知られてしまった I 事件¹⁷⁴において、人権裁判所は、個人データが違法に開示されたことについて、被告国の国内法における事後の損害賠償の救済手段だけでは十分ではなく、同意なしのアクセスが発生する可能性を排除するための実用的かつ効果的な保護措置を要請している¹⁷⁵。

第 5 款 欧州人権条約 8 条の定義と運用

ECHR8 条（私生活等の尊重を受ける権利）は、「すべての者は、その私的および家族生活、住居ならびに通信の尊重を受ける権利を有する（第 1 項）。この権利の行使に対しては、法律に従い、かつ、国の安全、公共の安全もしくは国の経済的福利のため、また、無秩序もしくは犯罪の防止のため、健康もしくは道徳の保護のため、または他の者の権利および自由の保護のため、民主的社会において必要なもの以外のいかなる公の機関による介入もあってはならない（第 2 項）」と規定している。ECHR8 条の基本的内容に関して最初に定義したのは、1976 年に人権委員会が X 事件において示したものである¹⁷⁶。同事件において、人権委員会は、「多くのアングロサクソンとフランスの学説にとって、私生活を尊重する権利は、プライバシー権であり、本人が望む限り、公開から保護され、生活する権利（Right to live）である。人権委員会の見解では、私生活を尊重する権利は、それだけにとどまらない。私生活を尊重する権利に、他の人間との関係、特に自己の人格の発達と実現のための感情的関係を確立し、発展させる権利もある程度含まれる」とした¹⁷⁷。人権委員会はこの事件を通じて、私生活の概念には、従来の私事を他人にみだりに公開されないという保護と、他人との関係を発展させる権利が含まれると述べたが、その後の人権裁判所の判例法の発展からすれば、私生活の概念がこの 2 つの側面だけではないことは明らかである¹⁷⁸。その後、人権裁判所は X 事件における人権委員会の見解をさらに発展させ、ECHR8 条に関連する種々

¹⁷³ Abdurrahimli, *supra* note 2, p. 37.

¹⁷⁴ I v. Finland, (App. 20511/03) 17 July 2008, (2008) 48 E.H.R.R. 31.

¹⁷⁵ *Id.* §47.

¹⁷⁶ X v. Iceland, (App.6825/74), Decision of 18 May 1976, (1976)5 DR 86, pp.88-89.

¹⁷⁷ *Ibid.*

¹⁷⁸ L. Doswald-Beck, The meaning of the "right to respect for private life" under the European convention on human rights, 4 (3) HRLJ. 283, 288(1983).

の事件を通じて、私生活の概念がカバーする範囲を拡大してきている¹⁷⁹。

また、ECHR8 条に違反するか否かを判断するために人権裁判所が用いる具体的な判断アプローチについては、人権裁判所はまず、個人への干渉主体が公的機関または私的機関を厳密に区別し、公的機関の場合は、ECHR8 条第 2 項によって形成される「3 要件審査」、つまり①干渉が法¹⁸⁰に従ったものであるかどうか、②干渉の目的が正当であるかどうか、③干渉が民主的社会において必要なものであるかどうかを行う。一方、私人間による侵害の場合、人権裁判所は、被告国の積極的義務に照らして ECHR8 条の権利への干渉が同条の範囲に含まれるか否かを広く審査し（受理可能性を審査する段階）、次に、人権裁判所は、被告国の裁判所が同条の権利を侵害する側の利益と侵害される側の利益との間において公平なバランスをとっているかどうかについて審査する（公平なバランスに関する審査）。この公平なバランスに関する審査の段階においては、前述の公的機関による侵害の事件で適用される 3 要件審査は判断の要素として考慮されている¹⁸¹。

第 6 款 小括

以上の人権裁判所と ECHR に関する議論をまとめると、以下のようになる。

欧州評議会はヨーロッパにおいて最も古い政治的組織として、欧州諸国の政治的なイデオロギーの形成や法制定の方向に対して大きな影響力を持っている。このような影響力は、特に個人の基本的権利を保護することを目的とした ECHR によって具体化されている。

ECHR は当初、締約国の主権等を考慮し、限られた場合しか適用されていなかった。しかし、ECHR 上の権利と自由を効果的に保護するため、欧州評議

¹⁷⁹ 例えば、ECHR8 条に自己情報コントロール権が含まれるとした *Leander* 事件 (*Leander v. Sweden* (App.9248/81) 26 March 1987, Series A No 116, (1998) 9 EHRR 433) がある。

¹⁸⁰ また、人権裁判所は、かねてより締約国の法の「質 (quality)」を厳格に捉えてきた。例えば、公権力による電話傍受が個人の私生活を侵害したかどうかが争われた *Malone* 事件 (*Malone v. the United Kingdom*, (App. 8691/79), 2, August 1984, Series A No. 82, (1985) 7 EHRR 14) において、人権裁判所は、ECHR8 条 2 項の「法に従ったもの」という要件を審査するにあたり、関連する法律の存在だけでなく、当該法律の質、つまり、その正確性、確実性、予測可能性についても審査している。また、上記法の正確性、確実性、予測可能性という 3 つの基準に加え、人権裁判所は、その法律が個人にとって利用可能なもの (accessible) であることも要請している。See *supra* case note 156, §49.

¹⁸¹ See Moreham, *supra* note 161, p.48.

会は議定書のような形で新たな内容を追加したり、個人による申立の手續等を整備したりすることによって ECHR の実効性を確保している。一方、人権裁判所は、ECHR が効果的な人権保護を提供するよう、事案当時の社会情勢やテクノロジーに照らして ECHR 上の権利を解釈し、適用している。さらに、人権裁判所は、ECHR によって保護されている個人の権利を侵害してはならないという消極的義務だけでなく、実効的解釈というアプローチを用いて締約国に対して私人間の人権侵害を積極的に防止するという積極的義務も課している。人権裁判所の解釈によれば、両義務の間に明確な線引きをすることはできないが、適用される原則（例えば、対立する利益の間に公平なバランスがとれているかどうか）は類似している。最後に、ECHR8 条の解釈に関しては、その内容は当初、従来の、私事を他人にみだりに公開されないという権利と、他人との関係を発展させる権利が含まれると解釈されていたが、その後の判決では、自己情報コントロール権などの内容が追加されている。

第 4 節 監視に関する欧州人権裁判所の判例法の考察¹⁸²

第 1 款 Niemietz v. Germany 事件¹⁸³

まず、裁判官に侮辱的な手紙を書いた疑いがある弁護士である原告 X の事務所が警察に捜査されたことについて、これが ECHR8 条「住居」の侵害となるか否かが争われた Niemietz 事件において、人権裁判所は、職業生活に私生活の概念が含まれるかどうかについて初めて正面から判断した。

人権裁判所は、『私生活』の概念を、個人が自らの選択によって私生活を送ることができる内輪（Inner circle）に限定し、内輪の中に含まれない外部のものをそこから排除するという解釈は、あまりにも制限的である」とし、さら

¹⁸² また、EU の欧州司法裁判所（European Court of Justice）はこれまで、職場における監視の問題について判決を下していない。See A. Komanovics, *Workplace Privacy in The EU: The Impact of Emerging Technologies on Employee's Fundamental Rights*, 7 ECLIC. 443, 458(2023), available at https://www.researchgate.net/publication/373476630_WORKPLACE_PRIVACY_IN_THE_EU_THE_IMPACT_OF_EMERGING_TECHNOLOGIES_ON_EMPLOYEE%27S_FUNDAMENTAL_RIGHTS.

¹⁸³ Niemietz v. Germany, (App. 13710/88), 16 December 1992 16, Series A No. 251-B, (1993) 16 EHRR 97. 本判決の日本語の評釈として、奥山亜喜子「弁護士事務所の捜索と住居の尊重」戸波江二ほか編『ヨーロッパ人権裁判所の判例 I』（信山社、2008 年）347-351 頁、横田直文「弁護士事務所に対する捜索と欧州人権条約第 8 条「住居」の尊重：欧州人権裁判所の Niemietz 判決と EU 競争法調査手続」慶應法学 6 号（2006 年）359-369 頁等がある。

に ECHR8 条の私生活尊重を受ける権利には、「他者との関係を築き、発展させる権利も一定程度含まれなければならない。このように理解すれば、職業的活動を『私生活』の概念から除外する理由は、原則として存在しない。というのも、職業上の活動は、大多数の人々が、外部世界と関係を築く、最大の機会ではないにしても、重要な機会になるのは労働生活の過程であるからである」とした¹⁸⁴。結論として、人権裁判所は、本件における X の職場の捜査は、ECHR8 条に対する干渉に該当し、上記の捜査は ECHR8 条 2 項に規定された 3 要件審査（本章第 3 節第 5 款）内の「X の人権に対する本件干渉が民主的社会において必要なものであるか否か（比例性の審査）」という要件を満たしていないとし、ドイツの国内裁判所の判断が ECHR8 条に違反すると判示した。

(1) 学説上の議論

本判決の意義は、職業生活と私生活との間に明確な境界線を引くことが不可能であるという観点から、人権裁判所が私生活の概念には「一定程度まで他の人間との関係を築き、発展させる権利が含まれる（Le droit de nouer et de développer des relations avec ses semblables）」と判示した点にある¹⁸⁵。この点について、本件における私生活の概念に関する解釈は、プライバシー権を「ひとりにしておいてもらう権利」として捉える英米法上の同権利の範囲よりも広いという指摘がある¹⁸⁶。さらに、本判決では明確に言及されていないにもかかわらず、職業生活も ECHR8 条の保護範囲に含まれていることから、ECHR8 条は、単に個人の私生活（Private life）にとどまらず、個人の私的な社会生活（Private social life）をも含むと主張する学説もある¹⁸⁷。この主張は、後述する人権裁判所の判決において承認された（後述する *Bărbulescu v. Romania* 事件）。なお、X は自営業者の弁護士であったため、伝統的意味での労働者ではないことに留意しなければならない。従属関係の下にある労働者に ECHR8 条の適用を認めた最初の事件は、本件から 5 年後の監視に関する

¹⁸⁴ *Id.* §29.

¹⁸⁵ Moreham, *supra* note 16, p.75.

¹⁸⁶ 横田・前掲注 183) 365 頁。

¹⁸⁷ J-P MARGUENAUD, *La cour européenne des droits de l'homme*, 5^e éd., 2011, pp. 82-83.

Halford 事件である¹⁸⁸。

第 2 款 Halford v. United Kingdom 事件¹⁸⁹

この事件は、職場における労働者の私生活保護を承認した最初の人権裁判所の判決として知られている。本件は、イギリスのマージーサイド警察署の女性警察官であった原告 X が、性別を理由に数年間にわたり、昇進を拒否されていたことが性差別に当たるとして、当該警察署長とイギリスの内務大臣に訴訟を提起した。訴訟の過程で、X は、上司の事前の許可を得た上でオフィス内の個人用の電話を使用し、弁護士に訴訟に関する内容を相談していたが、その電話の内容が X の上司によって盗聴され（以下では、本件盗聴と略称する）、当該訴訟において X に不利な証拠として使用されることを知った。これにおいて、X は、イギリスの監視と通信裁判所（Interception of Communications Tribunal）に対して別個の訴訟を提起した¹⁹⁰。

イギリス国内のあらゆる救済を尽くした後、X は人権裁判所に本件盗聴に関する訴訟を申立てた。人権裁判所は、まず、本件盗聴が ECHR8 条によって受理されるかどうかという大前提について、「自宅からだけでなく、職場から行われる電話も、ECHR8 条 1 項の意味における「私生活」および「通信」の概念に含まれていることは、人権裁判所の判例法から明らかである。マージーサイド警察署は、……X が行った通話が監視の対象となることを事前に通知していなかった。したがって、X はこれらの通話に対してプライバシーが保護されるという合理的な期待を有していた（下線は筆者による）。また、X は

¹⁸⁸ なお、日本では、労働者の人格権を承認する意義を「企業あるいは職場が労働者が活動的時間の大部分を過ごし人間的コミュニケーションが交わされる一つの社会であり、自由な人格の形成にとって決定的意味をもつ」と解した角田の見解と、労働者のプライバシー権の意義を「個人を社会から隔絶するためではなく、適正な均衡の下で他者との交流・接触を図るためのものである。まさに、適度の距離をもった人間関係をいかに形成すべきかが問題になる」とした道幸の見解がある。両者は本判決の判断との親和性が高いように思われる。角田邦重「企業社会における労働者人格の展開」日本労働法学会誌 78 号（1991 年）28 頁および道幸・前掲注 15）26 頁参照。

¹⁸⁹ Halford v. United Kingdom, (App. 20605/92), 25 June 1997, (1997) 24 EHRR 523, ECHR 1997-III. 本判決の日本語評釈として、日本労働研究機構「労働者の個人情報保護と雇用・労働情報へのアクセスに関する国際比較研究」調査研究報告 N° 155（2003 年）110-112 頁〔砂押以久子〕。

¹⁹⁰ また、X は自宅の電話も監視されていたとも主張したが、この主張は人権委員会と人権裁判所によって退けられた。この点については、本論文では割愛する。

自分のオフィスにある 2 台電話のうち 1 台を排他的に使用していたことも判明した。……以上の理由により、X がオフィスの電話で行った会話は、「私生活」と「通信」の概念の範囲内にあり、ECHR8 条が適用される」とした¹⁹¹。

次に、本件盗聴が ECHR8 条 2 項の「3 要件審査」をクリアできるかどうかについて、人権裁判所は、まず、本件盗聴が要件①の「法に従ったもの」であるか否かについて、これまでの人権裁判所の判例法に照らして、「『法に従ったもの』という条件は国内法の遵守を求めるだけでなく、法の支配に適合していることを要求し、その『法律の質 (Quality of law)』にも関係している。公的機関による監視や通信傍受の秘密措置については、ほかの公的機関による審査の欠如と権力の濫用の危険性から、国内法は ECHR8 条の権利に対する恣意的な干渉から個人をある程度保護しなければならない。したがって、公的機関による監視の秘密措置の使用が許される状況や条件について、国民に十分な情報を提供するために、国内法の規定は十分に明確でなければならない」¹⁹²との原則を示し、「事件当時は、1985 年法（イギリスの通信傍受法）はマージーサイド警察署のような公的機関が運営する内部通信システムに適用されず、被告国の国内法には上記通信システムで行われる電話の傍受を規制する他の規定がなかったため、被告国の国内法が X の私生活及び通信の尊重の権利の妨害に対する適切な保護を提供していなかった」とし、「本件盗聴は上記要件である『法に従ったもの』とは認められず、公的機関による X の電話傍受は ECHR8 条に違反する」と結論づけた¹⁹³。

(1) 学説上の議論

本件の意義には 2 つがある。第 1 に、人権裁判所が ECHR8 条をはじめて労働関係に適用したことである。したがって、少なくとも公的部門における労働者が同条の保護を享受できることは明らかである¹⁹⁴。第 2 に、上記の Niemietz 事件とは異なり、本件判決は前述したアメリカ法で発展したプライバシー保護への合理的期待という法理（第 1 章第 3 節第 2 款 (2) (ii.)) を採用したことである。特に 2 点目、つまり人権裁判所が上記のアメリカの法理を用いた点に関しては、学説上多くの批判が見られる。例えば、アメリカの

¹⁹¹ See case *supra* note 189, §44.

¹⁹² *Id.* §49.

¹⁹³ *Id.* §51.

¹⁹⁴ Abdurrahimli, *supra* note 2, p. 5.

上記法理を採用した本判決は、アメリカにおける同法理と同じ問題、つまり、使用者が事前に何らかの方法で労働者に監視装置の存在を通知した場合、監視は合法となり、労働者のプライバシー権が著しく制限されることになるとする見解がある¹⁹⁵。この点に対し、人権裁判所もこの問題を認識し、後述の Köpke 事件においてプライバシー保護への合理的期待という法理を制限し、修正した。

第 3 款 Copland v. United Kingdom 事件¹⁹⁶

本件では、ある大学の Y 副学長が、秘書として雇用されていた X が業務用のコンピュータを私的目的で過度に使用したかどうかを確認するため、監視に関する規定がないにもかかわらず、X の業務用コンピュータにおける電子メール、閲覧したウェブサイトおよび電話の利用状況を監視した（以下では、本件監視と略称する）。

人権裁判所は、まず、本件において被告国が負うのは消極的義務か積極的義務か（前述の第 2 章第 3 節 4 款参照）について性質決定し、「イギリス政府は、同大学は公的機関であり、その行為は ECHR の目的に照らして責任を負うものであると認めている。したがって、本件において ECHR8 条の下で判断される問題は、X の私生活および通信を妨害しないという被告国の消極的義務に関するものである」と判断した¹⁹⁷。次に、電子メール、インターネットまたは電話の利用状況に対する監視が ECHR8 条の範囲に含まれているか否かに関して、人権裁判所は、前述の Halford 事件の判旨を引用した上で、「職場からの電話は ECHR8 条第 1 項における『私生活』および『通信』の概念に含まれる。同様、職場から送受信される電子メールも、個人的なインターネット利用の監視によって得られた情報も、ECHR8 条の下で保護されるべきである」¹⁹⁸と判示した。さらに本判決も、Halford 事件判決で用いられた「プライバシー保護に対する合理的期待の法理」を再び採用し、本件では、X は通話などが監視されるとの警告を受けていなかったため、職場の電話の使用、電子メールおよびインターネットの使用に関してプライバシーの合理的期待があっ

¹⁹⁵ M. Ford, *Two Conceptions of Worker Privacy*, 31(2) INDUS. L.J. 133, 144-145(2002).

¹⁹⁶ Copland v. United Kingdom, (App.62617/00), 3 April 2007, (2007) 45 EHRR 959, ECHR 2007-IV.

¹⁹⁷ *Id.* §39.

¹⁹⁸ *Id.* §41.

たとした¹⁹⁹。また、本件監視によって得られたデータは使用していないという Y の主張に対し、人権裁判所は、「Y が保有するデータが開示されず、懲戒その他の手続において X に不利に使用されなかったことは、X が私生活の干渉を受けたかどうかという問題とは無関係である」とした。結論として、Y が、X の電話、電子メール、インターネットの利用状況に関する個人情報を X が知らないうちに収集・保存したことは、ECHR8 条にいう私生活・通信を尊重する権利に対する干渉にあたるとした²⁰⁰。第 2 段階の 3 要件審査（ECHR8 条 2 項）において、本件監視によってもたらされた X の私生活と通信への干渉が、同条によって正当化されるかどうかについて、本判決はまず、本件監視が『法に従ったもの』であるかどうかを判断した。具体的には、本件当時、使用者が従業員の電話、電子メール、インターネットの利用を監視することについては、イギリス国内法にも Y 大学にも規定が存在していなかったことを考慮し、人権裁判所は、本件監視は「法に従った」ものではないと結論づけた²⁰¹。

本判決には 2 つの特徴がある。一つ目は Halford 事件判決を踏襲し、ECHR8 条で保護される職場における私生活の範囲を、電話から電子メール及びインターネットにまで拡大した点である。もう一つは、監視によって得られた情報が使用されるか否かにかかわらず、労働者が知らないうちに監視だけで個人データを収集・保存するだけでも、ECHR8 条に違反する可能性があることを本判決が明らかにしたことである。特に、2 点目の特徴については、本判決は伝統的な私生活の保護から個人データ保護への架け橋であるといえよう²⁰²。

第 4 款 Köpke v. Germany 事件²⁰³

¹⁹⁹ *Id.* §42.

²⁰⁰ *Id.* §43-44.

²⁰¹ *Id.* §47-48.

²⁰² なお、たとえ上記のテレコミュニケーション規則が事件当時に存在していたとしても、本判決の結論は変わらなかったとの指摘がある。See S. Wallach, *The Medusa Stare: Surveillance and Monitoring of Employees and the Right to Privacy*, 27 (2) INT. J. COMP. LABOUR LAW IND. RELAT. 189, 210 (2011).

²⁰³ Köpke v. Germany (dec.), (App. 420/07), 5 October 2010. 本件は「判決」ではなく、「決定」であることに留意しなければならない。決定は、干渉が ECHR に違反しているかどうかを判断するものではなく、受理可能性の問題、あるいは人権裁判所に管轄権があるかどうかを判断するものである。さらに、決定は ECHR に対する解釈の既判力を有しないという点で、判決とは異なる。

本件は上記の事件とは異なり、民間企業と従業員、つまり純粋な私人間で生じた紛争である。したがって、人権裁判所が本件で審査したのは、締約国の消極的義務ではなく、積極的義務である。本件では、申立人 X をレジ係として雇用していた Y 社は、会計に不正があったことに気づき、X と他の従業員が会計を不正に操作したことを疑ったため、外部機関である探偵会社に調査を依頼した。同探偵会社は X が働いていたレジのところに秘密裏に監視カメラを設置し、さらに撮影によって得られた画像等に基づいて報告書を作成し、Y に提出した。最終的に、Y はこの報告書に基づいて X の横領行為を確認し、X を解雇した。X は、上記監視は X の知らないうちに行われたものであるため、上記カメラによって得られた証拠の使用は訴訟から排除すべきであると主張し、国内裁判所に訴えを提起した。X は国内の救済を尽くした後、人権裁判所に提訴した。

本決定はまず、監視カメラの使用は個人データを記録するという性質と、その記録が恒久的に保存される可能性があることから、個人の私生活に対する侵害が生じうると判断した²⁰⁴。次に、本決定は、職場における X の行動を監視する監視カメラは事前に X に知らせないまま行われ、しかも撮影された画像は使用者によって処理され、さらに国内裁判所の訴訟手続においても使用されたことを考慮し、Y による監視は ECHR8 条にいう X の「私生活」に影響を及ぼしたとした²⁰⁵。また、本決定は、Halford 事件で採用されたプライバシーの合理的期待の法理を用いながらも、「必ずしも決定的ではないが、重要な要素である」という一文を加えることによって、同法理を修正した。プライバシーの合理的期待の法理に対するこの修正は、本判決以降の監視に関する事件においてそのまま踏襲されている。

次に、本決定は、被告国の積極的義務について、「ECHR8 条に基づく締約国の積極的義務と消極的義務の間の境界は、精確な定義には適さない。いずれの状況においても、対立する利益の間で公平なバランスを図らなければならない。さらに、いずれの場合においても国には一定の評価の余地がある。…また、個人の行為に対する保護のための ECHR8 条を確保する手段の選択は、原則として、国家の裁量の範囲内である」とした。さらに、この判断を踏まえ、本決定は、ECHR8 条の締約国の積極的義務に関連し、X の私生活を尊重する権利と、議定書第 1 条によって保障されている企業の財産権の保護およ

²⁰⁴ *Id.* p.8.

²⁰⁵ *Ibid.*

び適切な運営という利益との間で公平なバランスを取ったかどうかを検討しなければならない。本決定は、事件当時の被告国であったドイツには使用者の監視を規制する法律がなかったものの、連邦労働裁判所の判例法理は使用者の監視が実施される際に労働者のプライバシーに十分な保護を提供していると判断し、さらに使用者による監視が適法なものと認められるためには、①監視の対象者、②監視実施の期間、④監視の範囲、⑤監視の結果にアクセスできる者、および⑥手段の代替可能性）を考慮する必要があるとした²⁰⁶。本件の状況を上記①から⑥の要件に当てはめると、本決定はまず、本件監視の対象となったのは X ともう一人の従業員のみであったこと、また、本件監視は 2 週間という限られた期間であったこと、さらに、監視が行われたのはレジの裏側のエリアのみであり、監視の結果にアクセスできたのは上記の探偵会社に勤務する限られた人数と使用者の従業員のみであったこと、本件で用いられた方法（使用者による直接監視や公開された監視カメラの利用）と同等の効果的な手段はなかったことから、被告国の国内裁判所が当事者間の公平なバランスをとっているため、X の請求は明らかに根拠が不十分として、棄却した。

なお、本判決は、同判決の最後の部分で、「私生活への侵入が新しい、より洗練された技術によってどの程度可能になったかを考慮すれば、将来、対立する利益には異なるウェイトが与えられるかもしれない」と付け加えた。この付言は次款の *Bărbulescu* 事件と呼応している。

第 5 款 *Bărbulescu v. Romania* 事件²⁰⁷

本判決は、世界中の労働法研究者の注目を集めており、民間企業が従業員を監視する問題を考える上で非常に大きな意義があるため、以下では本判決を詳しく検討する。

本件では、会社 Y に顧客エンジニアとして雇用されていた労働者 X が、使用者の命令に応じて業務のために登録したインスタントメッセージ（Yahoo! Messenger）のアカウントを使用者に監視された事件である。2007

²⁰⁶ *Id.* p.11.

²⁰⁷ *Bărbulescu v. Romania*, (App.61496/08), 5 September 2017[GC]. 本判決の日本語の評釈として、波多江悟史「判批」人権判例報 1 号（2020 年）39-45 頁と實原隆志「判批」国際人権 29 号（2018 年）104-105 頁がある。

年7月3日に、Yは、「業務用のコンピュータやインターネット等の私用禁止と監視される可能性」に関する通知書を、Xを含む従業員に対して当該通知書を熟読した上でそのコピーに署名するよう求めた。Xは、上記通知書の内容に署名した。その後、Yは同年7月5日から12日までの間、Xのインスタントメッセージでの通信を監視していた（以下では、本件監視と略称する）。その過程で、Yは、Xが勤務時間中にインターネットを私的に利用していたこと（婚約者や家族メンバーとの会話）を発見し、Xに対してそれに関する説明を求めたが、Xは上記私的利用の事実を否定した。最終的に、Yは、XがYの就業規則に違反したとして、Xを解雇した²⁰⁸。Xはルーマニア国内裁判所に対し、違法な監視手段による解雇の無効及び種々の支払いを求めた。被告国の国内裁判所は、Xが会社のコンピュータの私用禁止について事前に知らされていたとして、Xの請求を棄却した。Xは国内の救済を尽くした後、被告国の国内裁判所がYによるECHR8条の侵害侵害を是正しなかったとして、人権裁判所に申し立てた。

(1) 大法廷の判断

大法廷はまず、上記Xのインスタントメッセージによる通信が、ECHR8条における私生活等を尊重する権利の一部に属するか否かという受理可能性の問題について、上記検討した監視に関する諸事件の判断を踏襲し、『私生活』は広範な用語であり、網羅的な定義は不可能である。ECHR8条は、人格の面であれ、個人の自律の面であれ、人格形成の権利を保護するものであり、これはECHR8条の保障の解釈の基礎となる重要な原則である。当裁判所は、すべての人が私生活を営む権利を有し、不必要な注目を避けることができることを認めている。また、『私生活』という概念を、個人が自分の選択に従って個人生活を送ることができる『内輪』に限定し、その内輪に含まれない外界を完全に排除することは、あまりにも制限的であると考えている。このように、ECHR8条は、『私的な社会生活 (Private social life)』を営む権利、すなわち個人が社会的アイデンティティを発展させる可能性 (Possibility for the individual to develop his or her social identity) を含む、広い意味での『私生活』の権利を保障しているのである（下線は筆者による）。……また、『私生活』の概念には職業上の活動が含まれる可能性があり、公的な場

²⁰⁸ 事業場の秩序や規律を乱すこと、特に……コンピュータ、コピー機、電話、テレックス、ファクスを個人的な目的で使用することは固く禁じられている。

所で行われた活動も含まれている。そのため、個人の職業生活に対する制限が、他者との関係を発展させることによって自己の社会的アイデンティティを構築する方法に影響を及ぼす場合には、ECHR8 条の適用を受ける可能性がある。ほとんどの人が、外部世界との関係を発展させる最大の機会ではないにせよ、重要な機会を持つのは、職業生活の過程である」²⁰⁹。次に、X が利用したインスタントメッセージにプライバシー保護に対する合理的期待があったか否かについて、大法廷は、「プライバシー保護に対する合理的期待は、必ずしも決定的ではないが、重要な要素と明確に判断している」とし、明確に前掲の Köpke 事件（決定）を引用した²¹⁰。最後に、X の通信が私生活の定義に含まれているか否かについて、本件のインスタントメッセージは、たとえその送受信が Y のコンピュータから操作されたものであっても、個人が私的な社会生活を送るためのコミュニケーションの 1 形態にすぎないため、ECHR8 条の「通信」により保護されるものであるとした。さらに、大法廷は、X は、私的なインターネット使用の禁止については確実に知らされていた一方で、本件監視活動の範囲と性質、あるいは Y が実際の通信内容にアクセスできる可能性については事前に知らされていなかった（下線は筆者による）ため、本件 X のインスタントメッセージの通信内容は、ECHR8 条の「私生活」と「通信」に含まれると判示した²¹¹。

本件監視が X の ECHR8 条によって保護される権利を侵害したことを認めた大法廷は、国内裁判所が、本件監視について、同 8 条に基づく X の権利との間で公平なバランスを図っていたかどうかを審査し、被告国は少なくとも、①使用者が通信やその他のコミュニケーションを監視する措置を設置する可能性、およびその措置の実施について、労働者に知らせたかどうか、②監視の範囲と従業員の私生活保護に対する侵害の度合い、③使用者が監視を正当化する根拠を有していたかどうか、④従業員の通信内容に直接アクセスするよりも、より侵襲性の低い方法・手段で監視を行う余地がなかったか、⑤従業員に対する監視の結果、および使用者による監視結果の利用、特にその結果が本来監視によって追及された目的を達成するために利用されたかどうか、⑥侵入的性質を有する監視に対する十分な保護措置があったかどうか、とい

²⁰⁹ See case *supra* note 207, §70-71.

²¹⁰ *Id.* §73.

²¹¹ *Id.* §74-81.

う基準を設けるべきであるとした²¹²。

大法廷は、以上の①から⑥までの基準に照らし、国内裁判所が会社の円滑な運営を確保する使用者の権利と、X の私生活と通信を尊重する権利を判断する際に、上記の基準をどのように判断したかを審査した²¹³。①の X が事前に監視の対象となる可能性について知らされていたかどうかについて、「X は、使用者の監視活動の範囲と性質及び、使用者が通信の内容に直接的にアクセスできる可能性について事前に知らされていなかった」とし、この点について、国内裁判所が「従業員は会社の資源を私的な目的で使用してはならない」という Y の就業規則しか認定してないことから、大法廷は国内裁判所において、X が監視の可能性、監視の範囲と性質について事前に知らされていたかどうかについての判断を怠ったと判断した²¹⁴。②の監視の範囲とプライバシー侵害の度合いに関して、Y が監視期間中に X のあらゆる通信をリアルタイムで記録し、さらに X のアカウントの内容をプリントアウトしていた事実を考慮しなかった国内裁判所の判断は不十分であると判断した²¹⁵。③の本件監視に正当な理由があったかどうかについて、大法廷は、国内裁判所がこの基準についてある程度判断したが、いずれも抽象的なものにすぎず、X の行為が実際に Y にリスクをもたらしたことを認めるに足りる証拠はないとは認めず、④の本件監視よりも侵入性の低い監視を行う可能性があったかどうかに関して、大法廷は、国内裁判所が、X の通信内容に直接アクセスするよりも、より侵入性の低い方法で Y が追求した目的を達成できたか否かを十分に検討していなかったと判断し、⑤の監視の対象に対する影響に関して、国内裁判所が本件監視の結果、つまり懲戒解雇の重大性を考慮していなかったと判断し、⑥の侵入的性質を有する監視に対する十分な保護措置があったかどうかについて、大法廷は、Y が X に対してインターネットの私的利用について説明を求めた際、使用者がすでに X の私生活に関する内容にアクセスしたことを国内裁判所が判断していないとした²¹⁶。

結論として、大法廷は、被告国に評価の余地があることを考慮したものの、国内裁判所が X の私生活および通信を尊重する権利を十分な保護を提供する

²¹² *Id.* §121.

²¹³ *Id.* §132.

²¹⁴ *Id.* §133.

²¹⁵ *Id.* §134.

²¹⁶ *Id.* §135-138.

ことができなかったため、被告国は ECHR8 条に違反したと判断した²¹⁷。

(2) 反対意見

本件監視が ECHR8 条に違反したという上記の結論に反対した 6 人の判事によって執筆された反対意見がある。反対意見は、多数意見の一部（X がプライバシー保護に対する合理的期待を有していた点、本件を積極的義務の観点から検討した点、本件インスタントメッセージの通信が ECHR8 条に含まれる点）に同意するものの、国内裁判所が、対立する利益の間で公平なバランスをとっていないという多数意見の結論には反対した²¹⁸。具体的には、多数意見が被告国において使用者が実施する監視に対する適切な規制があったかどうかを判断した際、被告国の労働法上の規制のみを不当に絞っており、被告国の刑法や民法上の判断枠組みを考慮しなかった点に疑問があると指摘し、また、使用者が実施する監視を規制するための法的な判断枠組みをいかに構築するかということは、被告国の広い評価の余地の範囲内に属するため、多数意見は被告国の有する上記余地を十分に尊重しなかったと主張した²¹⁹。次に反対意見は、たとえ多数意見が提示した前述の①から⑥までの判断基準に基づいて本件を分析したとしても、その分析は不十分であると指摘した²²⁰。具体的には、まず X が Y による監視について事前に通知を受けていたかどうかについて、X が署名した「業務用のコンピュータやインターネット等の私用禁止」という通知書は、従業員の通信が監視の対象となる可能性を示唆したことから、X の通信に対するプライバシーに対する合理的期待は相当低下しており、そのため、X は自分の活動が監視の対象となることを合理的に予想できたと指摘した²²¹。次に、本件監視に正当な理由があったかどうかについて、国内裁判所が、会社の円滑な運営を確保するために労働者の業務遂行を監視する使用者の権利を、X の私生活や通信を尊重する権利よりも優先させたことは不合理ではないと述べた。というのも、使用者の利益を労働者の利益よりも優先させる国内裁判所の判断は、ECHR 上の問題を引き起こすこ

²¹⁷ *Id.* §139 and 141.

²¹⁸ Joint dissenting opinion of Judges Raimondi, Dedov, Kjølbros, Mits, Mourou-Vikström and Eicke, §1-2.

²¹⁹ *Id.* §15-16.

²²⁰ *Id.* §18.

²²¹ *Id.* §19-20.

とはできず、被告国が有する評価の余地内の問題だからである²²²。最後に、本件監視の期間、対象及び目的が限定的であり、X の通信内容に懲戒解雇手続の関係者しかアクセスできなかったことことに留意した²²³。なお、懲戒手続の間に X が示した態度について、多数意見は言及していないが、X が当初、通信内容には私的な内容は含まれていないと主張していたが、これは事実ではなかったことに留意した²²⁴。以上を踏まえ、反対意見は、国内裁判所が X の私生活および通信の尊重に対する保護を欠いていたとは言えず、被告国は ECHR8 条に違反しないと結論づけた²²⁵。

(3) 本判決の意義と学説上の議論

本判決は人権裁判所が初めて民間企業による監視に対する法的な判断基準（バルブレスク基準とも呼ばれている²²⁶）を提示し、監視の適法性を検討した「判決」である（前述の Köpke 事件は決定である）。また、本件は、前述の Halford 事件と Copland 事件で使用者が監視の可能性について従業員に通知しなかったのとは異なり、労働者は少なくとも職場における私的通信が禁止されていることを認識していたという点において異なる。また、本判決が確立した監視のバルブレスク基準は、使用者による監視が濫用にあたるかどうかを検討する際に、各国の裁判所が重要な基準となる²²⁷。というのも、ECHR 締約国の裁判所が本判決の判断基準に基づいて判断しない場合、締約国は ECHR 違反の責任を問われるからである²²⁸。さらに、バルブレスク基準は、各国の裁判所だけでなく、締約国の企業に対しても、同基準に一致させるよう就業規則の修正を間接的に要請しているとの重要な見解もある²²⁹。また、バルブレスク基準は、職場における監視の適法性に関する判断を明確化することができるだけでなく、GDPR が定めている個人情報処理の透明性を高め

²²² *Id.* §22-23.

²²³ *Id.* §24.

²²⁴ *Id.* §25.

²²⁵ *Id.* §27.

²²⁶ 波多・前掲注 207) 39 頁。

²²⁷ Eurofound, *supra* note 13, p. 20.

²²⁸ *Ibid.*

²²⁹ Abdurrahimli, *supra* note 2, p. 61; Q&A Grand Chamber judgment in the case of Bărbulescu v. Romania (App.61496/08) p. 3. https://www.echr.coe.int/documents/d/echr/Press_Q_A_Barbulescu_ENG, last visited 12 July 2023.

る効果もあるとの指摘がある²³⁰。このほか、プライバシー保護に対する合理的期待の法理の判断に関して、本判決が前掲の Köpke 事件の判断（プライバシー保護に対する合理的期待は、必ずしも決定的ではないが、重要な要素）を承認していることから、今後監視の適法性を審査する上で、これまで用いられてきた同法理の重要性は失われていくであろうとの見解がある²³¹。同見解によれば、同法理は個人が ECHR8 条の保護を受けるか否かの試金石（Touchstone）とみなされていたが、技術の発展に伴い、使用者がより優れた監視機器を職場に導入したことで、必然的に労働者のプライバシー保護に対する合理的期待を低下させ、その結果、ECHR8 条によって提供される保護の範囲が狭まるというリスクが生じると指摘されている²³²。本判決は、まさにこのリスクを認識した上で、労働者のプライバシーを制限するような就業規則が作成されたとしても、ECHR8 条の保護をゼロにすることは不可能であると判断したのである²³³。最後に、人権裁判所元所長である Raimondi は、2018 年の人権裁判所のヒアリングにおいて、バルブレスク基準が、今後使用者による監視の事件を判断する各国の裁判所の「必携なガイドライン（Vade mecum）」となることを明言した²³⁴

第 6 款 López Ribalda et al. v. Spain 事件²³⁵

本件では、Y が経営するスーパーマーケットにおいてレジ係またはカウンターでの販売補助者として雇用されていた原告労働者 X1～X5 が、スーパーマーケットに設置された複数の監視カメラ（本件では、X らは事前に可視的な監視カメラについては通知されていたが、レジ向きの隠し監視カメラについては通知されていなかった）によって撮影された X らが窃盗をしている画像に基づいて解雇された。国内で利用可能な救済を尽くした後、X らは、本件

²³⁰ K. Mania, Monitoring of the employee's Internet use in the workplace in the light of selected case law of the European Court of Human Rights and Polish case law, 4(4) Przegląd Europejski. 63, 75 (2019).

²³¹ J. Atkinson, Workplace Monitoring and the Right to Private Life at Work, 81(4) MLR. 688, 697 (2018).

²³² *Id.* p.696.

²³³ RAINEY ET AL., *Supra* note 138, p.697.

²³⁴ Solemn Hearing of the European Court of Human Rights President Guido Raimondi's opening speech Strasbourg, 26 January 2018, p.5. https://www.echr.coe.int/documents/d/echr/speech_20180126_raimondi_jy_eng, last visited 12 July 2023.学説も同旨, Komanovics, *supra* note 182, p. 461.

²³⁵ López Ribalda et al. v. Spain, (App.1874/13), 17 October 2019 [GC].

監視カメラが同人らの ECHR8 条に保護される権利を侵害したとして、人権裁判所に訴訟を提起した。

(1) 大法廷の判断

ECHR8 条の私生活の概念について、大法廷は前述の *Bărbulescu* 事件判決の判旨を引用したため、ここでは省略する。

X らは、プライバシー保護に対する合理的期待を有していたかどうか (ECHR8 条の受理可能性) について、大法廷は、「本件スーパーマーケットは公衆に開放されている場所であり、そこで監視カメラによる撮影は親密で私的な性質のものではない。したがって、本件のような場所におけるプライバシー保護に対する合理的期待は必然的に制限されるといわざるを得ない。しかし、公共の場であっても、特定された人物の画像を体系的または恒久的に記録し、さらに画像を処理することは、撮影の対象の私生活に影響を及ぼす可能性がある。X らは、Y がスーパーマーケットの出入り口に監視カメラを設置したことを事前に知らされていたにもかかわらず、事前に知らされていなかった店内の他の場所で監視の対象にならないとのプライバシー保護への合理的な期待を抱いていた。……したがって、本件において ECHR8 条が受理可能であることを認めた」とした²³⁶。次に、大法廷は、本件が私人間の問題であるため、被告国の積極的義務という観点、すなわち国内裁判所が X らの私生活の尊重を受ける権利と、Y の財産を保護し会社の円滑な運営を確保するという利益という対立する利益の間で公平なバランスをとっていたかどうかを審査した。具体的な審査において、大法廷は、前述の *Köpke* 事件判決の判断を参照した上で判断した²³⁷。まず、本件監視の実施に正当な目的があったかどうかについて、「盗難が従業員によって行われたという合理的疑いがあるため、使用者の財産の保護と会社の円滑な機能を確保する必要性がある」という国内裁判所の判断を認めた²³⁸。次に、本件監視の範囲と X らのプライバシーに対する侵害の度合いという点に関して、本件監視の対象となるエリアと対象は限定的であり、その期間は盗難の疑いを確認するために必要な限度を超えていなかったという国内裁判所の判断は不合

²³⁶ *Id.* §93-95.

²³⁷ *Id.* §116.

²³⁸ *Id.* §123.

理ではないと判断した²³⁹。具体的には、本件隠し監視カメラは、レジで働く従業員全員を対象としており、常時、無制限に作動していた（これに対して、前掲の Köpke 事件では、監視カメラは特定の従業員を対象としていた）。また、本件監視の期間という点に関して、Y は事前に監視カメラの期間を定めていなかったが、盗難を犯した従業員が特定されるとすぐに中止されたため、本件監視の長さ自体は過度的なものとは言えない（一方、前掲の Köpke 事件では、14 日間という期間は不釣り合いとは認められなかった）とした²⁴⁰。このほか、本件監視カメラによって得られた録画にアクセスできたのは、スーパーマーケットの店長、会社の法定代理人、労働組合の代表者だけであったことから、大法廷は、本件監視カメラによる X らのプライバシーへの侵害は高度の重大性は高くなかったと判断した²⁴¹。最後の 2 点について、まず、本件監視が X らにもたらした影響という点に関して、本件録画に基づく懲戒解雇が X らに与える影響は重大であったと認めている²⁴²。次に、本件監視より少ない他の手段があったかどうかという点に関して、本件窃盗の範囲や当該違法行為が複数の従業員による犯行であったことから、隠し監視カメラ設置に関する情報を従業員に事前に提供することは、本件窃盗の責任者を特定し、懲戒手続において犯人の特定に使用する証拠の取得を妨げる可能性が高いと判断した²⁴³。もっとも、大法廷は、使用者が従業員の私生活への侵害がより少ない他の手段を用いることができた可能性について、国内裁判所がより詳細に検討することが望ましいと付言した²⁴⁴。

また、本件で最も困難な問題、すなわち、Y が本件監視を行う前に X らに通知したかどうかという点に関して、大法廷は、「監視の対象となった個人への事前通知とその範囲は、使用者によって行われた監視措置の比例性を審査するために考慮されるべき基準の一つにすぎない（下線は筆者による）。しかし、そのような事前通知が欠如している場合、他の基準がより重要になる。……事前通知の重要性を考慮すると、重要な公共的利益または私人の利益の保護に関連する優先的要件（Overriding requirement）のみが、事前通知の欠如を正

²³⁹ *Id.* §124.

²⁴⁰ *Id.* §126.

²⁴¹ *Id.* §126.

²⁴² *Id.* §127-128.

²⁴³ *Id.* §127-128.

²⁴⁴ *Id.* §128.

当化しうる」という *Bărbulescu* 事件判決の判断とは異なる意見を判示した²⁴⁵。この点に関して、本件には重要な公共的利益または私人の利益を保護する優先的な利益があったかどうかに関して、「一般的には、従業員による窃盗やその他の不正行為に対するわずかな疑いが、使用者による隠し監視カメラの設置を正当化するという考え方を受け入れることはできないが、深刻な違法行為（*Serious misconduct*）が行われたという合理的な疑い（*Reasonable suspicion*）の存在と、本件で確認された Y の損失の程度は、本件における事前通知の欠如を正当化することができる。本件窃盗は、一人の従業員の違法行為だけでなく、むしろ複数の従業員による共同行動によって企業の円滑な機能が損なわれるようなものである。このことは、職場に不信の雰囲気を生み出した重大な問題がある」とした²⁴⁶。以上のことから、スペインの法的枠組（特に、スペイン個人情報保護法 5 条）によって提供された保護と国内裁判所の判断を考慮すると、大法廷は、被告国が ECHR8 条に基づく積極的義務を遵守していなかったとはいえないと結論づけた²⁴⁷。

（2）反対意見²⁴⁸

上記大法廷の判断に対し、3 人の判事からなる反対意見がある。反対意見によれば、まず、*Köpke* 事件以来、監視技術とそれを利用して収集されるデータの利用が大きく発展し、このような新しい技術によって、誰でも、特定の場所・時間に拘束されず、管理・追跡といった制限を受けることなく、保存されたデータにアクセスすることが可能になったことを考慮すると、「本件監視カメラによって得られた録画を閲覧したのは、Y、Y の法定代理人、および従業員代表だけであった」という多数意見の判断には疑問があるという²⁴⁹。次に、監視カメラは、技術の発展とともに安価でその利用が容易になっている一方で、ECHR8 条上の権利を大いに侵害する可能性があるとの観点から、ECHR の締約国は適切かつ効果的な保護枠組みを構築することが最も重要であるとした²⁵⁰。反対意見は、被告国の法的枠組みが、監視装置の設置・使用

²⁴⁵ *Id.* §131-133.

²⁴⁶ *Id.* §134.

²⁴⁷ *Id.* §137.

²⁴⁸ Joint dissenting opinion of judges De Gaetano, Yudkivska and Grozev.

²⁴⁹ *Id.* §3.

²⁵⁰ *Id.* §4.

に先立ち従業員への通知を義務付けており、この保障に対する例外を一切認めていないことが、本件における決定的な判断基準であると考えているが、多数意見はこの要件を、単に比例性テストを評価する際に考慮されるべき「一つの基準」として捉えた。このような多数意見の判断は、被告国の法的枠組みの要件を明らかに満たしていない²⁵¹。反対意見は、より侵入性の低い手段があったか否かとの要件について、多数意見は、国内裁判所がこの点を十分に検討したかどうかを審査していないという問題を指摘した²⁵²。さらに、本件窃盗の責任者を特定し、Y の損害を防止するという目的は合法的なものであるが、Y が従業員や顧客によるさらなる犯罪を阻止しようとする場合、監視カメラが設置されたことを公衆ないし従業員に知らせるだけで十分である。さらに、本件窃盗は犯罪行為であるため、使用者は自らの判断で隠し監視カメラのような措置を講じる前に警察に相談することができ、またはそうすべきである。しかし、多数意見は、使用者による私的調査を非難せず、むしろ使用者が自ら法的問題に対処するよう促す可能性がある²⁵³。

最後に、反対意見は、重大な違法行為があったという「合理的な疑い」がある限り、隠し監視カメラが正当化され得るという多数意見の判断は、従業員のプライバシーを保護するには不十分であると指摘した²⁵⁴。本件のように、使用者が従業員に事前に通知することなく隠し監視カメラを設置・利用した状況においては、刑事訴訟手続における公的機関による秘密監視の実施と同様に、手続上の保護措置を追加する必要がある。そのため、反対意見は、重大な違法行為の存在に関する「合理的な疑い」を、第三者の機関によって検証できる手続上の要件と、当該監視の正当性が「事後的に」その機関によって与えられることに対する保障は、ECHR8 条に基づく要件であると主張している²⁵⁵。

²⁵¹ *Id.* §7. ここでいう法的判断枠組みとは、スペインの個人情報保護法（Organic Law no. 15/1999）5条である。同法 5 条は、「1.個人データを要求されたデータ主体は、事前に、明示的に、正確かつ明確に、以下の事項を通知されなければならない：(a) 個人データファイルの存在またはデータ処理の事実、その目的および情報の受領者；(b) データ収集の要求に対する回答の義務性または任意性、(c)個人データを提供した場合または提供を拒否した場合の結果；(d) データへのアクセス、修正、消去、異議申し立ての権利の有無；(e) 管理者または必要に応じてその代理人の身元および住所」であると定めている。

²⁵² *Id.* §8.

²⁵³ *Id.* §9.

²⁵⁴ *Id.* §10.

²⁵⁵ *Ibid.*

(3) 学説上の議論

本判決は、前掲の *Bărbulescu* 事件以来、人権裁判所が再び民間企業と労働者の間の紛争について判断を下したものである。さらに、本判決は、バルブレスク基準に基づいて判断したが、前掲の *Bărbulescu* 事件判決とは正反対の結論を下したという点に特徴がある。すなわち、本件における大法廷の判断の最も大きな特徴は、ECHR8 条の侵害があったかどうかを判断する際に、本判決が監視装置の導入および利益に関する従業員への事前通知の要件を犠牲にする可能性を認めたということである。大法廷のこの判断に対して批判的な意見を示す学説は少なくない。例えば、使用者の事前通知の義務を不要にできるという本判決の判断は、その義務を課している大半の欧州各国の個人データ保護法と相容れないばかりか、GDPR5 条 1 項 (a) の透明性原則にも反しているとする見解がある²⁵⁶。また、本判決は、事件の特殊性（従業員による集団横領）に由来するものであると理解されているが、その判断によって前掲の *Bărbulescu* 事件判決が構築したバルブレスク基準の明確性が損なわれたとする見解もある²⁵⁷。これらの見解が共通しているのは、本判決がバルブレスク基準を曖昧にしたということである²⁵⁸。なお、上記本判決の解釈（従業員の事前通知義務を不要としたこと）が、バルブレスク基準を修正したとしても、その射程は非常に制限的であるとする見解もある²⁵⁹。というのも、人権裁判所は、各事案における「重大な正当性要件」、「合理的な疑い」及び「深刻な不正行為」の有無を慎重に評価する必要があると判示したからであ

²⁵⁶ É A. CAPRIOLI, *Cybersurveillance et respect de la vie privée - Absence de violation du droit à la vie privée de caissières espagnoles filmées par des caméras de surveillance non portées à leur connaissance*, CCE n°12, 2019, n° 80.

²⁵⁷ Bergiannis, *supra* note 258. P. Collins, *The Right to Privacy, Surveillance-by-Software and the “Home-Workplace”*, (3 Sept. 2020), <https://uklabourlawblog.com/2020/09/03/the-right-to-privacy-surveillance-by-software-and-the-home-workplace-by-dr-philippa-collins/>, last visited 12 Dec. 2023.

²⁵⁸ F. Bergiannis, López Ribalda and otehr V. Spain- Covert surveillance in the workplace: Attenuating the protection of privacy for employees, (6 Dec. 2019), <https://strasbourgobservers.com/2019/12/06/lopez-ribalda-and-others-v-spain-covert-surveillance-in-the-workplace-attenuating-the-protection-of-privacy-for-employees/#more-4471>, last visited 13 Nov. 2023 ; R. Federico, *The Employee’s Right to Privacy and the Employer’s Powers: Recent Jurisprudence of the European Court of Human Rights*, p. 16 (2020), Available at <https://ssrn.com/abstract=3586825>.

²⁵⁹ H. Sanzey, *Vie privée du salarié- Licéité de la vidéosurveillance en entreprise malgré l’absence d’information des salariés-*, JCP S 2020, n°6-7. Eurofound, *supra* note 13, p. 20.

る²⁶⁰。他方、本判決は、本件における従業員の私生活への侵害がより少ない他の手段があったかという基準について、国内裁判所がより詳細に検討することが望ましいと判断したが、大法廷自身もこの点を審査することなく、安易に国内裁判所の判断を受け入れた点には疑問があると解する見解がある²⁶¹。たとえば、警備員の設置や、労働組合との協議といった方法は、本件 Y が直接的に隠しカメラを導入することよりも、X らの私生活への侵害がより少ない例として挙げられている²⁶²。

第 7 款 Florindo de Almedia Vasconcelos Gramaxo v. Portugal 事件²⁶³

本件では、Y に医薬情報担当者（いわゆる、Medical representative, MR）として雇用されていた X が、Y から貸与された社用車に GPS 機能付き装置を取り付けた（以下、GPS 装置という）ことに反対し、社用車に搭載された GPS 装置を破壊し、業務と関係ない私的な目的での走行距離を実際より減し、業務目的での走行距離を不正申告したことを理由に懲戒解雇された。Y は X を含む MR に対して GPS 装置の導入とその影響に関する通知書を署名するよう求め、X はそれに署名していた。被告国のすべての救済手段を尽くしたため、X は GPS 装置の利用が ECHR8 条を侵害したとして、人権裁判所に申し立てた。

これまでの事件と同様に、本判決はまず、本件 ECHR8 条に対する侵害が同条の適用範囲に含まれているか否か（受理可能性に関する審査）を検討し、X と Y が私人であったことから、本判決は被告国の積極的義務に照らして、国内裁判所が対立する利益の間で公平なバランスをとっていたかどうかを審査した。まず、ECHR8 条の受理可能性に関して、本判決は前掲の López Ribalda et al 事件の判旨をそのまま引用した。すなわち、ECHR8 条にいう私生活は、「各個人が外部からの干渉を受けずに個人生活を送ることができる『内輪』に限らず、『私的な社会生活』を送る権利、すなわち個人が他の人間や外部との関係を確立し発展させる可能性も含まれている。そのため、私生活の概念は職業活動や公的場所で行われる活動を排除するものではない。……個人がプライバシーに対する合理的期待を有するかどうかは、必ずしも決定的

²⁶⁰ *Ibid.*

²⁶¹ Komanovics, *supra* note 182, p. 464.

²⁶² Bergiannis, *supra* note 258.

²⁶³ Florindo de Almedia Vasconcelos Gramaxo c. Portugal (App. 26968/16), 13 December 2022.

な要素ではないものの、重要な要素である」²⁶⁴。次に、GPS 機能付き装置による位置情報の監視について、本判決は、「本件 GPS システムは、恒久的かつ体系的に X の勤務時間中と勤務時間外の両方で位置情報を取得することが可能であり、また、本件 GPS 機能付き装置によって収集された X の位置情報は、X を解雇した根拠となり、X の私生活に深刻な影響を与えたことは否定できない」とし、ECHR8 条が本件に適用されると判断した²⁶⁵。

国内裁判所が本件 GPS 装置による干渉と従業員の私生活の尊重を受ける権利との間で公平なバランスをとっていたか否かについて、前述のバルブレスク基準の類推適用 (*Mutatis mutandis*) を通じて本件を判断できるとした²⁶⁶。具体的には、①X が事前に、Y が本件 GPS 機能付き装置による監視を導入・実施する可能性について知らされていたかどうか、②本件 GPS 装置の監視範囲と、X の私生活への侵害の度合い、③本件 GPS 装置による監視の実施には正当な理由の有無、④本件 GPS 装置による監視よりも、より侵入性の低い手段や方法があったかどうか、⑤本件 GPS 装置による監視の結果が X にどのような影響を与えたか、⑥被告国には本件 GPS 装置による監視に関する適切な保護措置があったかどうか。本判決は、以上の基準に照らして、上記①の要件（事前通知の有無）に関しては、X が社用車には GPS 装置が搭載されることを知らされていたことと、X が Y 社の送付した本件装置の設置及びその理由に関する文書に署名していることに留意し、X は、Y が社用車に GPS 装置を取り付け、自らの職業活動と私的活動における移動距離を監視したことを知っていたとした²⁶⁷。次に、②と③（監視の範囲と侵害の度合いと監視の導入・実施に正当な理由があったかどうか）に関しては、本件 GPS き装置が会社経費の管理のために利用されたという目的は正当であり、また、業務遂行の監視によって得られた X の位置情報（X の勤務時間中の位置情報）は国内裁判所から訴訟から排除されたことから、本件監視の範囲と X の私生活への侵入の度合いは必要な範囲に限定されていると判示した²⁶⁸。④の、本件 GPS 装置と比較してより侵入的でない手段があったかどうかという要件に関しては、Y が本件 GPS 装置を利用しなかった場合、業務上および個人的な移動距

²⁶⁴ *Id.* §92.

²⁶⁵ *Id.* §96-97.

²⁶⁶ *See case supra* note 263, §109.

²⁶⁷ *Id.* §116.

²⁶⁸ *Id.* §120.

離を決定することが困難であるという国内裁判所の判断に対し、本判決はこれと異なる判断を下す必要がないと判断した²⁶⁹。⑤の本件監視結果にアクセスできる人数とその職位等という要件に関しては、X の位置情報の伝達範囲は非常に限定的であり、実際、限られた一部の責任者だけが X の位置情報にアクセスできたと確認した²⁷⁰。最後に、⑥の要件に関しては、被告国には、労働法典 20 条²⁷¹を含めて使用者による監視を規制するいくつかの法律が存在していることを確認した²⁷²。

以上のことから、本判決は、国内裁判所が社用車の経費を管理するという本件 GPS 装置の利用に関する Y の利益と、X の私生活を保護する利益とのバランスをとっていたと判断した。したがって、被告国が与えられた評価の余地を超えておらず、X の私生活の尊重を受ける権利を保護する積極的義務を怠ったとは言えないと結論づけた²⁷³。

(1) 反対意見²⁷⁴

上記多数意見に対して、3 人の判事からなる反対意見がある。反対意見はまず、本件 GPS 装置による監視の時間は 3 年間に近く、使用者による監視に関する従来の人権裁判所の判例法が要求している期間を明らかに超えていると指摘した²⁷⁵。また、本件 GPS 装置によって収集された X の勤務期間中の位置情報のみを排除し、それ以外の期間の位置情報を排除しなかった国内裁判所の判断は、ポルトガル個人情報保護法に違反するとした²⁷⁶。というのも、ポルトガル個人情報保護法によれば、本件 GPS 装置の利用は上記のような勤務期間によって区別されていないためである²⁷⁷。最後に、多数意見が、社用車の業務用と個人用を区別するための簡易なスイッチの導入など、従業員を常時監視する代替手段の可能性を指摘したポルトガル個人情報保護委員会の見

²⁶⁹ *Id.* §122.

²⁷⁰ *Id.* §123.

²⁷¹ ポルトガル労働法典 9 条は、「使用者は、従業員の業務遂行を監視する目的で、技術的な機器の使用を含む職場での遠隔監視手段を使用してはならない」と定めている。

²⁷² *Id.* §112.

²⁷³ *Id.* §124-125.

²⁷⁴ Joint dissenting opinion of judges Motoc, Pastor Vilanova and Guerra Martins.

²⁷⁵ *Id.* §10.例えば、前掲の Köpke 事件においては、監視の期間は 14 日間にとどまった。

²⁷⁶ *Id.* §16.

²⁷⁷ *Ibid.*

解を見落とした点を指摘した²⁷⁸。

(2) 学説上の議論

この事件は、使用者が従業員の位置情報を監視するために利用した GPS 機能付き装置から生じた問題について、人権裁判所が初めて判断した点に特徴がある。学説上、本件の GPS 装置は、勤務時間中と勤務時間外の両方において監視するものであるが、本判決の判断からは、使用者が従業員の業務遂行のみを監視するための GPS 装置を利用する場合、ECHR8 条が適用されない可能性があることが指摘された²⁷⁹。また、前掲の López Ribalda et al. 事件判決と比較して、本判決はバルブレスク基準をより厳格に運用したように見えるとも述べられた。すなわち、バルブレスク基準の各基準を「要素」として捉えた前掲の López Ribalda et al 事件判決の判断とは異なり、本判決は同基準を個々の「要件」として捉え、特に GPS 装置の実施に先立ち、従業員がそれについて知らされていたかどうかという点を重視した²⁸⁰。また、X は約 3 年間、24 時間常時監視されていたことから、本件監視は比例性の基準（バルブレスク基準における、より侵襲性の低い方法・手段で監視を行う可能性の有無という要件）を満たしていないとする見解もある²⁸¹。私見としては、本件の情報提供の時期について若干疑問がある。X は、Y が本件 GPS 装置を利用することを認識したのは、GPS 装置がすでに作動していた時期（厳密に言えば、4 ヶ月後）であった。この場合において、バルブレスク基準が求めている「事前」通知の要件は、本件では満たされていないように思われる。

第 5 節 まとめ

上記で検討した監視に関する人権裁判所の諸判決の特徴をまとめると、以下のようになる。第 1 は、ECHR8 条の私生活の範囲を広く捉えている点である。1992 年の Niemietz 事件判決は、職場における労働者の私生活も ECHR8 条によって保護されることを初めて承認し、同条の保護範囲は、私生活から他者を排除する権利だけではなく、職業生活も含めて他者との関係を築き、発展させる権利もある程度含まれなければならないという重要な内容を示した。

²⁷⁸ *Id.* §17.

²⁷⁹ <http://libertescherries.blogspot.com/2022/12/geolocalisation-et-licenciement.html> , last visited 31 July 2023.

²⁸⁰ *Ibid.*

²⁸¹ Komanovics, *supra* note 182, p. 466.

Niemietz 事件判決の解釈の仕方は、Halford 事件における業務用の電話から、現在は Florindo de Almedia 事件における GPS 機能付き装置にまで及んでおり、人権裁判所の判例法において確立されている。第 2 に、「プライバシー保護の合理的期待」の法理は、ECHR8 条の解釈において重要な役割を果たしてきた。同法理は、Halford 事件判決において初めて用いられ、その後の監視に関する判決でも踏襲されたが、Köpke 事件判決以降、同理論の内容が大幅に修正され、労働者がプライバシー保護に対する合理的期待を有するかどうかは、「決定的な要件ではない」となされた。この法理を修正する目的は、前述したアメリカ法の同法理に関連する問題点を回避するためと推測される。第 3 に、監視に関する判断枠組みについて、人権裁判所は、Halford 事件判決が求めた事前通知義務から始まり、Bărbulescu 事件判決におけるバルブレスク基準の確立に至るまで、監視に関する様々な判決を通じて、監視の適法性審査に関する判断枠組みを漸次構築してきた。しかし、López Ribalda et al. 事件判決では、バルブレスク基準は「要件」から「要素」へと変更された。学説上、前述のように、このような変更は同基準の意義を損なうばかりでなく、結果の予見可能性という観点からも不適切であるとの指摘があり、さらに López Ribalda et al. 事件それ自体の特殊性（従業員による集团的横領）に鑑みれば、バルブレスク基準を要件と捉えることが妥当であるとする見解が多く存在している。実際、人権裁判所もこの点を認識しており、López Ribalda et al. 事件後の Florindo de Almedia 事件判決において、上記判断枠組み同を再び要件として判断した²⁸²。

以上のことから、人権裁判所が、これまでの監視に関する事件の判断をとりまとめて構築したバルブレスク基準は、監視装置の利用から生じる問題を事後的に判断するためだけでなく、企業自身が事前に監視装置の適法性をチェックできるようにするための重要な役割も果たしている。

²⁸² 一方、バルブレスク基準は私人間による紛争の判決で形成された基準であるため、例えば、Antović and Mirković v. Montenegro 事件 (Antović and Mirković v. Montenegro, (App. 70838/13), 28 November 2017) や、Libert v. France 事件 (Libert v. France, (App. 588/13), 22 February 2018) のような私人対公的機関の事件では、人権裁判所はバルブレスク基準を引用したが、依然として ECHR8 条 2 項の 3 要件審査に基づいて私生活侵害の有無を判断している点に留意しなければならない。

第3章 フランス法における問題状況

第1節 序説

日本の労働法学においては、フランス法における労働者のプライバシーと個人情報保護に関する状況を紹介した文献は比較的多いが²⁸³、使用者の監視を検討したものはほとんどない²⁸⁴。そこで、本章ではフランス法における監視の適法性に関する判断枠組みを検討する。

フランス法では長い間、使用者の監視に関する法規定はなく、監視の利用に実質的な制限を加えたのは破毀院とコンセイユ・デタの判例法理であった²⁸⁵。このような状況は、監視の行使を制限する法規定が制定された後もほとんど変わっていない。というのも、これらの法規定の大半は、破毀院の判例法理をそのまま明文化したものである。1990年代後半、監視カメラや自動電話交換機（Autocommutateur téléphonique）²⁸⁶といった新たな監視機器が次々と職場に導入されたことにより、フランスのデータ保護委員会（情報処理および自由に関する国家委員会、Commission nationale de l'informatique et des

²⁸³ 例えば、盛・前掲注 21) 241 頁、盛・前掲注 107) 199 頁以下；砂押以久子「労働者のプライバシー権の保護について（1）～（3 完）」（1）季労 184 号（1997 年）133 頁，（2）同 185 号（1998 年）165 頁，（3）同 186 号（1998 年）195 頁，同「フランスにおける労働者の個人情報保護」日本労働法学会誌 96 号（2000 年）207 頁，砂押・前掲注 20) 10 頁，同「職場のサイバー・サーベイランスと労働者のプライバシー保護」立教法学 65 号（2004 年）；河野奈月「労働関係における個人情報の利用と保護—米仏における採用を巡る情報収集を中心に（1）～（7 完）」①法協 133 巻 12 号（2016 年）1859 頁，②同 134 巻 1 号（2017 年）1 頁，③同 2 号（2017 年）217 頁，④同 3 号（2017 年）341 頁，⑤同 5 号（2017 年）765 頁，⑥135 巻 1 号（2018 年）73 頁，⑦同 11 号（2018 年）2864 頁，同「フランスの個人情報保護法制と労働関係への適用」労働問題リサーチセンター『環境変化の中での労働政策の役割と手法』（2013 年）113 頁。

²⁸⁴ フランス法における監視の問題を包括的に検討した文献として、河野奈月「使用者による労働者の監視に対するフランス労働法の規制」労働問題リサーチセンター『企業行動の変化と労働法政策の課題』（2014 年）258 頁がある。

²⁸⁵ 同上注，265 頁。

²⁸⁶ 従業員が業務用電話を利用する通話時間、通話料金、通話回数の記録を記録することができる装置である。CNIL は、このような装置は自動的に労働者の個人情報を収集することができるため、使用者がこのような装置を利用する前に、CNIL に届け出る必要があると決定した。Délibération 94-113 du 20 décembre 1994 portant adoption d'une norme simplifiée concernant les traitements automatisés d'informations nominatives mis en oeuvre à l'aide d'autocommutateurs téléphoniques sur les lieux de travail.

libertés.以下、CNIL と略称する²⁸⁷⁾ は、監視の実施を個人情報処理の一態様と捉える観点から、職場における監視に関する規制の構成に対して積極的に関与するようになった。このように、フランスにおける監視の適法性に関する判断枠組みを形成する上で、従来の破毀院とコンセイユ・デタに、CNIL が加わることとなった。さらに、近年、ますます高度化する監視装置の利用を規制するために、CNIL の役割はこれまで以上に重要になっている。

以下では、まず、監視に関する法規定を検討し、次に、監視に関する事件を、単純な監視に関するものと、機器を用いた監視に関するものに分け、各判例の意義、学説上の議論及びCNILの見解を分析し、最後に、監視に対する規制の特徴をまとめることとする。

第2節 使用者の監視に関する法規制の制定

第1款 1982年の法改正

前述したように、他の欧州諸国とは異なり、フランスの労働法典（Code du travail）には長い間、使用者の監視を直接規制する規定が設けられていなかった²⁸⁸⁾。しかし、急速な技術発展により、労働者の自由や権利等を保護することへの関心と必要性が高まっていた。その要請に応える目的で、1982年と1992年にそれぞれフランスの労働法典が改正され、その中で新たな技術がもたらす問題（たとえば、採用と業務遂行の監視など）に関する規定が盛り込まれた。以下では、1982年の改正法と1992年の改正法における直接的または間接的に監視を規制する規定を検討する。

1982年改正法は、当時の労働大臣であった Auroux が作成した報告書

²⁸⁷⁾ CNIL を紹介する労働法学上の文献として、砂押・前掲注 107) 166-167 頁、④河野・前掲注 283) 384-391 頁がある。

²⁸⁸⁾ 例えば、ポルトガルの労働法典 20 条（遠隔監視の手段）の第 1 項は「使用者は、従業員の職務遂行を監視する目的で、技術的な機器の使用を含む職場での遠隔監視手段を使用してはならない」と定め、同条第 2 項は「前項の機器の使用は、その目的が人及び財産の保護及び安全であるとき、又は活動の性質に固有の特定の要件によって正当化されるときは、合法的でなければならない」と規定している。また、イタリアの労働者憲章法（Statuto dei Lavoratori）4 条で、使用者が視聴覚設備を利用して遠隔監視する際の目的と手続要件（団体協定、accordo collettivo）を定めている。

(rapport Auroux²⁸⁹) に基づく 4 つの法律²⁹⁰から構成されている²⁹¹。同報告書の中で、Auroux は、「都市の市民である労働者は会社においても市民でなければならない (Citoyens dans la cité, les travailleurs doivent l'être aussi dans leur entreprise)」という理念を掲げている。その目的は、市民社会で個人に認められている権利と自由を、企業で従属関係にある労働者に移植することである²⁹²。同報告では、この目的を達成するためには、4つの柱、すなわち、①従業員の権利の回復と拡大、②労働共同体の再構築、③労働者代表制度の強化、④団体交渉の再生を通じて労働者の自由、尊厳の確保を実現することが必要であると述べられた²⁹³。1982 年改正法の中で、使用者の監視に最も関連しているのは、使用者の就業規則を制定する権限に対する制限である（上記①）。この点について、1982 年改正法は、後述するコンセイユ・デタの Corona 事件判決²⁹⁴の判断を踏襲し、フランスで長年論争となっていた問題、すなわち従業員の身体検査およびアルコール検査に関する就業規則上の規定の適法性を解決するために、使用者が就業規則に定める範囲を制限する規定（現在は、労働法典 1321-3 条 2 項。また、以下では、便宜上、フランスの労働法典をすべて L.と略記する）を新設した²⁹⁵。同条では、就業規則において労働者の自由と権利を制限する規定は、厳格な範囲内（正当性と比例性の審査）でのみ

²⁸⁹ J. Auroux, Les droits des travailleurs, Rapport au Président de la République et au Premier ministre, La Documentation française, 1981, Available at https://medias.vie-publique.fr/data_storage_s3/rapport/pdf/271626.pdf.

²⁹⁰ Loi n°82-689 du 4 août 1982 relative aux libertés des travailleurs dans l'entreprise ; Loi n° 82-915 du 28 octobre 1982 relative au développement des institutions représentatives du personnel ; Loi n° 82-597 du 13 novembre 1982 relative à la négociation collective et au règlement des conflits collectifs du travail ; Loi n° 82-1097 du 23 décembre 1982 relative aux comités d'hygiène, de sécurité et des conditions de travail.

²⁹¹ この法律を紹介した日本の文献として、砂押以久子「労働者のプライバシーの保護について（2）」季労 185 号（1998 年）167 頁以下、佐藤清「フランスにおける労働者権利の拡大」季労 128 号（1983 年）146 頁、保原喜志夫「オール法とフランス労働法の新展開」日本労働協会雑誌 302 号（1984 年）37-49 頁がある。

²⁹² Auroux, *supra* note 289, p.4.

²⁹³ *Ibid.*

²⁹⁴ CE 1 févr. 1980, n°06361.この事件は就業規則上の労働者に対するアルコール検査の適法性をめぐって争われたものである。

²⁹⁵ L.1321-3 条 2 項は、「個人の権利または個人的・集団的自由に対する、遂行されるべき職務の性質によって正当化されず、追求される目的に比例しない制限を就業規則に規定してはならない」と規定している。

許されるとされている²⁹⁶。このように、この規定は、使用者の就業規則の制定権における労働者の自由と権利を最低限度保障する「自由の憲章」として理解されている²⁹⁷。しかし、この規定は使用者の就業規則の制定権のみを対象としているため、新たな技術がもたらす人格権・個人の自由への脅威に十分に対処できていないとの懸念があると指摘された²⁹⁸。

また、使用者の就業規則の制定権を制限する規定に加え、1982年法改正により、従業員代表機関の権限を強化するため、L.2312-8 条も新設された。同条は、雇用、職能、賃金、職業訓練または労働条件に影響を及ぼす可能性のある新技術を導入する前に、企業委員会（Comité d'entreprise, 以下、CE という）に通知し、諮問することを使用者に義務づけている。この CE に対する通知と諮問の使用上の義務は、次款で検討する 1992 年改正法によってさらに拡大された。

最後に、労働者の自由と権利を保護するために最初に制定された 1982 年改正法の意義²⁹⁹が大きい。同改正には監視技術に関する直接的な規制は盛り込まれていないとの重大な問題があることも指摘された³⁰⁰。この問題を克服するため、労働法典は 1982 年の法改正から 10 年後の 1992 年に「雇用・パートタイム労働及び失業保険に関する法」と題した法改正が再び行われた³⁰¹。

第 2 款 1992 年の法改正

1992 年の改正法は、労働者及び求職者の個人情報と私生活を保護するという点において、1982 年の法改正の範囲を超え、さらなる大きな一歩を踏み出した³⁰²。1992 年の改正法では、上記の 1982 年の改正法には含まれていない監視を制限するための実体的・手続的規定が新設された。1992 年の改正法は、パ

²⁹⁶ PH. WAQUET, Le pouvoir de direction et les libertés des salariés, *Dr. soc.* 2000, p.1055.

²⁹⁷ 砂押・前掲注 20) 329 頁。

²⁹⁸ 砂押・前掲注 291) 170 頁。

²⁹⁹ 一部の論者は同法の意義について、「全体主義としての企業から、政治的・法的主体としての企業への移行を示すもの」と評している。A. JEAMMAUD & A. LYON-CAEN, *Droit et direction du personnel*, *Dr. soc.* 1982, p.67-68.

³⁰⁰ 砂押・前掲注 291) 170 頁。

³⁰¹ Loi n°92-1446 du 31 décembre 1992 relative à l'emploi, au développement du travail à temps partiel et à l'assurance chômage.

³⁰² O. DE TISSOT, La protection de la vie privée du salarié, *Dr. soc.* 1995, p.230.

リ第 1 大学名誉教授 G. Lyon-Caen が労働大臣の委託を受け、執筆した公的自由と雇用と題する報告書 (*Libertés publiques et l'emploi*) に基づいて行われたものである。同報告書は、採用 (*Recrutement*) に関する部分と労働のコントロール (*Contrôle du travail*) に関する部分に分かれている。採用の部分についてはすでに学説に詳しく紹介されているため、以下では主に後者に焦点を当てて紹介する³⁰³。

Lyon-Caen は、まずテクノロジーが急速に発展しており、従来の生身の上司による監視が高度なセンサーに代替され、このような質的にも量的にも進化している新たな監視方法が、労働者の自由や通信の秘密などにもたらす制限という問題に焦点を当てている³⁰⁴。具体例として、職場におけるバッジ (ID バッジ) の利用により、従業員代表が職場のドアを通過するたびに記録され、そのため、たとえ従業員代表が自由に職場内で移動できたとしても、匿名で移動することが不可能になっているなどの例が挙げられる³⁰⁵。また、個人情報保護との観点から、職場に導入される様々な監視装置に関して、CNIL の勧告や命令が不十分であると指摘した³⁰⁶。例えば、使用者が業務用の電話を監視する場合について、CNIL は監視の目的が仕事の質を保障するためであり、かつその目的が事前に従業員に通知されている限り、このような監視は許されるという意見を示しているが、労働者の私生活を保護するという観点からは、CNIL の上記見解には疑問があると指摘された³⁰⁷。最後に、立法への勧告に関して、集团的側面においては、前述の 1982 年改正法によって新設された使用者の CE への通知と諮問に関する義務だけでなく、労働条件に影響を及ぼしうる新しい情報処理の装置の導入に関する規定を、労働組合の年次交渉義務に加えるべきであると提案し、一方で個別的側面においては、新たな技術によって労働が「非人間性化 (*Déshumanisation*)」されつつあることから、フランスの個人情報保護法である情報と自由法 (*Loi informatique et libertés*, 以

³⁰³ ⑤河野・前掲注 283) 777-782 頁。

³⁰⁴ G. Lyon-Caen, *Les libertés publiques et l'emploi*, Paris, La documentation française, 1991.n°154, p.143.

³⁰⁵ *Ibid.*

³⁰⁶ *Id.* p.144.

³⁰⁷ *Ibid.*

下、情報と自由法という³⁰⁸⁾の理念に照らし、①労働者個人のアイデンティティを侵害しないこと、②コンピュータによる情報処理のみに基づく決定を行わないこと、③個人に不利な結果をもたらす情報処理の「予測」に異議を唱える権利を、業務遂行に適用される規制を作成するための基礎となるという内容を導入すべきであると提案した³⁰⁹⁾。これらの提案は、その一部のみが1992改正法において盛り込まれた。

1992年の改正法は、前述の1982年の法改正で新設された使用者の就業規則の制定権を制限する規定(L.1321-3条2項)をさらに拡大し、L.1121-1条というあらゆる状況に適用できる比例性審査の規定を新設した。同条は、「いかなる者も、個人の権利並びに個人・集団の自由に対して、遂行すべき職務の性質によって正当化されることなく、求められる目的に比例しない制限をもたらすことはできない」と規定している。学説によれば、この規定では、正当性と比例性の審査はもはや就業規則に限定されず、さらに「いかなる者」という表現が使用されていることから、労働者に制限を加える主体は使用者だけでなく、労働組合や従業員代表も含まれると解釈されている³¹⁰⁾。

また、1992年改正法のもう一つの重要な改正は、使用者が収集できる情報の内容を制限し、情報収集の装置を利用する前に、労働者個人と従業員代表に通知する義務を使用者に課すことである。学説では、使用者が労働者に直接的に情報を提供すること義務を直接的情報提供義務、使用者がCEに情報を提供する義務を間接的情報提供義務と分けている³¹¹⁾。まず、直接的情報義務に関しては、新設されたL.1222-2条は、「いかなる形態であれ、労働者に要求できる情報は、その労働者の職業上の能力を評価するためのものに限られる(第1項)。これらの情報は、本人の適性評価と直接的かつ必要な関連性を有

³⁰⁸⁾ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.同法は1978年に制定され、2004年にCNILの権限強化を含めた法改正が行われ、2018年にGDPRに対応する大幅に改正された。同法の変遷を紹介したものについては、カロリース・ルブルトン「フランスにおける個人情報の保護制度の変遷」法政大学大学院紀要79巻(2017年)179頁参照。また、GDPR施行以後の同法の改正については、同「(研究ノートフランスにおける個人情報の制裁制度と近年のCNILのコントロール活動についての考察)」EU法研究第11号(2022年)156頁以下参照。

³⁰⁹⁾ Lyon-Caen, *supra* note 304, p.150.

³¹⁰⁾ 本条を詳細に紹介したものについては、④河野・前掲注283)772-773頁参照。

³¹¹⁾ B.Bossu, *Nouvelles technologies et surveillance du salarié*, *R.J.S* 8/9, 2001, p. 663.

さなければならない（第2項）」と定めている³¹²。次に、L.1222-3条は、「労働者は、自分に関して実施される業務の評価方法および技術について、その実施に先立って明示的に通知される必要がある（第1項）。……労働者を評価するために使用される方法と技術は、追求される目的に適切でなければならない（第3項）」と規定している。この規定の第1項は透明性原則（Principe de transparence）に基づき、第3項は直接関連原則（Principe de pertinence）に基づいて制定されたものである³¹³。最後に、L.1222-4は、「従業員に事前に知らされていない従業員個人に関する情報は、装置によって収集してはならない」と定めている。この規定は後述する Néocel 事件判決³¹⁴の判旨を踏襲し、誠実さの原則（Principe de loyauté）に基づいて制定されたものである³¹⁵。なお、L.1222-4条の規制対象は、従来の使用者による直接的監視ではなく、むしろ個人データの取得を通じた技術的な監視装置を規制するものであり、また労働者の業務遂行の状況を対象としない監視装置は同条に含まないことに留意しなければならない³¹⁶。

一方、間接的情報提供に関しては、1992年の改正法では、1982年改正法において導入されたCEの情報と諮問を受ける権限がさらに強化された³¹⁷。まず、使用者は、従業員の募集や人事管理を補助する自動処理システムを導入またはあらゆる変更（Toute modification）する際に、CEに通知しなければならない（L.2312-38条1項と2項）。次に、使用者は、従業員の業務遂行の状況

³¹² この規定は、破毀院判決の司祭判決（Cass. soc., 17 oct. 1973, n°72-40.360.）によってすでに確立された判例法理を明文化したものである。同事件では、Y社にフライス工として雇用されていた原告労働者が、採用選考の際にかつて司祭（Prêtre）として勤務していた事実を秘匿したことを理由に解雇されたことについて争われた。破毀院は、「Y社の就業規則や労働協約等に照らして、使用者は人種的身分や労働組合、政治・哲学・宗教団体の会員であることを考慮しない義務を負う」とし、「Xは自分の業務上の能力について被告会社に十分に説明し、原告労働者の仕事ぶりについてもいかなる苦情も出されていないため、原告労働者は神父であったことを明らかにしない権利がある」とした。「採用時に要求される情報や書類の目的は、使用者が従業員の応募業務に関する適格性を評価することであり、そのため応募された業務と直接的かつ必要な関連性のないものに関連付けることはできない」と結論づけた。この判決の紹介について、⑤河野・前掲注283）774頁参照。

³¹³ 砂押・前掲注107）173頁。

³¹⁴ Cass. soc., 20 nov. 1991, n°88-43.120.

³¹⁵ J. DUPLAT, Loyauté et fichiers personnels, SCL n°1218, 2005, p.10.

³¹⁶ J. DUPLAT, Surveillance des salariés et vie privée, RJS 2/03, p.105. A. BAREGE & B. BOSSU, Informatique et libertés - Les TIC et le contrôle de l'activité du salarié -, JCP S n° 41, 2013, p.1393(§9).

³¹⁷ 盛・前掲注20）242頁。

を監視するための装置を導入する前に、CE に通知し、諮問しなければならない（L.2312-38 条 3 項）³¹⁸。ここで留意しなければならないのは、上記規定の第 1 項と第 2 項では、使用者は CE に「通知」するだけで足りるとされているのに対し、同条の第 3 項では、CE に通知するだけでは足りず、使用者は「諮問（Consulté）」を行う必要があると規定されている。また、上記規定の第 3 項は、従業員の活動を監視することを唯一の目的とする装置にとどまらず、このような監視を実施する可能性のあるすべての装置を対象としている³¹⁹³²⁰。

第 3 款 1992 年改正法に関する学説上の議論

学説では、監視を含む情報収集に実体的・手続的な規制を加えた前述の

³¹⁸ なお、2017 年 9 月 22 日付のオルドナンス（いわゆる、マクロン・オルドナンス、Ordonnance n° 2017-1386 du 22 sept. 2017 relative à la nouvelle organisation du dialogue social et économique dans l'entreprise et favorisant l'exercice et la valorisation des responsabilités syndicales）の発効により、CE は従業員代表委員（Délégué du personnel, 以下、DP という）労働衛生安全条件委員会（Comité d'hygiène, de sécurité et des conditions de travail, 以下、CHSCT という）とともに、新たな社会経済委員会（comité social et économique, CSE）によって統合されることとなった。企業は上記オルドナンスに従い、遅くとも 2020 年 1 月 1 日まで統合を完成しなければならない。また、CSE を設置する条件は、従来の DP を設置する条件と同様である。すなわち、従業員 11 人以上を雇用する企業は CSE を設置しなければならず（L.2311-2 条）、さらに CSE は統合前の組織と同じ権限を有する。このように、統合前に従業員 50 人以下（11 人～49 人）の企業には、DP と CHSCT（労働監督官の命令のもとで）の設置のみが義務づけられていたため、統合後の CSE は DP の権限と CHSCT の大部分の権限を承継することになる。一方、統合前に従業員 50 人以上の企業には、DP と CHSCT に加えて CE の設置も義務づけられていたため、統合後の CSE は 3 つの組織の権限を引き継ぐこととなる。したがって、使用者が従業員の活動を監視する場合、事前に CE に通知・諮問することを義務付ける前述の L.2312-38 条は、従業員 50 人以上の企業内における CSE のみを対象としている。マクロン・オルドナンスと CSE の権限等を詳しく紹介する文献として、野田進『フランス労働法概説』（信山社、2022 年）387 頁以下参照。

³¹⁹ J-E RAY, Comité d'entreprise, transparence et dissuasion, *Dr. soc.* 1993, p.218.

³²⁰ 以上の CE に対する通知と諮問の規定に加え、使用者が実施する監視が、労働者の自由と権利を不当に制限する場合、1992 年の改正法は労働者の自由と権利を保護するために、従業員代表委員（Délégué du personnel, DP）に警告権（L.2312-59）を行使する権利も与えた。本論文の主題との関連性が低いため、ここでは割愛する。フランス法における警告権を紹介した文献として、盛・前掲注 107）218-219 頁、河野・前掲注 283）284-285 頁がある。また、警告権は、当初 DP にしか付与されていなかったが、2017 年 9 月 22 日付のオルドナンスの発効に伴い、現在では、11 人以上の従業員を雇用している企業における CSE の委員は警告権を行使できる（警告権の行使について、11 人～49 人の CSE は、L.2312-5 条 3 項、50 人以上の CSE は L.2312-59 条）。

1992年の改正法について、多くの議論がなされている。まず、上記 L.2312-38 条 3 項は、労働者の業務遂行の状況を監視する装置の導入に関して、いくつかの疑問が呈された。まず、同条項は 1992 年改正法の予備草案において「CE は従業員の『行動 (Comportement)』もしくは業務遂行の状況 (Activité des salariés) を監視する手段や手段について諮問を受けなければならない」と規定していたが、現行法では、草案にあった上記の「行動」という用語が削除されたため、労働者が勤務時間外に企業内の社員食堂やカフェテリアなどの場所を移動することは、上記の「労働者の業務遂行の状況」に該当しないため、使用者がこれらの場所に設置・利用される監視装置について CE に通知・諮問する義務があるかどうかは不明である³²¹。この点について、同条の目的が職場で利用される監視の透明性を最大限に高めるという観点から、勤務時間外の従業員の行為も CE による諮問の対象として捉えられるべきであるとする見解がある³²²。また、L.2312-38 条に関するもう一つの問題は、従業員の活動に対する監視を定める第 3 項が、第 1 項と第 2 項とは異なり、講じられた技術を変更する場合、CE に通知する義務が定められていないことである。しかし、技術が急速に発展している今日においては、使用者がかつて CE に通知した監視装置が、より一層洗練された技術に置き換わった場合、その変更に関する通知の義務を使用者に課さないことは適切ではないとする見解がある³²³。

一方、前述した直接的情報提供にする規定の問題点に関しては、例えば、上記 L.1222-2 条にいう「直接的かつ必要な関連性」と、L.1222-3 条にいう「適切」はあまりにも抽象的であり、政府によって発行された通達 (Circulaire) においても一部の例しか挙げられておらず、具体的には何を指すかが不明であり、さらに L.1222-4 条の制定は、判例法理を成文化した点に重要な意義があるが、既存の判例法理が要求している要件とよりもかなり緩和していると指摘された³²⁴。すなわち、監視に関する従来の判例法理³²⁵では、使用者が合法的に従業員を撮影し記録する場合、①使用者が監視を行う前に従業員に通知をしなければならず、②例外的状況 (機械の盗難など) でしか監視を実施できない、とされているが、今回の法改正 (L.1222-4 条) は①のみを盛り込

³²¹ RAY, *supra* note 319, p.218.

³²² *Ibid.*

³²³ *Ibid.*

³²⁴ TISSOT, *supra* note 302, p.225.

³²⁵ CE 11 Juill. 1990, n°86022, Cass. crim., 23 juill. 1992, n° 92-82.721.

み、後者を無視した点に問題があるということである³²⁶。しかし、この批判的な意見を述べた Tissot が指している上記の「判例法理」は、テクノロジーを用いた機械ではなく、所持品検査の問題に関する判決であることから、そもそも所持品検査の判例法理が事前通知なしの監視カメラによる監視が問題となった後述する破毀院の Néocel 判決の判断によって明文化された L.1222-4 条の適用範囲を包含しているかどうかには疑問があるように思われる。加えて、1992 年改正法によって導入された情報収集の制限に関する諸規定に違反する効果について法律で何も規定されていない点にも問題があると指摘された³²⁷。この点に関して、次節で検討するように、今日のフランスにおける違法な監視に対する法的制裁は、違法な監視によって得られた懲戒処分や解雇に用いる証拠を訴訟から排除するという破毀院の判例法理と、CNIL が情報と自由法上の規定に基づき違法な監視に制裁を加えることである。

第 4 款 小括

前述したように、長い間、フランスの労働法典には使用者の監視に関する法規定はなく、監視の利用に実質的な制限を加えたのは、破毀院とコンセイユ・デタの判例法理であった。しかし、急速な技術発展がもたらす労働者の自由と権利の侵害に対処するため、フランスは 1982 年と 1992 年にそれぞれ、直接的または間接的に、監視を制限する手続的、実体的規制を労働法典に導入した。そのなかで、使用者が監視装置を利用する前に労働者に通知することを義務づけている一連の規定は、ほとんどが破毀院の判例法理を成文化したものにすぎないため、従来の状況と大きな差異はない。他方、集団的なレベルでは、上記改正法では、監視に関して従来なかった新たな制限、すなわち、労働者の業務遂行の状況を監視するために導入する装置について、使用者が CE に事前に通知し、諮問する義務が新設された。また、同様に、判例法理に基づいて明文化された比例性の審査に関する規定は、監視の利用による侵害の場合だけでなく、労働者の自由と権利に対するあらゆる侵害の審査にも適用される。この規定は労働者の自由と権利を保護するための憲章とも理解されている。

しかし、前述のように、1982 年と 1992 年の法改正にもいくつかの欠点があ

³²⁶ TISSOT, *supra* note 302, p.225.

³²⁷ 砂押・前掲注 107) 173 頁。

る。そのなかで最も問題視されたのは、新設された上記の規定に違反する場合の法的制裁が設けられていないことである。この点に関して、次節では、今日のフランスにおける違法な監視に対する法的制裁は、違法な監視によって得られた懲戒処分や解雇に用いる証拠を訴訟から排除するという破毀院の判例法理と、CNIL が情報と自由法上の規定に基づき違法な監視に制裁を加えることについて検討する。

第3節 監視に関する破毀院の立場と学説上の議論

第1款 序説

使用者が労働者の業務遂行を監視する権利は、就業規則またはその他のものにおいて定められているか否かにかかわらず、一般的に、労働契約の締結に伴って生じた使用者の指揮命令権に基づくものであると考えられている³²⁸。破毀院は多くの事件において、監視が陰険（Insidieux）や密か（Clandestin）な手段³²⁹によって行われるものではない限り、使用者は労働時間中の従業員の行動を管理・監視する権利を有することを承認している³³⁰。また、監視の適法性要件に関して、監視の手段と形態によって適用される具体的な要件が多少異なるものの、破毀院が求めている要件は基本的に共通している。この観点から、フランスにおける監視の規制には、判例法理の発展に断絶がある日本では見られない連続性がある。また、監視の利用は、その性質上労働者

³²⁸ 河野・前掲注 284) 259 頁。M-P FENOLL TROUSSEAU, *Vie privée du salarié : les nouveaux enjeux de la cybersurveillance*, *JCP E* n°27-28, 2007, p.1878, §1.

³²⁹ *See* PH. WAQUET ET AL., *POUVOIRS DU CHEF D'ENTREPRISE ET LIBERTES DU SALARIE*, 1^{re} éd., 2022, pp.239-240. 例えば、使用者 Y が、従業員 X の配偶者が経営するレストランでの勤務時間中の兼業活動を調査する目的で、顧客になりすまして従業員である X を密かに撮影した事案において、破毀院は、「使用者は、勤務時間中の従業員の活動を管理・監視する権限を有するとしても、密かに不当な監視システムを実施することはできない。Y が X の配偶者が経営するレストランで単なる顧客のふりをして監視をしたことは、策略（Stratagème）をもって密かで不正な方法で行われたものであるとした（Cass. soc., 18 mars 2008, n°06-45.093）。また、被告郵便会社が、一部の従業員が手紙の中身を盗んでいると疑い、手紙を開封した従業員にインクで特殊な文字をマーキングして犯人を特定する装置を使用した事件において、破毀院は、「たとえ使用者は勤務時間中の従業員の活動を管理・監視する権限を有しているとしても、秘密裏（Clandestin）に不誠実（Déloyal）な監視装置を使用してはならない。従業員の知らないところで仕掛けられた措置によって得られた証拠は、違法な策略（Stratagème）に該当する」とした（Cass. soc., 4 juil. 2012, n°11-30.266）。

³³⁰ Cass. soc., 15 mai 2001, n° 99-42.219.

の自由と権利に制限をもたらすものであることから、誠実さの原則、比例性審査（L.1121-1条）および私生活保護尊重請求権（民法典9条）に基づき、破毀院は使用者に対し、それぞれ、監視を誠実に実施する義務、監視に関する公正な手続を遵守する義務、監視が労働者の私生活を侵害してはならない義務を課している³³¹。使用者が上記いずれかの義務に違反した場合、後述する1991年のNéocel事件判決³³²で確立された違法な証拠を訴訟から排除する法理が適用される。最後に、フランスの監視の規制に関するもう一つの特徴は、個人情報保護に精通するCNILの役割である。CNILが新たな監視技術に対応するため、積極的に命令を下したり、勧告を発したりする一方、破毀院はCNILの勧告と命令を積極的に判例に組み入れることで、CNILの意見等を「司法化」し、その過程で、既存の判例法理を拡大・充実させてきた。このように、フランスの監視の規制は、破毀院とCNILによって構築されている。以上を踏まえ、以下では、監視に関する破毀院の判決およびそれに関連する学説上の議論。CNILの命令と勧告を検討する。

第2款 単純な監視に関する事件

（1）従業員個人用のロッカーの検査

使用者が従業員に割り当てたロッカーの状態と内容の検査に関する問題について最初に判決が下された1987年6月12日のGantois事件において、衣服や私物を保管する従業員の更衣室内にあるロッカーについて、使用者は、その状態や内容を確認するために……いつでも開放する権利を留保する、という被告Y社の就業規則の規定に関して、コンセイユ・デタは、「R. 232-24条6項³³³に照らして、（上記Yの就業規則上の規定は）関係従業員への事前通知を定めていないため、使用者が企業の安全を確保するために使用者が合法的に個人の権利と自由を制限できる範囲を超えるものである」とした³³⁴。次に、Gantois事件とほぼ同じ事実を有する事案において、コンセイユ・デタは、

³³¹ F. FAVENNEC-HERY, *Vie professionnel, vie personnelle du salarié et droit probatoire*, Dr. Soc. 2004, p.52.

³³² See case *supra* note 314.

³³³ R. 232-24条6項は、「個人のロッカーには鍵または南京錠が取り付けられていなければならない。個人用のロッカーは、就業規則に定められた条件に従って清掃されなければならない」と規定したが、1987年のデグレ³³³によって廃止された。同条の内容を引き継いだ現行法のR.4228-6条4項は、「個人のロッカーには鍵または南京錠が取り付けられていなければならない」のみを規定している。

³³⁴ CE 12 juin 1987, n° 72388.

「R.232-24 条 6 項に照らして、使用者は、衛生上または安全上の必要性がある場合にのみ、従業員の個人用ロッカーの状態や中身を検査することができる。加えて、上記検査は、例外的な場合を除き、関係従業員の立会いのもとで実施されなければならない」と判示した³³⁵。

一方、破毀院の立場に関して、使用者が従業員個人のロッカーを検査した際、原告労働者のロッカーにビールがあったことを発見し、それを理由として当該従業員を解雇したことについて争われた有名な *Ratajczak* 事件において、破毀院は、上記の 1992 年法改正で新設された L.1121-1 条（比例性審査）を引用した上で、「使用者が従業員個人用ロッカーを開錠できるのは、就業規則に当該検査の実施条件が定められており、関係従業員が検査に立会う場合、または当該従業員が事前に通知された場合に限られる。本件検査は原告労働者が立ち会うことなく行われ、しかも『特別なリスクや出来事 (*Risque ou événement particulier*)』によって正当化されるものでもなかった」とした³³⁶。*Ratajczak* 事件判決が示した所持品検査の適法性要件（通知要件と必要性の要件）は、その後の類似の事件において踏襲されている³³⁷。これに対して、原告従業員 X が、被告 Y 社の許可を受けていない私物を所有者不明の個人ロッカーに置いたことを理由に解雇されたことが争われた 2008 年 5 月 15 日の事件において、破毀院は、「X を含めた Y の従業員は、3 週間前に、所有者不明のロッカーを開錠する日付について各労働者のロッカーに掲示することで個人的に通知され、さらに開けられるロッカーは期間内に特定されなかったものに限定した。本件ロッカーの開錠は、労働組合の代表者と合意した一定の手続に従い、かつ従業員代表と警備員の立ち会いの下で行われた」とし、X が Y の就業規則に許可されていない物品を所有者不明のロッカーに置いたことが、解雇の真正かつ重大な理由に当たるとしたドゥーエ控訴院の判断を是認した³³⁸。このほか、もっぱら業務のために従業員に割り当てられた手提げ金庫の中身に対して行われた検査の結果に基づく懲戒処分の効力をめぐって争われた事件において、破毀院は、上記手提げ金庫はもっぱら「業務のために」

³³⁵ CE 9 oct. 1987, n°72220.

³³⁶ Cass, soc., 11 déc. 2001, n°99-43.030.

³³⁷ 学説上、*Ratajczak* 事件判決が求めた通知要件は、警察が家宅捜索を行う際には対象者その場で立ち合う必要があるというフランスの刑事訴訟法の原則に由来するものであると指摘された。PH. WAQUET ET AL., *supra* note 329, pp.241-242.

³³⁸ Cass. soc., 15 avr. 2008, n°06-45.902.

使用されるものであることから、使用者はこの金庫を就業規則に基づいて検査することができると判示した³³⁹。

以上の従業員個人用のロッカー内の状態及び内容に対する検査の適法性をめぐって争われた諸判決から明らかなように、コンセイユ・デタも破毀院も、R.4228-6 条 4 項上の規定に加え、使用者が検査を行う前に、従業員に通知しなければならない、さらに検査実施中は例外的な場合を除き、関係従業員の立ち会いのもとで検査を実施しなければならないとしている。また、破毀院は L.1121-1 条の比例性審査に基づいてロッカー検査の適法性を判断しているのに対し、コンセイユ・デタは、従業員の自由と権利を保護する目的に照らして、ロッカー検査の目的を厳格に「安全衛生上の必要性の確保」に限定している。両者の立場を比較すると、ロッカー検査の目的そのものを制限するコンセイユ・デタの立場は、比例性審査をケースバイケースで審査する破毀院の立場よりも、明確性が高いように見える。また、ロッカーの検査が適法と判断された事件について、破毀院は、検査対象の金庫が従業員の私的使用のために割り当てられているものではなく、専ら業務使用のために従業員に貸与されている場合、従業員への事前通知や検査時の関係従業員の立会いは不要であるとした。これは、破毀院が業務用のものと従業員個人用のものを厳格に区別したからである。前者の場合、使用者は原則として自由に検査の対象の中身を調査することができる。

(2) 所持品検査

所持品検査の問題に関して、1988 年 7 月 8 日の判決において、コンセイユ・デタは、「貴金属の冶金と化学を業とする被告会社に、盗難防止の必要性から、従業員のバックや持ち物などに対する検査を正当化することはできず、したがって当該従業員がこのような検査を拒否できる権利と、所持品の検査時に従業員が証人の立ち会いを求める権利を就業規則に明記すべきである」とし、被告会社の就業規則には上記の内容が含まれていないため、労働監督官の被告会社に対する就業規則を修正する命令を是認した³⁴⁰。この事件に類似している 1990 年 11 月 26 日の事件において、コンセイユ・デタは、「所持品検査が個人の権利と自由を制限することを考慮すると、使用者は、就業規則が以下の要件を満たす場合に限り、合法的に従業員の所持品を検査することができ

³³⁹ Cass. soc., 21 oct. 2008, n°07-41.513.

³⁴⁰ CE 8 juill. 1988, n°71484.

る。まず、当該検査は、機器の紛失時や社内で盗難の危険性が特に高い場合にのみ実施されること、次に、従業員には検査の結果に異議を唱え、証人の立会いを求める権利があること、最後に、当該検査は個人の尊厳と私生活上の親密性を保護する条件で実施されなければならないことである」と判示した³⁴¹。本判決で示された 3 つの要件は、本判決以降のコンセイユ・デタの判例法理において確立されている³⁴²。

一方、破毀院の判例法理においても、所持品検査に関する事件も多く蓄積されているが、そのなかで、最も重要な判決として考えられているのは、2001 年の Sarrasin 事件である。この事件では、破毀院は使用者が合法的に所持品を検査できる例外事由を明確に判断した点に特徴がある。この事件では、爆破事件と様々な爆破予告を受けた後、被告会社 Y は警備員が入り口で従業員のカバンを検査することについてメモで従業員に通知した。組合代表であった原告従業員 X は、所持品検査を拒否し、強引に被告会社に入ったとして、出勤禁止の処分を受けた。破毀院は、「1995 年夏に一連の爆弾があったことを考慮し、爆弾の警告を受けた Y が、CE と CHSCT に諮問した後、従業員が警備員の前でカバンを開けることを一時的に要求したことは、例外的な状況 (Circonstances exceptionnelles) 及び安全確保の必要性によって正当化され、さらにその方法は本人に鞆を開けさせるのみであって、その中身までは調査するものではないため、本件調査は Y によって追求された目的に比例している」とし、X が上記検査を拒否したことにフォートがあったというパリ控訴院の判断を是認した³⁴³。

また、所持品検査を違法とした事件として、被告 Y 社に包装員として雇用された原告従業員 X が、所持品検査において Y 社の化粧品を無断で持ち出したことが発覚したことを理由に解雇されたことが争われた事件がある。この事件において、破毀院は、Y 社が行った上記の所持品検査は、従業員がカバンの検査に異議を唱える権利や証人の立ち会いを求める権利を知らされていたかどうかは不明であり、就業規則を掲示しただけでは、X が上記権利を知らされていたとはいえないとして、Y 社の上告を棄却した³⁴⁴。このほか、上記 2 要件（検査に異議を唱える権利と検査中に証人の立ち会いを求める権利）に

³⁴¹ CE 26 nov. 1990, n°96565.

³⁴² 他に同じ判断を下した判決として、*See case supra* note 325 (CE.)がある。

³⁴³ Cass, soc., 3 avr. 2001, n°98-45.818.

³⁴⁴ Cass. soc., 8 mars 2005, n°02-47.123.

加え、従業員の同意を求めた判決もある。2009年2月11日の事件において、破毀院は、「例外的な状況を除き、使用者が従業員のカバンの中身を検査できるのは、当該検査に対する労働者の同意があり（下線は筆者による）、かつ労働者が、異議を唱える権利と証人の立会いを求める権利を知らされていた場合に限られる。……Xが所持品検査に異議を唱える権利を事前に知らされていたかどうかは明らかではない」とし、本件所持品検査を適法としたドゥオーエー控訴院の判断を破毀した³⁴⁵。

他方、所持品検査の実施を適法とした判決もある。例えば、所持品検査において、原告従業員Xが、被告会社Yの機密書類を持ち出したことが発覚したことを理由に解雇されたことについてその適否が争われた事件がある。この事件において、破毀院は、「XがYに危害を加える意図が確認されたかどうかにもかかわらず、Xの行動が重大な違法行為に該当する」と判示した³⁴⁶。なお、本件では、検査の態様は使用者が従業員のカバンの中身を探ったのではなく、従業員自身が鞆の中身を使用者に提示する程度にとどまったことも考慮された。この点について、上記Sarrasin事件判決も、実施された検査は使用者が直接労働者の鞆を調べるのではなく、従業員自身が鞆の中身を提示したことを強調している。

以上の検討を踏まえ、使用者による所持品検査を正当化する要件として、破毀院もコンセイユ・デタも、当該検査を実施する高度な必要性和例外的な状況を求めており、また、使用者が所持品検査やロッカーの検査を実施する前に、従業員に、異議を唱える権利と証人の立ち合いを求める権利を通知することを要請している³⁴⁷。最後に、所持品検査に関する破毀院の判決では、上記従業員への通知義務に加え、所持品検査の態様、つまり使用者が直接的に所持品の中身を探るか、あるいは従業員自らでその内容を使用者に提示したかについても強調されており、所持品検査の適法性については、破毀院は後者のような場合に、をより緩やかに判断している。

(3) 尾行と調査

³⁴⁵ Cass. soc., 11 févr. 2009, n°07-42.068.

³⁴⁶ Cass. soc., 22 sept. 2009, n°08-41.873.

³⁴⁷ 所持品検査に関しては、コンセイユ・デタは検査の正当性を判断するにあたり、審査基準に「（検査の）必要性（nécessité）のほかに手続の尊重（respect d'une procédure）」を含めているという指摘がある。砂押・前掲注107）170頁。

フランスでは、使用者による尾行と調査は、外回りの多い業務に従事する労働者の労働時間を把握するために、社内従業員または社外機関の私立探偵を依頼して実施される場合が多い。この種の監視は、ロッカーと所持品に対する検査よりも不透明であり、実施の場所次第では、労働者の私生活を著しく侵害する場合がある。破毀院の判例法理には、使用者が行う尾行と調査に起因する紛争が多く存在し、すべての事件を網羅的に取り上げることは困難であるため、以下では尾行と調査に関する重要な判決のみを取り上げて検討する。

まず、尾行の問題について破毀院が初めて正面から判断を下した 1995 年 5 月 22 日の事件では、使用者 Y が私立探偵に依頼し、外回りの業務を担当した原告従業員 X を尾行させ、その探偵が作成した報告書を理由に X を解雇した。この事件において、破毀院は、「たとえ使用者が勤務時間中に従業員の活動を管理・監視する権利を有するとしても、従業員に事前に通知されない手段を用いることはできない」とし、事前に X に通知しなかった、X を尾行した結果に基づいて作成された報告書を違法な証拠方法としたナンシー控訴院の判断を是認した³⁴⁸。私立探偵による尾行をめぐるその後の判決は、上記判決の判断を踏襲していることに加え、上記判決では明示されていない法的根拠について、民事訴訟法第 9 条がその根拠となることを明確にした³⁴⁹。また、2001 年 5 月 15 日の事件で、破毀院は、職場にあるサンドイッチと飲み物を提供する自動販売機を破壊した犯人を特定する目的で、使用者が、従業員や CE に事前に通知することなく外部機関に調査を委託した場合、その機関が作成した報告書は違法な証拠となるとした³⁵⁰。この事件では、破毀院の法的根拠は、民法典 9 条（私生活尊重請求権）ではなく、上記 1992 年法改正で新設された、L.2312-38（CE に対する事前の通知と諮問の義務、第 3 章第 2 節 2 款）である。

次に、労働者の私生活保護に正面から抵触した尾行の問題として、Montaigu

³⁴⁸ Cass. soc., 22 mai 1995, n°93-44.078.

³⁴⁹ Cass. soc., 4 févr. 1998, n°95-43.421, Cass. Soc., 23 nov. 2005, n°03-41.401.

³⁵⁰ See case *supra* note 330.破毀院は、「たとえ使用者が労働時間中の従業員の活動をコントロール、監視する権利を有する場合でも、L.432-2-1 条（現、L.2312-38 条）により、使用者は事前に従業員や従業員代表に通知していない監視装置を利用することができない」とし、被告企業が従業員の知らないうちに社外企業に依頼し、従業員が利用する飲料・サンドイッチ販売機の使用を監視したことに基づいて作成された報告書を違法とした控訴院の判断を是認した。

事件では、Y 社が、医薬情報担当者として主に外回りの業務に従事していた原告従業員 X が、労働時間や経費について虚偽申告を行ったことを証明するために、X の上司を X の自宅付近まで尾行させ、調査結果に基づいて作成された報告書を理由に、重大なフォートとして X を解雇したことについて争われた。破毀院は、ECHR8 条、民法典第 9 条³⁵¹、民事訴訟法第 9 条及び L.1121-1 に鑑みれば、「従業員の活動を管理・監視するために使用者が行う尾行は、必然的に従業員の私生活に対する侵害をもたらすものであり、その不釣り合いな性質からして、本件尾行は使用者の正当な利益によって正当化できず、違法な証拠方法を構成する」とし、本件尾行の結果に基づいて作成された報告書は違法であり、訴訟から排除すべきであると判示した³⁵²。学説では、本件と前述の尾行事件（1995 年 5 月 22 日）との間にいくつかの違いがあると指摘された³⁵³。まず、本件では尾行を実施した主体は X の上司であり、外部の私立探偵を依頼する場合よりも、本件調査の客観性に疑問があり、次に、本件の尾行は X の自宅付近まで行われたものであるため、通常の監視と比べて、労働者の私生活保護さらには住居の不可侵の問題を侵入する可能性が高い³⁵⁴。また、本判決は、前述の尾行事件（1995 年 5 月 22 日）のように、「従業員に事前に通知されない手段を用いることはできない」という部分に言及しておらず、むしろ本件尾行が労働者の私生活を侵害するという点から、直接的にその証拠を訴訟から排除している点に特徴がある。言い換えれば、本件では、事前通知の要件が求められていない。これに対して、本判決の結論に疑問を呈する見解もある。例えば、本件尾行は上司が労働者の労働時間等を確認する目的で実施されたにとどまり、この尾行は労働者の職業生活と関連するも

³⁵¹ 民法典 9 条は、「各人は、私生活の尊重を受ける権利がある（第 1 項）。裁判官は、損害賠償は別段として、私生活の親密圏に対する侵害を阻害し、または差止めるのに適切な、係争物寄託、差押、及びその他の全ての措置を命じることができる。これらの措置は、緊急の場合、急速審理において命じられる（第 2 項）」と規定している。

³⁵² Cass. soc., 26 nov. 2002, n°00-42.401. 本件に類似している事案として、2006 年 5 月 17 日の事案では、使用者 Y は従業員 X が競業行為を行っていたことを疑い、大審裁判所（日本の民事訴訟第一審に相当するもの）に証拠調査の命令を申請し、大審裁判所はこの申請を許可した。X はこの調査命令の適法性について訴訟を提起した。破毀院は、上記 2002 年の判決を踏襲し、従業員の自宅付近で行われる調査ないし尾行は労働者の私生活を侵害するものに該当し、その報告書は訴訟から排除されるべきであると判断した。See Cass. 2° civ., 17 mars 2016, n°15-11.412.

³⁵³ DUPLAT, *surpa* note 316, p.105.

³⁵⁴ *Ibid.*

のであるため、労働者の私生活を侵害するものには当たらないとする見解³⁵⁵, また、「本件尾行は、使用者の正当な利益によって正当化できず、違法な証拠方法を構成する」とした本判決の判断に照らせば、いかなる尾行と調査が違法となるという結論に至る恐れがあるとする見解もある³⁵⁶。しかし、後者の指摘については疑問があるように思われる。この点、前述の学説でも指摘されているように、本件尾行は、労働者の私生活保護に対する重大な侵害を伴う特殊な性格を有する事案であるため、本件判決の射程はあらゆる尾行には及ばないと解されるべきである。

学説上、次の3つの累積的な条件を満たす調査等に関しては、破毀院は従業員への事前情報の提供を義務づけていないと指摘された³⁵⁷。第1の条件は、調査等は職場内で行われることである。第2の条件は、調査が使用者自身または社内の従業員を利用して行われることである。言い換えれば、社外機関の私立探偵を利用しないこと。第3の条件は、調査等が機器を利用しないで行われること、すなわち、上司が直接の視覚または聴覚による「観察」である³⁵⁸。例えば、職場で上司による機械を使わない監視は事前に従業員に通知する必要がないとした判決³⁵⁹や、使用者が事前に従業員に通知しなかった場合でも、当該調査が上司ではなく企業の内部部門(Service interne)によって実施される場合は適法とした判決がある³⁶⁰。

近時、破毀院は上記のような使用者等による調査と尾行に関する判断枠組みに対し、2021年5月17日の事件で新たな例外を打ち出した³⁶¹。この事件では、前述した使用者が従業員の正確な労働時間を把握するために実施される尾行及び調査とは異なり、使用者 Y が、DP の同意を得て、心理社会的リスク (Risques psycho-sociaux) を専門とする外部機関に、原告従業員 X がモラルハラスメント (人種差別的発言) を行った事実があったか否かの調査を依頼したことが違法であるかどうか争われた。破毀院は、まず、「使用者は、従業

³⁵⁵ J. SAVATIER, Employeur. Pouvoir de direction. Surveillance des salariés. Respect de la vie privée. Caractère illicite d'une preuve par filature, *Dr. soc.* 2003, p.226.

³⁵⁶ FAVENNEC-HERY, *supra* note 331, p.53.

³⁵⁷ D. CORRIGNAN-CARSIN, Surveillance du salarié sur le lieu de travail, *JCP S* n°23, 2006, p.1444.

³⁵⁸ *Ibid.*

³⁵⁹ Cass. soc., 26 avr. 2006, n°04-43.582.

³⁶⁰ Cass. soc., 4 juill. 2012, n°11-14.241.

³⁶¹ Cass. civ., 17 mars 2021, n°18-25.597.

員に事前に通知していない装置を用いて、労働者に関する情報を収集してはならない（L.1222-4 条）。また、使用者は勤務時間中に従業員の活動をコントロール、監視する権限を有するが、不正または秘密裏に監視することはできない」という原則を示した。次に、X が当該調査の実施について事前に知らされていなかったことを理由に、同調査に基づく報告書を訴訟手続から除外した控訴院の判断に対し、破毀院は、「モラルハラスメント行為の告発を受けて企業内で行われる調査は、上記の L.1222-4 条の適用を受けず、従業員の活動を秘密裏に監視するものではなく、不当な証拠方法に該当しない」とし、控訴院の判断を破毀した³⁶²。学説上、上記破毀院の判断は、使用者が調査する前に従業員に事前に通知する必要があるとの原則を放棄するのではなく、あくまでも、本件の特殊性、つまりモラルハラスメントの立証が複雑であることと、フランス法が使用者に対してモラルハラスメントを防止するための厳格な安全配慮義務を課していることとに起因するとの見解がある³⁶³。また、本判決を担当した Grivel 法院検事（Avocat général）は、本件において L.1222-4 条が適用されない理由には2点があると指摘した。第1に、本件調査は L.1222-4 条に規定されている「装置（Dispositif）」を利用したものではないこと、第2に、本件のモラルハラスメントに対する調査は、使用者が安全配慮義務を果たすために行ったものにすぎず、従業員の自由を危うくするようなものでもないという点である³⁶⁴。

（4）小括

以上のように、使用者が従業員個人用のロッカーと所持品検査を合法的に実施するためには、破毀院とコンセイユ・デタが定めた厳格な目的要件と、関係従業員への事前通知と検査時の立ち合いという手続要件を満たさなければならない。まず、検査の目的要件について、コンセイユ・デタがそれを「安全衛生上の必要性の確保」に明確に限定しているのに対して、破毀院は、目的の内容を明示せず、L.1121-1 条の比例性審査を引用したにとどまっている。この点で、コンセイユ・デタの立場は破毀院の立場よりも明確であるといえよう。次に、破毀院とコンセイユ・デタはともに、使用者は上記検査を実施する前に労働者に通知しなければならないか、または検査中に関係労働

³⁶² *Ibid.*

³⁶³ PH. WAQUET ET AL., *supra* note 329, p.43.

³⁶⁴ Grivel 法院検事の意見は、前掲注 329) から引用した。

者を立ち合わせなければならないという見解を示している。もっとも、両者は、特別なリスクや出来事がある場合には、上記の通知要件が免除される可能性がある」と述べた。

一方、尾行と調査の場合においても、破毀院は使用者に上記と同様の通知義務を課している。尾行等が通知要件を満たさない場合は、それによって得られた証拠は訴訟から排除されなければならない。また、職場以外の場所で行われる尾行等は、使用者がその存在を従業員に事前に通知したかどうかにかかわらず、従業員の私生活保護（民法典 9 条）を侵害するものとして違法とされている。最後に、ハラスメントの調査のような例外的な場合において、破毀院はこれまで厳格に要求してきた通知要件を緩和し、例外的にそのような調査を合法とした。これは、使用者による尾行と調査の場合において、通知義務の唯一の例外である。

第 3 款 機器を用いた監視に関する事件

(1) 監視カメラに関する規制

前述した 1992 年改正法において、監視に関する一連の実体的と手続的規定が定められたが、監視に関する具体的な規制は依然として従来の破毀院の判例法理がリードしている。また、この判例法理に加え、監視装置が個人情報を取得するという観点から、監視を実施する使用者は、情報と自由法上の規定を遵守する必要があるとともに、CNIL の監督に服することとなる。監視カメラの適法要件に関して、破毀院は、使用者に対し、従業員の業務遂行の状況を監視するための監視カメラを設置する前に、監視の対象となる従業員と CE に当該監視装置の存在を通知し、さらに CNIL に届出することを義務づけている³⁶⁵。使用者がいずれかの義務を果たさなかった場合、利用された監視カメラによって得られた証拠は訴訟から排除されなければならない（とりわけ、後述する ID バッジに関する事件）。また、GDPR の施行により、使用者が監視カメラの利用について CNIL に届出する義務はなくなったが、使用者の義務は厳格化され、義務に違反した場合の制裁金も引き上げられた。職場における監視カメラの利用が GDPR の規定を満たしていない場合、当該監視カメラによって得られた画像等は違法な証拠方法に該当し、訴訟から排除されなければならないかについて、この点を正面から判断した破毀院判決はまだ

³⁶⁵ 例えば、Cass. soc., 31 janv. 2001, n° 98-44.290, Cass. soc., 7 Juin 2006, n° 04-43.866.

登場していないが、学説では、GDPR に違反した監視装置によって収集されたデータは、従来の通り、訴訟から排除されなければならないと解する見解が多い³⁶⁶。

以下では、監視カメラによる監視、GPS機能つき装置による監視、IDバッジの利用による監視に関するそれぞれの問題を検討する。

(i.) 事前通知義務の確立

破毀院の判例法理において、監視カメラに関する規制が初めて示されたのは、1991 年の有名な Néocel 事件判決である。この事件では、被告 Y 社にレジ係として雇用されていた原告労働者 X が、Y の商品を窃盗したことが重大なフォートであるとして解雇された。この事件で問題となったのは、X の窃盗行為を証明するために、Y が秘密裏に監視カメラを利用して得た証拠をどのように評価すべきかであった。破毀院は、民事訴訟法 9 条³⁶⁷のみに基づき、「使用者が勤務時間中の従業員の行動をコントロール・監視する権利を有するとしても、いかなる理由であれ、従業員の知らないうちに肖像及び会話を記録することは、違法な証拠方法となる」とした³⁶⁸。この判決は、民事訴訟法 9 条に基づき、使用者に対し、監視カメラを利用する前にその存在を従業員に通知する義務を課しており、使用者がその義務を遵守しない場合、同条に基づき、監視装置によって得られた証拠は訴訟から排除されなければならない。このような証拠排除の判例法理は、その後の監視に関する事件においても踏襲されており、最終的に前述した 1992 年の法改正において L.121-8（現 L.1222-4）によって明文化された³⁶⁹。しかし一方で、Néocel 事件判決の上記法理に対する批判的な見解もある。例えば、Néocel 事件判決が使用者の監視

³⁶⁶ E. PESKINE & C. WOLMARK, *Droit du travail*, 14^e éd., 2020, p.240.

³⁶⁷ フランスの民事訴訟法 9 条は、「当事者は、自己の主張が認められるために必要な事実を法的に従って証明する責任を負う」と規定している。

³⁶⁸ See case *supra* note 314.

³⁶⁹ この判例法理（違法な証拠の排除）の根底にある基本理念は、判決理由には明示されていないが、この事件を担当した Waquet 判事は、Néocel 判決は実際には個人の尊厳と誠実さの原則に基づいていると指摘した。See PH. WAQUET, *Un employeur peut-il filmer à leur insu ses salariés ?*, *Dr. soc.* 1992, p.28. また、同様に、この判決の法院検事を担当した Chauvy は、この点について、「使用者は誠実さの義務と公正の義務によって拘束されているため、労働者の道徳と尊厳を尊重し、誠実さの義務等に合致した証拠方法を用いなければならない」と指摘した。See Y. CHAUVY, *Conclusions sous Cass. soc.*, 20 novembre 1991 *Mme Néocel c/ Spaeter*, *D.* 1992, jurisprudence p. 73.

カメラ設置の事前通知の義務にしか言及していないことは、間接的にすべての監視カメラの利用を助長するという逆効果が生じるおそれがあるとの見解がある³⁷⁰。言い換えれば、監視カメラの存在を事前に労働者に通知するだけで、使用者が監視カメラの利用を正当化できるという誤解が生じかねないからである。また、同見解では、いかなる正当な理由であれ、監視カメラの利用は、その性質上、労働者のアイデンティティに脅威をもたらすものであることから、厳格的に解釈されなければならないとされている。具体的には、使用者は、監視カメラを設置・利用する際に、適切性、合目的性、比例性という基本的な要件に加え、情報と自由法によって課されている諸義務を果たさなければならない³⁷¹。

また、Néocel 事件判決に由来する L.1222-4 条は、使用者が監視を実施するために労働者にその存在を通知しなければならないが、同条では通知の具体的な方法について明示されていないため、その解釈は判例法理に委ねるほかならない。この問題に関する 2018 年 11 月 7 日の事件において、被告 Y 社は設置した監視カメラの存在に関する掲示を職場の入り口に貼り付け、さらに監視カメラを実施する前に CE に通知・諮問し、その当該装置の利用について CNIL にも届け出た。破毀院は、「従業員が監視装置によって自分の画像が撮影されることを知らなかったとは考えられず、秘密でも不誠実でもない限り、その後行われた録画を証拠としての使用は違法ではない」と判断した³⁷²。このほか、監視カメラに関する事件ではなく、客室乗務員やパイロットの日々の業務を管理するために導入された監視装置の通知方法が問題となった事件において、破毀院は、個人データの自動処理の存在、その目的、収集されたデータの受領者、およびその作成日以降のアクセス、修正および削除の権利を記載した紙の回覧メモの存在と、パイロット専用のイントラネットに本件装置に関する情報が常時閲覧可能であったことから、上記監視装置はすでに労働者に知らされたと判断した³⁷³。このように、L.1222-4 条に基づき通知義務をどのように履行するかに関して、破毀院は、労働者が知ろうと思えば知りうるような状態のみを要求している。

³⁷⁰ M. GRÉVY, Vidéosurveillance dans l'entreprise: un mode normal de contrôle des salariés?, *Dr. soc.*1995, p.330.

³⁷¹ *Ibid.*

³⁷² Cass. soc., 7 nov. 2018, n°16-26.126.

³⁷³ Cass soc., 13 juin 2018, n°16-25.301.

(ii.) 事前通知義務の例外

監視カメラが関係する事件では、通常、従業員が立ち入ることのできない場所に設置された監視カメラの存在も通知義務の対象となるかどうかはしばしば問題となる。この問題について、破毀院の立場は一貫している。破毀院の立場が最初に示された2001年1月31日の事案において、破毀院は、通常、従業員がアクセスできない倉庫の監視カメラについて、「L.2312-38 条 3 項（前述第3章第2節第2款）に鑑み、使用者は従業員の行動を監視する手段や技術について、企業内で監視を実施する決定前に CE に通知・諮問する必要がある。事前に従業員に通知することない監視装置によって得られた画像は、証拠として使用してはならない」という原則を示し、「しかし、使用者は労働者が働いていない倉庫やその他の収納場所で自由に監視を行うことができる。本件監視カメラは倉庫に設置されたものであり、従業員の業務遂行状況を記録するものではなかったため、それによって得られた録画の証拠方法は認められる」とした³⁷⁴。同じ見解を示した、被告 Y 社の取引企業が倉庫（entrepôt）に設置した監視カメラによって犯罪行為が録画されたことを理由に、Y 社に雇用されていた原告警備員 X が解雇されたことについてその有効性を争った事件において、破毀院は、「上記監視カメラの設置は取引先企業によって決定されたものであり、従業員の業務状況を監視するためのものではなく、従業員が勤務しない倉庫への出入り口を監視するためだけのものであった」とし、本件監視カメラによって得られた画像を合法的証拠方法と判断した³⁷⁵。他方で、従業員の業務遂行の状況を確認する目的で設置された監視カメラの場合、それが取引先企業に設置されているかどうかにかかわらず、使用者が事前に従業員にその存在を通知しない場合、監視カメラによって得られた録画は違法な証拠方法となる³⁷⁶。また、原告従業員 X が顧客の携帯電話を横領した様子が、店舗のセキュリティを確保するために設置された監視カメラによって撮影された事案において、破毀院は、「上記監視カメラは、店舗の安全を確保するために設置されたものであり、従業員の職務遂行を監視するために使用

³⁷⁴ See case *supra* note 365 (31 janv. 2001).

³⁷⁵ Cass. soc., 19 avr. 2005, n° 02-46.295. 同じ判断の事件として、Cass. soc., 19 Janv. 2010 n°08-45.092 がある。この事件は、普段、従業員の出入りが禁止されている工場の屋根に登った原告従業員 X が、事前に従業員と CE に通知しなかった監視カメラに撮影され、その画像を証拠として X に懲戒処分（出勤禁止）を課した有効性が争われたものである。

³⁷⁶ Cass. soc., 10 janv. 2012, n°10-23.482.

されたものではないため、X が、従業員の活動を監視する手段および技術に関する労働法典の規定を援用することはできない」とした³⁷⁷。

近時では、上記事前通知義務の例外を認めた事案とは異なり、事前通知義務それ自体を求めておらず、L.1121-1 条（比例性審査）のみに基づき監視カメラによる監視を違法とする、これまでにはなかった特別な判決が登場した。この事件では、調理師として雇用されていた原告労働者 X の犯行が常時稼働する監視カメラによって撮影され、それによって得られた証拠に基づく解雇の有効性が争われた。破毀院は、L.1121-1 条に照らして、「台所で一人作業をしていた X が、そこに設置された監視カメラによって常時撮影されており、この監視カメラの録画は、従業員の個人生活（Vie personnelle）を侵害し、従業員や財産の安全を確保するという使用者が主張する目的とは比例的ではなく、したがって上記録画は（解雇手続で）従業員に対抗することができない」とした³⁷⁸。本判決には 2 つの特徴がある。第 1 は、破毀院は、労働者を間断なく撮影する監視カメラの利用は、使用者がその存在を事前に労働者に通知義務したかどうかにかかわらず、L.1121-1 に照らしてこのような監視は比例的ではないと明確に判示した点である。第 2 は、使用者は労働者の業務状況を間断なく撮影してはならないという CNIL がかねてより主張してきた見解が、この判決で初めて取り入れられた点である³⁷⁹。フランスの学者は、このような現象を CNIL 見解の司法化と呼んでいる。なお、後述する GPS による監視と ID バッジによる監視に関する判決でも同じ現象がある。

(iii.) 監視カメラの利用目的変更

本来は職場のセキュリティのために設置された監視カメラが、その後、当初の目的から逸脱して従業員の行動を監視するために利用されるようになったという問題はしばしば争われている。この点に関しては、破毀院の立場は一貫している。その嚆矢となったのは、2006 年 6 月 7 日の判決である。この事件において、破毀院は、「使用者は、勤務時間中の従業員の行動を監視する権

³⁷⁷ Cass. soc., 26 juin 2013, n°12-16.564.

³⁷⁸ Cass. soc., 23 juin 2021, n°19-13.856.

³⁷⁹ H. BOUCHET, CNIL la cyber surveillance sur les lieux de travail, 5 fév. 2002, p.9. <https://www-igm.univ-mlv.fr/~dr/XPOSE2002/CyberSurveillance/Telechargements/cybersurveillance.pdf>. CNIL, La vidéosurveillance-vidéoprotection au travail 27 novembre 2019, <https://www.cnil.fr/fr/la-videosurveillance-videoprotection-au-travail>, last visited 23 Dec. 2023.

利を有するが、事前に CE に通知と諮問を行っていない監視カメラを導入することはできない」との一般論を述べ、「使用者が顧客の窃盗を防止するために設置した監視カメラが従業員の活動の監視にも使用された場合、使用者が CE に事前の通知と諮問を行っていないため、当該カメラで撮られた従業員の映像は違法な証拠方法に該当する」とした³⁸⁰。しかし一方、カジノのバーテンダーとして被告 Y 社に雇用されていた原告従業員 X が、Y によって設置された監視カメラに録画されていた、実際には注文されていない大量の飲み物をレジに打ち、売り上げを水増ししていた様子が重大なフォートに当たるとして解雇された事案において、上記監視カメラが人や財産の安全を守る目的で設置されていることしか通知されていなかったという X の上告理由に対し、破毀院は、「カジノのバーで働くすべての従業員が、この業界の規制（Prescriptions réglementaires）に従って常時稼働する監視カメラの存在を知らされていたため、……本件で問題となった録画は合法的な証拠方法であり、レジ系の行動を録画したことはバーテンダーである X の私生活を侵害するものではない」とした³⁸¹。上記 2006 年の先例とは異なり、この判決は、監視カメラが実質的に従業員の活動を監視することにも用いられていたことを審査しなかったこと点に少し疑問が残る。もっとも、本件結論は、本件のカジノという特殊な場所に大きく影響されていると言える。

また、近時では、前掲の Néocel 事件判決で確立された事前通知義務の原則を揺るがすように見える判決が登場した。2021 年 11 月 10 日の事件においては、被告 Y 社（薬局）にレジ係として雇用されていた原告労働者 X が、職場のセキュリティを保護するために設置された監視カメラによってその犯罪行為が録画され、それによって得られた証拠を理由に X が解雇されたが、X は、上記監視カメラの導入の際に通知を受けておらず、また、CE にも通知・諮問されていないため、本件録画は訴訟から排除されるべきであると主張した。これに対して、破毀院は、「ある証拠が違法であるということは、必ずしもそれが訴訟から除外されなければならないことを意味するわけではない。裁判官は、従業員の個人生活（Vie personnelle）を尊重する権利と証拠権（Droit à la

³⁸⁰ Cass. soc., 7 juin 2006, n°04-43.866.他の事件として、後述する GPS 機能付き装置による監視の Cass. soc., 3 nov. 2011, n°10-18.036 や、前述の Cass. soc., 10 janv. 2012, n°10-23.482 などある。

³⁸¹ Cass. soc., 2 févr. 2011, n°10-14.263.

preuve)³⁸²のバランスを図ることにより、当該証拠の使用が全体訴訟手続の公正を損なったかどうかを評価しなければならない。従業員の個人生活を侵害する証拠の利用を正当化できるのは、上記証拠権の行使が不可欠であり、かつ同権利の行使によってもたらず侵害が追求される目的に対して厳格に比例する場合に限定される」という原則を示し、「Y の敷地内の警備を目的とした本件監視カメラが、従業員の行動を管理・監視することが可能であったことからすると、Y は従業員個人に関する情報を収集・利用する目的で上記監視カメラを使用することについて従業員に通知し、CE に通知・諮問すべきであったにもかかわらず、Y はこの手続を怠ったため、本件監視カメラによって得られた録画は違法な証明手段を構成する」とした³⁸³。本判決の意義は、前掲の Néocel 事件判決以降、破毀院が民事訴訟法 9 条や誠実さの原則に基づき、従業員の知らない間に録音・撮影された記録は違法な証拠方法に該当し、当該証拠は訴訟から排除されなければならないと判示してきたのに対して、本件判決は従業員の個人生活を侵害する証拠の利用が、証拠権の行使にとって不可欠であり、かつその侵害が追求される目的に対して厳格に比例する場合、その証拠は例外的に利用できるとした点にある。この判例法理の変化は、前掲の López Ribalda et al. 事件の影響を受けたことが指摘された³⁸⁴。しかし、このような変化によって、これまで従業員に与えられてきた保護の程度が低下したわけではない。というのも、上記判旨から明らかなように、従業員と CE に対して事前に通知していない監視装置は、依然として違法な証拠方法に該当すると判断されたからである。言い換えれば、従業員に通知しなかった監視によって得られた証拠の利用は、証拠権の行使にとって不可欠であり、かつその侵害が追求される目的に対して厳格に比例する「ものではない」ということである³⁸⁵。

ところで、前掲の 2021 年の判決のように、本来は職場のセキュリティを保

³⁸² 証拠権（証明権、証拠提出権などの訳もある）とは、「訴訟当事者が、私生活保護の権利、通信の秘密の権利、業務上の秘密の権利などを侵害することなく、自己の主張の成功に必要な事実または行為を証明できる特権」を意味する。S. GUINCHARD & T. DEBARD, *LEXIQUE DES TERMES JURIDIQUES* 2021-2-22, 29^e éd., 2021, p.819. また、証拠権に関する日本の文献として、町村泰貴「フランスにおける le droit à la preuve の観念」北大法学論集 38 巻 1 号（1987 年）93 頁以下参照。

³⁸³ Cass. Soc., 10 nov. 2021, n°20-12.263.

³⁸⁴ Y. STRICKLER, *Vidéoprotection ou vidéosurveillance - Licéité de la preuve et proportionnalité des moyens mis en œuvre*, *Procédures* n°1, 2022, comm. 4.

³⁸⁵ *Ibid.*

護するためのビデオカメラが、従業員の活動を監視する目的に用いられる用になった場合 (De vidéoprotection à vidéosurveillance, from video protection to video surveillance), 裁判所はその用途を如何にして特定するかについて簡潔に紹介する。フランス法では、監視カメラに適用される規制はその設置場所によって異なる。公共のアクセス可能な場所（一般に開放されている店舗、レジ）に設置された監視カメラを設置しようとする使用者は、県知事（Préfet du département）の許可が必要（国内安全法典（Code de la sécurité intérieure）252-1 条）であり、さらに 2018 年 5 月 25 日に施行された GDPR³⁸⁶ 35 条に規定されるデータ保護影響評価（Data Protection Impact Assessment, DPIA）を実施することも義務づけられている。これに対し、公衆のアクセスできない、いわゆる会社内の倉庫のような私的な場所に設置された監視カメラについて、使用者はかつてそのような監視カメラの利用を CNIL に届出する必要があった³⁸⁶。このように、使用者が履行した手続に応じて、裁判所は簡単に監視カメラの本来の目的を容易に特定し、ビデオカメラ用途の変更の問題を判断することができる。

(iv.) CNIL の立場

1978 年に制定された情報と自由法の実効性を確保するために設置された独立的に設置された CNIL の主な任務は、データ主体およびデータ処理の管理者に対し、その権利と義務に関する情報を提供することと、個人データの取扱いが情報と自由法や EU 法等によって定められた規定を遵守していることを監視することである（情報と自由法第 8 条）。さらに、CNIL は、積極的にガイドラインや意見を策定し、違法なデータ処理を行った企業に対して過料を科し、データ処理を停止させ、場合によっては共和国検事（Parquet）に告発（Dénoncer）したりする権限を有する。また、CNIL は雇用関係における個人データの処理から生じる諸問題に対処する必要性を認識したため、1983 年に労働部分を担当する「情報と労働の自由（Informatique et Libertés du travail）」分科委員会を設立した³⁸⁷。このことは、雇用関係における個人情報処理に関

³⁸⁶ 2018 年に GDPR の施行に伴い、CNIL への事前届出の項目のほとんどが廃止され、その代わり使用者は GDPR と情報と自由法上の規定を遵守することが求められるようになった。諸義務のなかで、GDPR 30 条（情報と自由法 57 条）に基づく情報処理の記録義務は特に重要である。See PH. WAQUET ET AL., *supra* note 329, p.419.

³⁸⁷ A. MOLE, *Informatique et libertés du travail : les nouveaux enjeux*, Dr. soc. 1990, p.59.

するガイドラインの策定等に積極的に取り組んでいるとは言えない日本の個人情報保護委員会の立場とは対照的である³⁸⁸。

監視カメラが労働者の肖像や音声といった個人を識別できる個人データを取得することができることから、CNIL は 2002 年の報告書において、職場における監視カメラの利用は情報と自由法の諸規定を遵守する必要があると明確に示した³⁸⁹。このように、CNIL は、職場における監視カメラの適法性に関する従業員からの苦情に対処する権限がある。以下では、監視カメラによる個人データの処理の適法性に関する CNIL の勧告や決定等を検討する。

CNIL によって策定された職場に設置される監視カメラに関する意見では、いくつかの原則が示されている³⁹⁰。同意見では、まず、一般に公開されていない場所に設置される監視カメラは、情報と自由法におけるデータ処理に関する諸規定（事前に特定された目的やデータ処理の適法根拠など）を遵守しなければならないとされている。ここでいう例外的な状況とは、金銭を扱うレジ係または貴重品を保管する倉庫で勤務する従業員が撮影される場合を指す。しかし、このような例外的な状況であっても、監視カメラはレジ係ではなく、レジに向けられるべきであり、同様に、倉庫で働く従業員ではなく、倉庫そのものに向けられるべきであるとされている。次に、職場における監視カメラの適法性について、CNIL は、主に次のような 3 点を中心に審査する。第 1 に、監視カメラによって得られた録画にアクセスする権利を有する人数とその資格（職位など）が適切であるかどうか、第 2 に、監視カメラの利用目的に照らして、監視カメラによって取得された画像の保存期間が過剰であるかどうか（原則として 1 ヶ月以内）、第 3 に、監視カメラの利用について従業員に適切かつ十分に知らされていたかどうか、当該カメラを設置した管理者の氏名と保管期間を記載した目立つ標識があったかどうか。CNIL は上記の基準に基づき、CNIL は苦情の対象となっている監視カメラの適法性を審査する。

具体例として、2009 年 4 月 16 日の決定においては、CNIL は、被申立人であ

³⁸⁸ 2023 年 9 月 8 日までは、雇用の分野に直接関連するものは、「雇用管理分野における個人情報のうち健康情報を取り扱うに当たっての留意事項」の一つにすぎない。また、従業員の個人情報処理と保護に関する個人情報保護委員会の意見は、ガイドライン（通則編）や Q&A に散見している。

³⁸⁹ BOUCHET, *supra* note 379, p.2.

³⁹⁰ <https://www.cnil.fr/la-videosurveillance-videoprotection-au-travail>, last visited 31 sept. 2023.

る X 社が設置した監視カメラが、従業員を常時撮影していたことに加え、一部の監視カメラが従業員専用の部屋や従業員が着替えをする部屋まで撮影していたとの申立てを受けた。X 社の職場に設置された監視カメラを検査した後、CNIL は Y に対して当該カメラに関する改善命令（Mise en demeure）を発した³⁹¹。しかし、X 社は当てられた期限内に上記改善命令の要求を履行しなかったため、X 社に対する制裁の移行に移行した。CNIL は X 社が設置した上記監視カメラについて以下のように判断した。まず、CNIL は、「監視カメラの導入は、比例性原則を遵守し、追求される目的にとって厳密に必要なでなければならない」という原則を示し、監視カメラを設置する際には、「カメラの台数、位置、向き、稼働時間または従業員が行う業務の性質等の要素」を考慮する必要があるとした。これらの原則を踏まえ、第 1 に、CNIL は、X 社の監視カメラが常時従業員を撮影していたことから、このような監視カメラの利用は過度であり、さらに、本件監視カメラは盗難対策という目的に厳格に限定されていないため、X 社によって追求される目的に比例していないとした。したがって、本件監視カメラは、情報と自由法 6 条第 1 項³⁹²および第 2 項³⁹³（現在は、同法 4 条 1 項および 4 条 2 項）に違反するとした。第 2 に、CNIL は、本件監視カメラの導入後に雇用された従業員の労働契約書には本件監視カメラの存在に関する通知が含まれたが、本件監視カメラの目的、録画にアクセスする権限を有する者の詳細、本件監視カメラの対象となる従業員がアクセス権を行使できる具体的な手続は明記されていないため、X 社が従業員に提供した本件監視カメラに関する情報は不十分であると述べた。したがって、本件監視カメラは、情報と自由法 32 条³⁹⁴（現在は、同法 48 条）に違反

³⁹¹ Délibération n° 2009-201 du 16 avr. 2009 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société X.

³⁹² 情報と自由法 6 条第 1 項は、「個人データは公正かつ合法的に収集・処理されなければならない」と定めている。

³⁹³ 情報と自由法 6 条第 2 項は、「個人データは、特定され、明示された合法的な目的のために収集されなければならない、それらの目的と相容れない方法でさらに処理されてはならない」と定めている。

³⁹⁴ 情報と自由法 32 条は、「自己に関する個人データを収集されたデータ主体は、事前に通知されていない限り、データ管理者またはその代理人から以下の事項を通知されなければならない。1° 管理者の身元、および該当する場合はその代理人の身元；2° 個人データ処理の目的；3° 回答が義務であるか任意であるか；4° 回答しなかった場合の結果；5° データの受領者または受領者のカテゴリー；6° 本章第 2 節の規定に基づいて享受する権利；7° 該当する場合、EU の非加盟国への個人データの移転計画」と規定している。

するとした。以上により、CNIL は X 社に対して 1 万ユーロの制裁金を科すことに加え、X 社の上記違反の重大性に鑑み、上記の決定を CNIL のウェブサイトと Légifrance のウェブサイト³⁹⁵で公表することを決定した。

監視カメラの問題に関する CNIL の別の決定において、CNIL は、被申立人 X 社が管理するビルで警備員として雇用されていた申立人が従業員 Z から、X 社が設置した監視カメラが従業員を常時撮影しており、情報と自由法に違反しているという苦情を受けた。立入検査を実施した後、CNIL は X 社に対し、X らを常時撮影する監視カメラを撤去するよう求める改善命令を下したが、X 社は、本件監視カメラは人および財産を保護する必要性が高いため、上記 CNIL の命令に従わなかった。制裁手続において本件問題となった監視カメラの違法性を審査する際、CNIL は、L.1121-1 と情報と自由法 6 条 3 項³⁹⁶に鑑み、「上記監視カメラによる処理の目的は、Z ら警備員の安全を確保するものではなく、ビルの居住者の安全を確保することである。したがって、Z らの安全を確保する必要性が証明されない限り、上記常時監視できる監視カメラを使用してはならない」とし、「従業員を常時撮影できる監視カメラを正当化するためには、使用者は第三者や財産の安全確保を根拠とすることはできず、『特定の状況または特定の危険 (Situation particulière ou le risqué particulier)』³⁹⁷の存在を証明しなければならない」とした³⁹⁸。以上の判断により、CNIL は、X 社が上記改善命令を無視したことを考慮し、上記監視カメラの稼働を停止

³⁹⁵ フランス政府が開設したデータベースウェブサイトであり、行政サービスの一環として、法令情報、官報などと同様に判決情報を公開している。

³⁹⁶ 情報と自由法第 6 条 3 項は、「個人データは、その収集目的およびその後の処理との関連において、適切かつ適切であり、過度でないこと」と規定している。

³⁹⁷ 同旨、Décision n° 2013-029 du 12 juill. 2013 mettant en demeure X qui exploite l'enseigne « Y » à BOURG-EN-BRESSE. この事案では、被申立人 X 社がショッピングセンター人と財産を保護するために設置した一部の監視カメラが、従業員の更衣室や従業員用のトイレを撮影していたことの違法性に関するものである。また、CNIL は、Délibération de la formation restreinte n°2014-307 du 17 juill. 2014 prononçant une sanction pécuniaire à l'encontre de la société X という決定において、「従業員が常時監視下に置かれるのは、監視対象者がさらされている特定の状況または特定のリスクによって正当化される場合のみであることは一般的である。……同様に、財産や人の安全を保護するという唯一の目的として、職場の休憩所、衛生施設、更衣室内またはその周辺にいる従業員の画像を体系的に収集することは、具体的な正当理由がある場合に限り、比例しているとみなされる」とより詳細に述べている。

³⁹⁸ Délibération de la formation restreinte n°2012-475 du 03 janv. 2013 SYNDICAT DES COPROPRIETAIRES X.

するよう差止命令³⁹⁹を発し、さらに、本件警備業務の性質と財産を保護するというXの主張を考慮に入れ、X社に「1ユーロ」の制裁金を課し、最後に、本件の事実を鑑み、CNILは本件をCNILのウェブサイトとLégifranceのウェブサイトで本件事実と制裁内容を公表することを決定した。

(v.) 小括

監視カメラの問題に関して、破毀院は原則として、使用者が職場に監視装置に設置する前に、CEに通知・諮問することと、監視の対象となる従業員に通知することを義務付けている一方、従業員が働くことが想定されていない場所や、監視カメラが純粹に人と財産の安全を確保する目的で設置される場合には、上記の通知・諮問義務を履行する必要はないとしている。この点で、監視カメラの規制に関する破毀院の判例法理は、尾行と調査の事件に関する判例法理と共通している。さらに、使用者が、従業員とCEに対する監視装置の存在を通知（CEの場合は諮問も義務である）することに違反した場合、監視カメラから得られた録画は、違法な証拠方法となり、その録画は訴訟から排除されなければならない。しかし、前述で検討したように、破毀院は2021年11月10日の判決で、人権裁判所の影響を受け、長年にわたって（前掲1991年のNéocel事件から）堅持してきた判例法理をある程度緩和した。つまり、違法で取得された証拠が訴訟から排除されるかどうかは、従業員の個人生活を尊重する権利と使用者の証拠権とのバランスを図ることによる。もっとも、使用者による通知の義務は、新たに形成された判例法理においても依然として重要であることに留意しなければならない。さらに、監視カメラの目的変更について、本来、職場の人と財産のセキュリティを保護するために設置された監視カメラが、後に従業員の行動を監視するために利用されるようになった事案において、破毀院は、使用者が主張する監視カメラの設置理由に拘束されることなく、設置された監視カメラが従業員の業務状況を監視したかどうかを実質的に審査している⁴⁰⁰。

また、フランスにおける監視カメラの適法性に関する判断枠組みを形成する

³⁹⁹ Délibération n°2010-112 du 22 avril 2010 de la formation restreinte décidant l'interruption d'un traitement mis en œuvre par la Société X. という CNIL の決定においても、CNIL は「本決定の通知から3カ月間、オフィスに設置された2台のカメラを対象とするビデオ監視システムの停止を命じ、その間、情報と自由法の規定を遵守する責任を遵守しなければならない」と命じた。

⁴⁰⁰ B. BOSSU & A. BARÈGE, *Preuve et surveillance des salariés, regard français*, C. & D., 54(2-3), 2013, pp. 287-288.

もう一つ重要な役割である CNIL は、個人データ保護の観点から、当該装置の利用に種々の制限を加えている。CNIL は、違法な監視装置によって得られた証拠を排除すべきであるという限定的な破毀院の判例法理よりも、違法な監視カメラを停止させ、使用者に金銭的サンクションを科し、必要な場合には、共和国検事に刑事訴訟を告発することができるなど、強力な権限を有する⁴⁰¹。CNIL は、破毀院のように監視カメラが事前に従業員に知らされていたかどうかのような比較的単純な審査ではなく、詳細な情報提供の有無、個人データの質 (Qualité)、録画にアクセスする権限を有する者の資格等も審査の対象となり、データ保存期間の合理性、個人データを保護するための安全措置の妥当性などの複数の基準から、監視カメラ利用の適法性を審査する。特に、データ処理の目的性の要請の延長線にある比例性の審査において、CNIL は、従業員を対象とする常時撮影できる監視カメラが過剰であり、監視がもたらす侵害と従業員の権利が比例しないものであると一貫して判断している。最後に、CNIL の見解は、かねてより破毀院の判断と相互に影響し合っており、特に近年は、デジタル化の進展により、職場で行われるほとんどの監視が個人データの処理にあたるため、CNIL の見解が破毀院の判例法理に次々と浸透している。このような現象は、以下で検討する GPS 監視に関する事件と ID バッジに関する事件において最も顕著である。

(2) GPS 機能付き装置による監視

(i) CNIL の立場

2009 年 4 月 16 日の決定においては、CNIL は、2006 年 3 月 16 日の審議⁴⁰²において、GPS 機能付き装置を通じて使用者が、従業員の利用する社用車の位置情報を収集することによって、私生活における従業員の行動を特定することは、従業員の移動の自由及び私生活保護を侵害しうるため、GPS 機能付き装置の利用は情報と自由法に定められている規制に従う必要があると明示した。まず、社用車に搭載された GPS 機能付き装置の利用目的は厳格に限られ

⁴⁰¹ L. MARINO, Vidéosurveillance au travail : le principe de proportionnalité mis en œuvre par la CNIL, *Rev.dr.trav.*, 2010, p.108

⁴⁰² Délibération n°2006-067 du 16 mars 2006 portant adoption d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel mis en œuvre par les organismes publics ou privés destinés à géolocaliser les véhicules utilisés par leurs employés.

ている⁴⁰³。例えば、輸送の種類または輸送品の性質により、GPS 機能付き装置の実施を必要とする法的または規制上の義務の遵守に関する場合や、他の手段で従業員の労働時間を計算できない場合（下線は筆者による）などが挙げられている⁴⁰⁴。次に、上記の審議によれば、使用者は、GPS 機能付き装置を利用する前に、労働者個人と従業員代表に対し、当該装置の利用によって追求される目的、当該装置を設置する法的根拠（労働法典に基づく義務や正当な利益等）、当該措置によって得られた位置情報の保存期間、位置情報の受取者の身元とカテゴリー、従業員が行使できるアクセス権や訂正権などの存在とその手続等の情報を提供しなければならない⁴⁰⁵。また、GDPR が施行されたことに伴い、使用者は GPS 機能付き装置の利用について CNIL に事前届出をする必要がなくなったが、GDPR 上の厳格な規制を遵守する必要がある。例えば、使用者は GPS 機能付きの装置の利用を通じて取得した個人データの処理を記録する義務があり（GDPR30 条）、一定の状況では DPIA（データ保護影響評価、GDPR35 条）を実施する義務が挙げられる。具体的には、使用者が DPIA を実施する義務がある場合に関して、CNIL は GDPR35 条（4）に基づいて策定した通達において、従業員の業務遂行状況を常時監視することを目的としたデータ処理（例えば、GPS 機能付き装置の利用）の場合、使用者は DPIA を実施する義務があると定めている⁴⁰⁶。

また、上記審議と同じ日に採択された GPS の利用に関するもう一つの審議⁴⁰⁷において、CNIL は、GPS 機能付き装置の利用は従業員を常時監視するために使用されるべきではないという原則を強調し、さらに、従業員の私生活保護の観点から、使用者は勤務時間外に従業員の位置情報を収集すべきではないと述べた。さらに、使用者が私的利用で社用車の使用を許可している場合、CNIL は社用車に GPS の機能をオフにできる（Désactiver）装置を設置するこ

⁴⁰³ *Ibid.*

⁴⁰⁴ その他の目的として、分散した場所で業務を行う際、企業のリソースをより効率的に活用できる場合、旅客または物品輸送といった車両の使用に直接関連するサービスの提供を監視する場合、従業員の安全、従業員が管理する商品または車両の安全性を確保する場合が挙げられている。

⁴⁰⁵ *See Délibération supra* note 402.

⁴⁰⁶ Délibération n°2018-327 du 11 octobre 2018 portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise.

⁴⁰⁷ Délibération n° 2006-066 du 16 mars 2006 portant adoption d'une recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme privé ou public.

とを推奨した。もっとも、従業員が勤務時間中に長時間にわたって GPS 機能付き装置をオフにした場合、使用者は当然、社用車を利用した従業員を呼び出して説明を求める権利を有し、場合によっては従業員を懲戒または解雇することができる⁴⁰⁸。このほか、使用者が GPS 機能付き装置を利用して労働組合の代表および従業員代表がその任務を遂行する状況を監視してはならないも強調されている⁴⁰⁹。

(ii.) 破毀院の立場

破毀院において、GPS 機能付き装置による監視について争われた事案はいくつかある。そのリーディング・ケースである 2011 年 11 月 3 日の事件では、被告 Y 社は、外回りの多い営業職（原告労働者 X を含む）の移動時間を分析し、実施する訪問をより最適化する目的で、GPS 機能付き装置を原告労働者 X が利用していた社用車に搭載することを事前に X に通知したが、GPS によって収集された X の位置情報を人事管理の目的で使用するについては通知しなかった。X は、上記装置によって得られた位置情報を根拠とした懲戒処分（減給）は違法であると主張した。破毀院は、L.1121-1 条（比例性審査）に基づき「労働時間を監視するための GPS 機能付き装置の利用は、他の手段では実行できない場合にのみ合法である」（下線は筆者による）。次に、従業員が自由に業務を計画できる場合、GPS 機能付き装置の使用は正当化されない。最後に、使用者は、CNIL に届出をし、従業員に通知した GPS 機能付き装置の利用目的以外の目的に使用してはならない」とした⁴¹⁰。この判決は GPS 機能付き装置の利用に関していくつかの原則を示した。第 1 に、GPS 機能付き装置の利用は、従業員の権利と自由に制限をもたらすものであるため、その制限は使用者が利用した手段と従業員の権利等に比例したものでなければならない。第 2 に、GPS 機能付き装置による労働時間の監視は唯一の手段の場合でなければならない。第 3 に、使用者は、CNIL への届出と従業員に通知した目的以外で GPS 機能付き装置を使用してはならない。破毀院は、労働法典における従来の比例性審査の規定だけでなく、CNIL に対する手続要件や前述し

⁴⁰⁸ <https://www.cnil.fr/fr/la-geolocalisation-des-vehicules-des-salaries>, last visited 18 Oct. 2023.

⁴⁰⁹ Délibération n° 2015-165 du 4 juin 2015 portant adoption d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel mis en œuvre par les organismes publics ou privés destinés à géolocaliser les véhicules utilisés par leurs employés (norme simplifiée n° 51).

⁴¹⁰ Cass. soc., 3 nov. 2011, n°10-18.036.

た CNIL の審議の内容も監視の適法性の判断枠組みに組み込み、GPS 機能付き装置による監視について非常に厳格な規制を設けている⁴¹¹。この点で、本判決において積極的に上記 CNIL の見解を取り入れていることは、学説で「CNIL 意見の司法化 (Judiciariser)」と表現されている⁴¹²。その後の GPS 機能付き装置による監視に関する事案は、基本的にこの判決を踏襲してきた⁴¹³。

また、2017 年 12 月 15 日の事件⁴¹⁴において、コンセイユ・デタは、情報と自由法第 6 条 1 項と 3 項⁴¹⁵および L.1121-1 条に鑑み、「使用者が従業員の労働時間を監視するために GPS 機能付き装置を使用することは、それよりも効果的でないとしても (下線は筆者による)、他の監視手段が利用できる場合は違法となる。したがって、本件では、GPS 機能付き装置以外の手段 (Y 社には労働時間の申告制度があった) が存在し、当該装置を利用して従業員の労働時間を監視するために個人データを収集・処理することは、情報と自由法第 6 条 3 項にいう過剰なデータ処理に該当する」とした⁴¹⁶。監視の目的を達成するために GPS 機能付き装置以外の方法が存在する場合 (上記の「たとえ代替装置の効果は GPS よりも低いとしても」の部分)、GPS 機能付き装置の利用は違法であるという上記コンセイユ・デタの判断から、このコンセイユ・デタの立場は上記 2011 年 11 月 3 日の破毀院判決よりも厳格であると指摘された⁴¹⁷。

その後、破毀院がコンセイユ・デタの上記判断を破毀院の判例法理に組み入

⁴¹¹ A. LEPAGE, Libertés et protection des personnes geolocalisation, CCE n°3, 2012, p.2. B. BOSSU & T. MORGENROTH, La géolocalisation ne doit pas être détournée de sa finalité, *Rev.dr.trav.*, 2012, p.158.

⁴¹² G. LOISEAU, Durée du travail, La géolocalisation sous contrôle, *JCP S* n°6, 2012, p.1054

⁴¹³ 例えば, Cass. soc., 17 déc. 2014, n°13-23.645 事件がある。

⁴¹⁴ この事件では、IT 機械の修理を業とする被告 Y 社は、作業計画を改善するために、事故や運転に関するデータ、従業員の労働時間に関するデータを収集できるリアルタイムの GPS 装置を外回りの多い原告労働者 X の社用車に取り付けた。上記 GPS 装置の利用に関する苦情を得て CNIL は、Y の施設に立ち入り検査を行い、上記 GPS 機能付き装置は従業員の労働時間を管理する手段以外の目的で利用されたため、同装置の利用は過剰であるとし、GPS で収集した位置情報の処理を停止するよう Y 社に改善命令を出した (Décision n°2016-055 du 27 juill. 2016)。Y 社はこの決定に不服を唱え、当該決定の取消を求めた。

⁴¹⁵ 情報と自由法 6 条は、「データ処理は、以下の条件を満たす個人データのみを対象とする。データは公正かつ合法的に収集・処理される (第 1 項)。……収集目的およびその後の処理に関して、適切、適切かつ過度でないこと (第 3 項)」と規定している。

⁴¹⁶ CE 15 déc. 2017 n°403776.

⁴¹⁷ M-C SARRAZIN, Liberté et droit fondamentaux, *Dr.ouv* n°844, 2018, p.705.

れた。2018 年 12 月 19 日の事件においては、被告 Y 社は、チラシや無料な新聞を配布する配布者 Z らに、10 秒ごとに従業員の位置情報を記録する GPS 機能付き装置を取り付けるよう命じたところ、Z らが加入した原告スイス郵便通信連盟 X はこの装置の利用は違法であると主張した。リヨン控訴院は、「X が提案した自己申告制や調査管理者の任命は、Y が実現しようとする目的に適しない」という Y の主張を支持したが、破毀院は、前述したコンセイユ・デタと同様、L.1121-1 と情報と自由法 6 条に鑑み、「使用者が従業員の労働時間を監視するために GPS 機能付き装置を使用することは、たとえそれよりも効果的でないとしても、他の監視手段が利用できる場合は違法となる。したがって、本件では、GPS 機能付き装置以外の手段（Y 社には労働時間の申告制度があった）が存在し、当該装置を利用して従業員の労働時間を監視するために個人データを収集・処理することは、情報と自由法第 6 条 3 項にいう過剰なデータ処理にあたる」とし、上記 GPS 機能付き装置が Z らの労働時間を管理する唯一の手段であったとは認められないとして、上記リヨン控訴院の判断を破毀した⁴¹⁸。このように、破毀院とコンセイユ・デタは、従業員の業務遂行の状況を監視するために利用される GPS 機能付き装置を厳格に制限している点で、見解が一致している。

一方、学説上、GPS 機能付き装置による監視に関する破毀院とコンセイユ・デタで用いられている比例性の審査には、以下の 3 つの要件が含まれているとの指摘がある⁴¹⁹。第 1 は、適切性の基準である。すなわち、選択された手段が追及する目的を達成するのに適したものでなければならない。第 2 は、必要性の基準である。すなわち、使用者が講じた措置は不可欠であり、同じ目的をより労働者の自由を尊重した手段で達成できる手段がないことを意味する。第 3 は、狭義の比例原則の基準である。つまり、従業員の私生活への GPS 監視の侵害が、労働時間管理の利点を明らかに上回る場合、GPS の使用は不釣り合いとなる⁴²⁰。最後に、前述した 3 点の基準をまとめた Bossu は、比例性の原則は、技術の現状を考慮した技術がもたらす最大限のことを対象として審査されるのではなく、私生活保護を個人の基本的権利とみなす社会において許容できることを対象として審査されるものである。言い換えれば、個人の私生活の価値を尊重する社会においては、テクノロジーの利用は基本

⁴¹⁸ Cass. soc., 19 déc. 2018, n°17-14.631.

⁴¹⁹ B. BOSSU, *Durée du travail -Géolocalisation: la Cour de cassation persiste et signe-*, *JCP S* n° 6, 2019, p.1038.

⁴²⁰ *Ibid.*

権の保護が保障されていることが前提であり、したがって場合によっては、テクノロジーの利用が基本権の保護に道を譲ることもあるということである⁴²¹。

(3) ID バッジその他の装置による監視

GDPR が 2018 年に発効されるまで、情報と自由法は、使用者が GPS を含む自動化されたデータ処理の装置を利用する前に、CNIL に事前届出 (Déclaration préalable) することを義務付けていた (旧情報と自由法 22 条)。使用者が上記手続を履践しない場合、同法に基づく制裁 (データ処理の中止や制裁金の賦課) だけでなく、刑法典 (Code pénal, 同法 226-16 条) に基づいて罰せられることもある。しかし、上記 CNIL に届出していない監視装置によって得られたデータを、従業員の解雇や懲戒処分に際して証拠として用いた場合、どのような法的効果が生じるのかは、長い間不明なままであった。破毀院は以下の判決で、この問いを次第に明確してきた。

まず、上記の問いに直接答えるものではないが、原告労働者が、企業が CNIL に届け出ていない ID バッジの着用を拒否したことを理由に解雇された 2004 年 4 月 6 日の事件において、破毀院は、「労働者に関する個人情報の自動処理について CNIL への届出がない場合、従業員が当該処理の実施に関わる使用者の要求に従うことを拒否しても、非難されることはない」と判示した⁴²²。この判決は、破毀院が初めて CNIL への届出に違反した装置の問題について判断したものである。破毀院はこの判決を通じて使用者に対し、自動化されたデータ処理の装置の利用条件は、前述する通知義務 (L.1222-4 条, L.2312-38 条) だけでなく、CNIL への届出も必要であるという重要なメッセージを発した⁴²³。その後、正面から上記の問いに答えた、被告 Y 社は CNIL に届け出ることなく従業員の送受信メールを監視できるシステムを利用し、原告従業員 X が大量の私的メールを送受信していたことが発覚したため X を解雇した 2014 年 10 月 8 日の事件⁴²⁴においては、破毀院は、「CNIL に申告する前に自動個人データ処理システムによって収集された情報は、違法な証拠方法に該当する。

⁴²¹ *Ibid.*

⁴²² Cass. soc., 6 avr. 2004 n°01-45.227.

⁴²³ P. ADAM, Cour de cassation 6 avril 2004 Honeywell Longlaville SA contre P., *Dr.ouv.*2004, p.379.

⁴²⁴ Cass soc., 10 oct. 2014 n°13-14.991.

そのため、Y社がCNILに届け出る前の監視システムによって得られた証拠は訴訟から排除されなければならない」と判示した⁴²⁵。最後に、CNILに届け出なかった入口防犯システムによって解雇の証拠が収集されたことが違法であるかどうか争われた2016年11月2日においても、破毀院は、「企業は、個人情報の自動処理に関する装置はCNILに届け出なければならず、L.2312-38条に従い、従業員の業務遂行の状況を監視する手段または技術を利用する前にCEに通知し、諮問しなければならない」とし、CEに事前通知（諮問）せず、CNILにも届けなかった上記システムによって収集された証拠を訴訟から排除すべきであるとしたリヨン控訴院の判断を是認した⁴²⁶。

また、前述したように、2018年にGDPRが施行されて以降、企業の自動化されたデータ処理装置をCNILに届け出る義務がなくなり、代わりにGDPR上の厳格な規制（例えば、前述したGDPR35条のDPIAの実施義務やGDPR30条のデータ処理の記録義務⁴²⁷）を遵守しなければならなくなった。ここで新たに問題となるのは、使用者が実施した監視がGDPRの規定に違反した場合、その監視装置によって収集された、解雇や懲戒処分のために使用されるデータは、従来のように、違法な証拠として訴訟から排除されなければならないかどうかである。この点を正面から判断した破毀院判決はまだ登場していないが、学説では、GDPRに違反した監視装置によって収集されたデータは、従来の通り、訴訟から排除されなければならないと解する見解が多い⁴²⁸。

以上の判決から明らかなように、従来の従業員及びCEに対する通知義務に加え、破毀院はCNILへの届出義務を、使用者が適正な監視を実施するための必須要件としたことが見られる。これは、前述で検討したCNILのGPSに関する意見を司法化したことと同様、破毀院が情報と自由法上のCNILへの届出要

⁴²⁵ *Ibid.*

⁴²⁶ Cass. soc., 2 nov. 2016, n°15-20.540. また、企業が自動化されたデータ処理装置の利用を事前に CNIL に届け出ていた場合、その後の同システムの単純な更新を CNIL に届け出る必要はなく、そのため当該システムによって得られた解雇の証拠を適法とした判決がある。Cass. soc., 23 avr. 2013, n°11-26.099.

⁴²⁷ また、GDPR 上の諸義務に違反した場合、高額の制裁金が科される規定も新設された。GDPR83 条参照。

⁴²⁸ PESKINE & WOLMARK, *supra* note 366, p.343, F. LEFRANÇOIS, La surveillance de l'activité des salariés, *LIAISONS SOCIALES QUOTIDIEN* n°216, 2020, p.4.

件を監視の適法性の判断枠組みに再び組み込んだもう一つの具体例である。

このように、監視の適法性に関する判断枠組みが、司法機関である破毀院、CNILの意見、使用者のCNILに対する法的義務の絡み合いによって形成されていることがフランス法の特徴であるといえよう。

第4節 まとめ

フランスの労働法における監視の規制に関しては、長い間労働法典に監視の実施を直接規制する規定を持たなかったが、前掲 1991 年の Néocel 事件判決は、初めて使用者が監視カメラを利用する前に労働者に通知する義務を課しており、それ以来、破毀院の判例法理において定着している。その後、1992 年の労働法典の改正により、上記破毀院の判例法理が明文化され、とりわけ、使用者は機器を用いた監視を実施する前に従業員と従業員代表（CE、または現在の CSE）に通知する義務が新設された。しかし、上記の改正法では、使用者が新設された事前通知義務に違反した場合にどのような法的効果が生じるかについての規定が定められていないため、破毀院は従来のように、証拠排除に関する判例法理で対処している。

また、フランスにおける監視の適法性に関する判断枠組みの特徴は次のように要約できる。単純な監視にせよ、機器を用いた監視にせよ、いくつかの例外を除き、破毀院は使用者に対し、従業員の行動を監視・検査する前にその存在を従業員に通知しなければならないことを厳格に求めており、さらに、この事前通知義務を共通の基盤とし、さまざまな監視形態に応じて追加的規制を発展させてきた。例えば、GPS 機能付き装置による監視に関しては、代替手段の可能性という規制、ID バッジによる監視に関して、CNIL への事前届出という規制を加えた。これらの要件は情報と自由法の規制及び CNIL の見解に由来するものであることから、フランスでは、機器を用いた監視の適法性に関する判断枠組みが、破毀院と CNIL の緊密な協力関係によって形成されている点に特徴がある。

第4章 共同規制方式の可能性

第1節 序説

第2章と第3章では、人権裁判所の判例法とフランスにおける監視の適法性に関する判断枠組みについて検討した。これらの判断枠組みは監視の違法性を審査する役割だけでなく、使用者が適正な監視を行うインセンティブを与えるものでもあるとわかった。しかし、これらの判断枠組みをそのまま日本に取り入れることは必ずしも適切とは言えない。というのも、まず、これらの判断枠組みの内容は依然として不明確性が残っており、使用者が適正な監視を行うのに十分なものとはいえない。また、テクノロジーの急速な変化により、監視を含む個人データ処理がもたらす問題に対処する際、法律制定ないし改正は新たな技術発展のペースに追いつくことができず、このような規制手法の限界が顕在化しつつあることを考慮すると、こうした規制の具体的な内容を定めるに当たっては、公的機関よりも情報量と知識で優位な産業団体の関与が重要である。実際に、近時、公的機関と産業団体によるデータ保護の分野においては共同規制（Co-regulation）という規制手法が提唱されてきた。共同規制の概念はすでに後述するデータ保護の分野以外の様々な分野で用いられているが、データ保護とプライバシー保護の分野で、最初に共同規制について法的拘束力のある法規制に明記したのは、EUの1995年のデータ保護指令における行動規範（Code of conduct）である。しかし、データ保護指令上の行動規範に実効性が乏しかったため（第4章第2節1款参照）、その利用は一般的ではなかったが、その後2018年に施行されたGDPRはデータ保護指令上の行動規範を大幅に修正し、その欠陥を改善した。

また、日本にも、上記のEU型の行動規範に類似している制度がある。個人情報保護法上の認定個人情報保護団体（以下では、認定団体と略称する）の制度は、公的機関である個人情報保護委員会と事業者団体の協働によって運用されていることから、共同規制の一態様と言える⁴²⁹。同制度については、個人情報保護法の制定当初からすでに存在していたが、認定団体が策定した保護指針に違反した対象事業者に対する効果的なサンクションがなかったため、広く利用されていなかった。しかし、令和2年の法改正により、認定団体に対象事業者を監督する権限が新たに付与されたため、今後この制度の重要性が高まると予想される。

⁴²⁹ 大内伸哉「労働法の規制手法はどうあるべきか」季労280号（2023年）7頁。

以上を踏まえ、以下では、第2章と第3章での検討内容との繋がりを意識しつつ、まず、共同規制を含めた規制手法の種類や定義や問題点を分析し、次に、これまで労働法学⁴³⁰ではまだ十分に検討されてこなかったデータ保護の分野における共同規制の手法に焦点を当てて検討し、最後に、共同規制の概念を具体化した上記EU型の行動規範と日本の認定団体の制度を対象として考察する。

第1款 規制手段の種類と特徴

規制手法の種類は、大きく3つのタイプに分類できる。第1に、国家規制（Government regulation, State regulation, Command and control）があり、これは、国の議会によって制定され、公的機関によって執行される強い法的拘束力を有す伝統的な手法である。この種の規制は、複雑で流動的かつ革新的な分野ではない場合、最も効果的なものである。また、国家規制は、業界団体のニーズよりも、公衆の利益を優先させなければならず、さらに、民主的正統性を維持するために、ルールの制定過程の透明性も確保しなければならない⁴³¹。他方、複雑で流動的かつ革新的な分野においては、公的機関と産業団体との間に情報量と知識の非対称性があり、公的機関が規制対象の具体的な状況を把握できないため、国家規制はイノベーションを阻害する事態を招く可能性がある⁴³²。データ保護の分野はまさにその典型例である。

⁴³⁰ 規制手法を検討する文献として、荒木尚志「労働立法における努力義務規定の機能－日本型ソフトウェア・アプローチ」中嶋士元也還暦『労働関係法の現代的展開』（信山社、2004年）19頁以下、内藤忍「イギリスの行為準則（Code of Practice）に関する一考察--当事者の自律的取組みを促す機能に着目して」労働政策研究・研修機構ディスカッション・ペーパー09-05（2009年）1頁。
<https://www.jil.go.jp/institute/discussion/2009/documents/09-05.pdf>（最終アクセス日 2023年12月12日）、山川隆一「労働法における法の実現手法」佐伯仁志編『岩波講座 現代法の動態第2巻法の実現手法』（岩波書店、2014年）171頁以下、鎌田耕一「労働法の実効性確保」日本労働法学会編『講座労働法の再生第1巻』（日本評論社、2017年）225頁以下、土岐将仁「労働法の実現手段としての業界自主ガイドライン」季労280号（2023年）50頁以下などがある。また、労働法学における共同規制の手法に関する先駆的業績として、大内・前掲注429）2頁以下。

⁴³¹ D.D. Hirsch, *In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector-Based Codes of Conduct*, 74(6) OHIO ST. L.J. 1029, 1041(2014). Hirsch は、国家規制は製造業から排出される有毒汚染物質を規制するのに適切であると指摘した（p.1041）。

⁴³² I. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 I/S: J.L. & POL'Y FOR INFO. Soc'y. 355, 367 (2011).

第2に、自主規制（Self-regulation）があり、多くの分野で用いられている。自主規制には、国家規制よりも柔軟性があり、実施コストも低く、個々の産業団体のニーズを反映できるという利点がある⁴³³。しかし、自主規制は、エンフォースメントが弱く、透明性もないという問題を抱えている。さらに、公衆の利益よりもルールを設ける当事者の利益を優先させる可能性がある点（公的な目的を達成できない）、第三者（主に消費者）にとって不公正な規制の制定、策定されたルールが中小企業や新規参入企業の競争力を阻害する可能性（独占禁止法の問題が生じうる⁴³⁴）などの問題点が挙げられる⁴³⁵。

実際には、自主規制と国家規制の間に多くの規制モデルが存在しえるのであり、それらは「国家が自主規制の中でどのように位置づけられるか」の違いによって区別することができる⁴³⁶。例えば、公的機関が直接関与することなく、産業団体がルールを制定（Rulemaking）し、その執行（Enforcement）を行うという徹底した自主規制のモデルでは、その構成員は互いには説明責任を負うが、公的機関に対して説明責任を負わないなどの問題が生じやすい⁴³⁷。他方、委任型と呼ばれる自主規制もあり、これらは、公的機関がルールの過程に関与する場合と、自主規制の結果を事後的に承認する場合で区別される⁴³⁸。

データ保護の分野では、アメリカには民間企業に適用される包括的な個人情報保護法がないため、アメリカ政府は長い間、この分野における自主規制の利用を強く勧奨してきた⁴³⁹。その理由は、関連法規定の欠如だけでなく、複雑で流動的かつ革新的な分野の発展のペースに国家規制が追いつくことは困難であり、過剰な規制はインターネット上のビジネスの発展を阻害すること

⁴³³ *Id.* p. 368.

⁴³⁴ 大内・前掲注429) 8頁。

⁴³⁵ 生貝直人「プライバシー共同規制の近年の動向—米国・EUの制度改革を中心に—」信学技報 48号(2013年)15頁以下。また、純粋な自主規制（pure self-regulation）は、法的なコンプライアンスを保障することができないという点で、産業界の関与を集めることも、特定の分野における国際的基準に対処することもできないとの問題があると指摘された。See Hirsch, *supra* note 431, p. 1043.

⁴³⁶ Rubinstein, *supra* note 432, p. 368.

⁴³⁷ *Ibid.*

⁴³⁸ I. Kamara, Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate', 8 (1) EJLT. 1, 3(2017).

⁴³⁹ C. Bennett & D. Mulligan, The Governance of Privacy Through Codes of Conduct: International Lessons for U.S. Privacy Policy, p. 2 (2012), Available at <https://ssrn.com/abstract=2230369>.

になりかねないという事情が考慮されたからである⁴⁴⁰。とはいえ、自主規制には、前述したような欠点があるため、データ保護の分野で自主規制が多用されているアメリカでは、多くの問題が生じている⁴⁴¹。

第2款 共同規制の概念

共同規制（共同統治「Collaborative governance」とも呼ばれている）は新しい概念ではなく、環境保護政策や労働安全衛生などの分野⁴⁴²ですでに使われていたが、2000年代から、急速に変化し続けているインターネット技術がデータ保護にもたらす問題に対処するために、その有用性が新たに注目されるようになった⁴⁴³。広い意味での共同規制とは、自主規制の利点を活かしつつ、自主規制の不完全性やリスクを公的機関が補完するものであると理解されている⁴⁴⁴。したがって、共同規制は、純粋な自主規制でもなければ、純粋な国家規制でもなく、この2つアプローチ間の「ハイブリット」な手法として位置付けられている⁴⁴⁵。

共同規制の定義について、「特定の問題に対応するにあたり、効率的かつ実効的なコントロール・ポイントを特定し、それらが行う自主規制に対し一定の公的な働きかけを行うことにより、公私が共同で解決策を管理する政策手法」とする見解⁴⁴⁶や、「政府がガイドラインの策定などにより、ルール形成に緩やかに関与しているに過ぎず、あとは政府以外の主体によるルール形成を

⁴⁴⁰ 生貝直人「オンライン・プライバシーと自主規制-欧米における行動ターゲティング広告への対応-」情報通信学会誌 96 号（2011 年）108 頁。

⁴⁴¹ 例えば、典型的なケースとして、プライバシー及び個人情報保護の分野と最も密接な関係がある消費者保護を担当するのはアメリカの連邦取引委員会（Federal Trade Commission, FTC）は、NAI 協会（Network Advertising Initiative）にオンライン広告の規制を策定させるために自主規制の手法を利用したが、NAI が本文で述べたような自主規制の欠陥を克服できなかったため、最終的に失敗に終わった。See D. D. Hirsch, The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?, 34 SEATTLE U. L. REV. 439, 463(2011).

⁴⁴² 具体例について、*Id.* p.466.

⁴⁴³ *Id.* p.441.

⁴⁴⁴ 生貝・前掲注 440) 14 頁。

⁴⁴⁵ Hirsch, *supra* note 441, p.441.

⁴⁴⁶ 生貝直人『情報社会と共同規制-インターネット政策の国際比較制度研究-』（勁草書房、2011 年）33 頁。

前提とし、その実効性確保に委ねるような場合」と広く捉える見解がある⁴⁴⁷。いずれにせよ、共同規制の形態には、いくつかの共通している特徴があり、すなわち、①共同規制の当事者（公的機関と産業団体）は敵対的ではなく協力的であるという傾向があること、②共同規制は、国家が制定した目的を果たすために企業や仲介者などに依拠すること、③国家規制に比べ、共同規制は開放的（Open-ended）な性質を有するため、産業団体は具体的な実施計画を策定する際により大きな裁量を持つこと、④事業者は自らが関与して作成するルールをより重視する傾向があるため、共同規制の手法はルールの遵守率を高めることが挙げられている⁴⁴⁸。ただ、前述したように、自主規制には多くのモデルがあるので、共同規制との区別は必ずしも明確ではない⁴⁴⁹。両者の区別については、「共同規制は、公的機関から産業団体に対して何らかの形で明示的な法的権限の委譲が行われているか否かという点で、自主規制と区別される」と解する見解⁴⁵⁰、「公的機関が規制に関与する度合いだけでなく、説明責任（Accountability）、規制の制定、規制の調整、規制違反への制裁と公衆の関与という点で、自主規制と区別される」とする見解⁴⁵¹、「両者の違いはどの主体が規制の目標と基準を設定し、執行するかにある」との見解がある⁴⁵²。このほか、共同規制の擁護者は、共同規制には、国家規制にある情報の非対称性の問題と自主規制に見られる実効性欠如の問題を是正する利点があり、さらにより費用対効果が高く、実効性があり、激しく変化する分野に適応できると主張している⁴⁵³。これに対して、共同規制に懸念を抱く論者は、共同規制は公的機関と業界団体の間で密室での取引や透明性に欠けるアプローチになりかねないこと、産業団体は内部の情報を公的機関に開示せず、その代わりに情報優位性を利用して自身らに有利な、より低い基準を形成する可能性があることに警鐘を鳴らしている⁴⁵⁴。

以上の検討を踏まえ、次節では、最初に共同規制の手法をデータ保護法で具

⁴⁴⁷ 大内・前掲注 429) 4 頁。

⁴⁴⁸ Rubinstein, *supra* note 432, p.371.

⁴⁴⁹ J. Winn, *Electronic Commerce Law: Direct Regulation, Co-Regulation and Self-Regulation*, Cahiers du CRID (forthcoming Sept. 2010), p. 10 (2010). Available at <https://ssrn.com/abstract=1634832>.

⁴⁵⁰ *Ibid.*

⁴⁵¹ Rubinstein, *supra* note 432, p.371.

⁴⁵² Hirsch, *supra* note 441, p.465.

⁴⁵³ *Id.* p.467.

⁴⁵⁴ *Id.* pp. 441-442.

体化した EU のデータ保護法における行動規範の制度について検討する。

第 2 節 EU データ保護法における共同規制の具体化

第 1 款 1995 年データ保護指令上の行動規範

個人データ保護の分野では、行動規範（Code of conduct）は共同規制の方式を具体化する代表例の一つであると考えられている⁴⁵⁵。その理由は、EU の行動規範が、公的機関と産業団体との緊密な協力のもとに、個々の産業団体の特殊性を反映し、データ保護法の適用をより明確にするために作成された法的ツールであるからである。実際、共同規制の概念を具体化した後述する EU の 1995 年のデータ保護指令が制定される前、行動規範というツールは、すでにいくつかのプライバシーや個人データ保護に関する国際的なガイドライン等において言及されていた。例えば、1980 年 OECD の「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」の附属文書（Explanatory memorandum）では、アカウントビリティ（説明責任）の項目で、「アカウントビリティの履行は、法的制裁と行動規範によって支えられる」と述べられており、その後、上記 1980 年 OECD のガイドラインの 2013 年改正版の 19 条（d）では、行動規範の利用が奨励されている。また、欧州評議会の第 108 号条約の解説においても、行動規範は国内法のデータ保護を補強することができると明記されている⁴⁵⁶。しかし、これらは、いずれも法的拘束力がなく、行動規範の策定や運用に関する詳細を定めていない。

行動規範が初めて法的拘束力のある法規定に盛り込まれたのは、EU 加盟国間のデータ保護法を調和するために制定された上記の 1995 年のデータ保護指令である。同保護指令においては、行動規範に関するいくつかの規定が定められた。まず、行動規範の意義について、同保護指令の前文 61 号では、行動規範の目的が「特定の分野で行われるデータ処理の特性を考慮し、……本保護指令の適用を容易にすること」と明記されている。次に、同保護指令 27 条は、行動規範の作成やその規範へのデータ保護機関（Data Protection Authority, 以下、DPA という）の関与などを次のように規定している。「各加盟国の政府

⁴⁵⁵ 生貝直人「プライバシー共同規制の近年の動向—米国・EU の制度改革を中心に—」信学技報 48 号 (2013 年)16 頁, M. von Grafenstein, Co-Regulation and the Competitive Advantage in the GDPR: Data Protection Certification Mechanisms, Codes of Conduct and the 'State of the Art' of Data Protection-by-Design, p. 15(2019), available at <https://ssrn.com/abstract=3336990>.

⁴⁵⁶ See C. Kuner et al., The EU General Data Protection Regulation: A Commentary, p.720 (2020).

と欧州委員会は、加盟国が保護指令に従って採択した国内規定の適切な実施に役立てるために、様々な分野の特性を考慮しつつ、行動規範の策定を奨励しなければならない（第 1 項）。各加盟国は、国内の行動規範の草案を策定し、または既存の国内の行動規範を修正、または拡充しようとしている産業団体その他の事業者の代表機関が、行動規範の草案を各加盟国の DPA の意見を聞くために提出できるように定めなければならない。各加盟国は、DPA が、提出された草案が指令に従って採択された国内規定に準拠しているかどうかを審査（Ascertain）するための規定を定めなければならない。また、適切と判断される場合には、DPA はデータ主体またはその代理人に意見を求めなければならない（第 2 項）。EU 全体に適用される行動規範の草案、および既存の EU 全体に適用される行動規範の修正または拡充は、保護指令第 29 条の作業部会に提出することができる。作業部会は、提出された草案が本保護指令に従って採択された国内規定に準拠しているかどうかを判断しなければならない。また、適切と判断される場合、作業部会はデータ主体またはその代理人に意見を聴取しなければならない。欧州委員会は、作業部会によって承認された行動規範の適切な公開を確保することができる（第 3 項）」。以上の内容から、保護指令における行動規範の特徴は次のようにまとめられる。第 1 に、加盟国は産業団体が行動規範の策定をするよう奨励する義務を有する⁴⁵⁷。第 2 に、DPA は行動規範の草案について意見を述べ、その草案が保護指令と同指令を国内法化したデータ保護法に準拠しているかどうかを審査する必要がある。第 3 に、適切と判断される場合には、DPA は、データ主体またはその代理人に意見を聴取する必要がある。これらの特徴に関しては、学説上、いくつかの問題が指摘された。まず、上記の「奨励（Encourage）」と「行動規範の草案に対する DPA の意見」に関する具体的な定義が定められていないため、加盟国によってその運用に大きなばらつきが見られた⁴⁵⁸。前者の「奨励」の方法については、保護指令の時代に行動規範と共同規制との関係を先駆的に研究した Hirsch は、まず、EU 加盟国間における「奨励」の解釈を、①産業界の選択（Industry choice）、②力の均衡（Balance power）、③政府による選択

⁴⁵⁷ 同指令の前文 61 項では、「加盟国および欧州委員会は、それぞれの権限範囲において、特定の分野で行われる処理の特定の特性を考慮し、その実施のために採択された国内規定を尊重しつつ、本指令の適用を容易にするために、関係する業界団体およびその他の代表団体が行動規範を作成するよう奨励しなければならない」と規定されている。

⁴⁵⁸ Hirsch, *supra* note 441, p.471.

(Government choice) という3つの種類に分類した⁴⁵⁹。①のアプローチを採用したドイツやオーストリアの法律では、行動規範を策定するかどうかはすべて産業団体に委ねられており、加盟国の政府とDPAは、上記の保護指令27条第1項の通り、行動規範の制定に関する具体的なインセンティブを設けることなく、行動規範の策定を単に奨励するだけであった。②のアプローチを採用したイタリアやマルタの法律では、保護指令27条に基づくDPAと加盟国の義務がより強調されており、DPAは行動規範を作成するよう各産業団体に「要請」することが義務づけられ、また、DPAが産業団体と協力するための具体的な手続も定められた。③のアプローチを採用したルーマニアやイギリスの法律では、産業団体が行動規範を策定することを強く奨励しており、産業団体が行動規範を策定しない場合、DPAがそれに代わって行動規範を策定すると規定された。このようなアプローチは、条文上の「奨励」の範囲を超えているが、産業団体の行動規範を策定するかどうかの裁量権を剥奪するものではない。というのも、産業団体には依然として、行動規範を策定する選択肢が残っているからである。また、後者の「行動規範の草案に対するDPAの意見」については、DPAの意見を法的拘束力のあるものとした加盟国と、それを単に事実上の意見とした加盟国があった⁴⁶⁰。

次に、前述したHirschは、たとえ加盟国間における行動規範の運用にばらつきがあっても、①行動規範がない分野ないし部門でも、保護指令自体の規範はデフォルトとして当該分野の事業者には適用されており、アメリカのように全く規範が存在しない状況にはならない、②すべてのDPAは、行動規範の草案が、データ保護指令（またはそれを国内法化した国内のデータ保護法）に準拠しているかどうかを審査することを義務づけている、いう共通点を抽出することができる指摘した⁴⁶¹。

以上のように、保護指令において初めて共同規制に基づく行動規範が導入さ

⁴⁵⁹ *Id.* pp. 475-479.

⁴⁶⁰ *Id.* p. 471. Hirschの論文で挙げられた一つの具体例はイタリア法の状況である。DPAの意見を法的拘束力のあるものと認めたイタリア法では、イタリアのDPAによって承認された行動規範は、DPAとイタリア国内裁判所を拘束することができ、さらに司法大臣の命令(*decréto*)により、承認済みの行動規範はイタリアの個人データ保護法の附則(*annex*)に添付され、イタリアの個人データ保護法の一部になっているため、当該行動規範に加入していない同じ分野(産業)の事業者もその規範の内容を遵守する必要があるとされている。

⁴⁶¹ *Id.* p.475.

れた意義は大きいといえるが、行動規範の策定やその運用を監視する加盟国と DPA の役割が明確ではなかったなどの問題から、保護指令時代には行動規範（特に EU 全体に適用されるもの）は結局あまり活用されなかった⁴⁶²。

第 2 款 GDPR 上の行動規範

(1) 序説

データ保護指令時代の行動規範の問題を解決するため、GDPR は行動規範の趣旨と内容を大幅に修正・拡充した。特に行動規範のコンプライアンスを監視する機関が欠如していたという重要な問題を克服するため、監視機関（Monitoring bodies）を新設し、さらに産業団体が行動規範を作成するインセンティブをもたらす諸規定も整備した。なお、保護指令時代に批准された行動規範は、GDPR の行動規範として認められるためには、新たに各国の DPA によって審査・批准される必要がある⁴⁶³。以下では、本論文の主題との関連性が低いため、複数の加盟国間で適用される行動規範（保護指令 27 条 3 項と同様）の分析は割愛し、GDPR における特定の加盟国に適用される行動規範のみに焦点を当てて、EDPB（第 2 章第 2 節 2 款（2））が定めた行動規範の内容と関連ガイドライン（以下では、EDPB ガイドラインと略称する⁴⁶⁴）を参考にしつつ、GDPR における行動規範制度の意義について検討する。

(2) 新たな行動規範の概説

GDPR 上の行動規範の目的について、GDPR40 条 1 項は、「各加盟国、DPA、EDPB 及び欧州委員会は、データ処理の分野と中小零細企業の特性を考慮しつつ、GDPR の適正な適用に貢献することを目的とした行動規範の策定を奨励するものとする」と規定している⁴⁶⁵。この規定から明らかなように、行動

⁴⁶² もっとも、データ保護指令 27 条所定の手続を踏まない行動規範が多く存在していたことも指摘された。KUNER ET AL, *supra* note 456, p.718.

⁴⁶³ EDPB, Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, p.6 (§6).

⁴⁶⁴ *Ibid.*

⁴⁶⁵ 本論文で扱う GDPR の和訳はすべて、個人情報保護委員会のウェブサイトに掲載されているものに基づいている。https://www.ppc.go.jp/enforcement/infoprovision/EU/#outside_adoption_EU (最終アクセス日 2023 年 12 月 2 日)。

規範の主な目的は、事業者⁴⁶⁶が各分野の特性を反映し、GDPR に基づく義務を遵守していることをよりよく示すことと⁴⁶⁷、及び、GDPR への対応が困難な中小零細企業が集団的な方法で GDPR を遵守できるようにすることである⁴⁶⁸。

また、EDPB ガイドラインとフランスの DPA (CNIL) の意見では、行動規範の策定によってもたらされる利点として、まず、行動規範は IT 憲章や倫理規範のようなものではなく、GDPR によって法的拘束力を与えられる強力なツールであるため、その加盟者に法的拘束力のある義務を課すことができること、特定の分野で、より透明で効率的かつ、潜在的に費用対効果が高い 방식으로データ保護の問題に対処できること、GDPR5 条 2 項に定めるデータ処理のアカウントビリティの遵守を証明する手段として利用できること、個人データを EU 域外に移転する場合に適切な保護措置を提供できるツールとして用いることができること (GDPR46 条 2 項 (e))、個人データの処理に関する一般市民の信頼を向上させるために、適切な保護措置が講じられていることを証明することができること、ビジネスの観点からは、企業の競争優位性を提供することもできること、などが挙げられている⁴⁶⁹。

(3) 行動規範が批准されるまでの手続

EDPB のガイドラインでは、行動規範の草案を策定する前に、行動規範の保持者 (英: Code owners; 仏: Porteur du code) は、次のような基準を満たす必要があるとされている⁴⁷⁰。①説明文書および補足文書の添付、②代表性を有すること、③データ処理の範囲、④同規範が適用される地理的な範囲、⑤管轄権を有する DPA への提出、⑥監視のメカニズムの要件、⑦GDPR41 条の監視機関 (Monitoring body) の指定、⑧利益関係者との協議、⑨国内のデータ

⁴⁶⁶ 実際、GDPR では、事業者という言葉ではなく、管理者 (controller) と処理者 (processor) という概念が用いられている。しかし、本節では GDPR 上の行動規範にのみ焦点を当てて検討するため、便宜上、ここでは両者を区別せず、一括して「事業者」と呼ぶことにする。また、データ保護指令においては、行動規範を策定できる主体は管理者のみであったが、GDPR における行動規範は管理者だけでなく、処理者も新たに追加された (GDPR40 条 2 項、前文 81 項)。

⁴⁶⁷ GDPR 前文 77 項。

⁴⁶⁸ EDPB, *supra* note 463, p.8(§11).

⁴⁶⁹ *Id.* p.8(§10). KUNER ET AL, *supra* note 456, p.718. CNIL の意見については、<https://www.cnil.fr/fr/ce-qu'il-faut-savoir-sur-le-code-de-conduite>, last visited 2 Dec 2.

⁴⁷⁰ EDPB, *supra* note 463, p.11.

保護法の遵守、⑩言語選択の要件。以下、重要な要件である①②③⑥⑦⑧のみを簡潔に説明する。①については、行動規範の保持者は、同規範の目的や規範の適用範囲を明確にし、その行動規範の策定を通じて、如何にしてGDPRの規定をより効果的に適用できるかを示す必要がある。②については、行動規範の保持者は、自らの協会や組織が当該分野における「代表性」を有するものと証明しなければならない⁴⁷¹。③については、行動規範の保持者は策定された行動規範を適用する事業者を明示する必要がある。⑥については、行動規範の草案は、その適用を約束するステークホルダーが同規範の内容を遵守していることを監視できるような仕組みを含まなければならない。⑦については、行動規範の草案の作成には、GDPR41条の要件を満たす監視機関を含めなければならない。⑧については、行動規範の保持者は、行動規範の草案を策定する際に、ステークホルダーと協議したことを証明する必要がある⁴⁷²。

行動規範の保持者が上記の要件を満たした規範の草案を提出した後、下記図1で示すように、DPAは行動規範の保持者と草案をめぐって協議した上で、それを承認するかどうかを決定する。仮に行動規範の草案が否定される場合、DPAは行動規範の保持者にその理由を開示し、再提出を求める。また、DPAが行動規範を批准する場合、通常、行動規範の批准（Approved）と同時に、次款で検討するGDPR41条の監視機関の資格も認定する（Accredited, GDPR58条3項（d））。というのも、行動規範には監視機関を含めなければならないからである（GDPR40条4項）。最後に、DPAは批准した行動規範を登録し、それを公表しなければならない（GDPR40条6項）。なお、行動規範の承認後も、DPAの関与がなくなるわけではなく、DPAは、批准された行動規範の運用状況を間接的かつ継続的にモニタリングし続ける。例えば、行動規範で指定された下述の監視機関は、行動規範の加盟者が同規範に違反した際、当該加盟者に対して資格の停止や規範からの排除などの制裁を科した後、直

⁴⁷¹ 具体的には、行動規範の保持者は、DPAに対して特定の分野において策定する行動規範に加盟する潜在的なメンバーのニーズを理解し、当該分野における実務経験があったことなどを証明する必要がある。

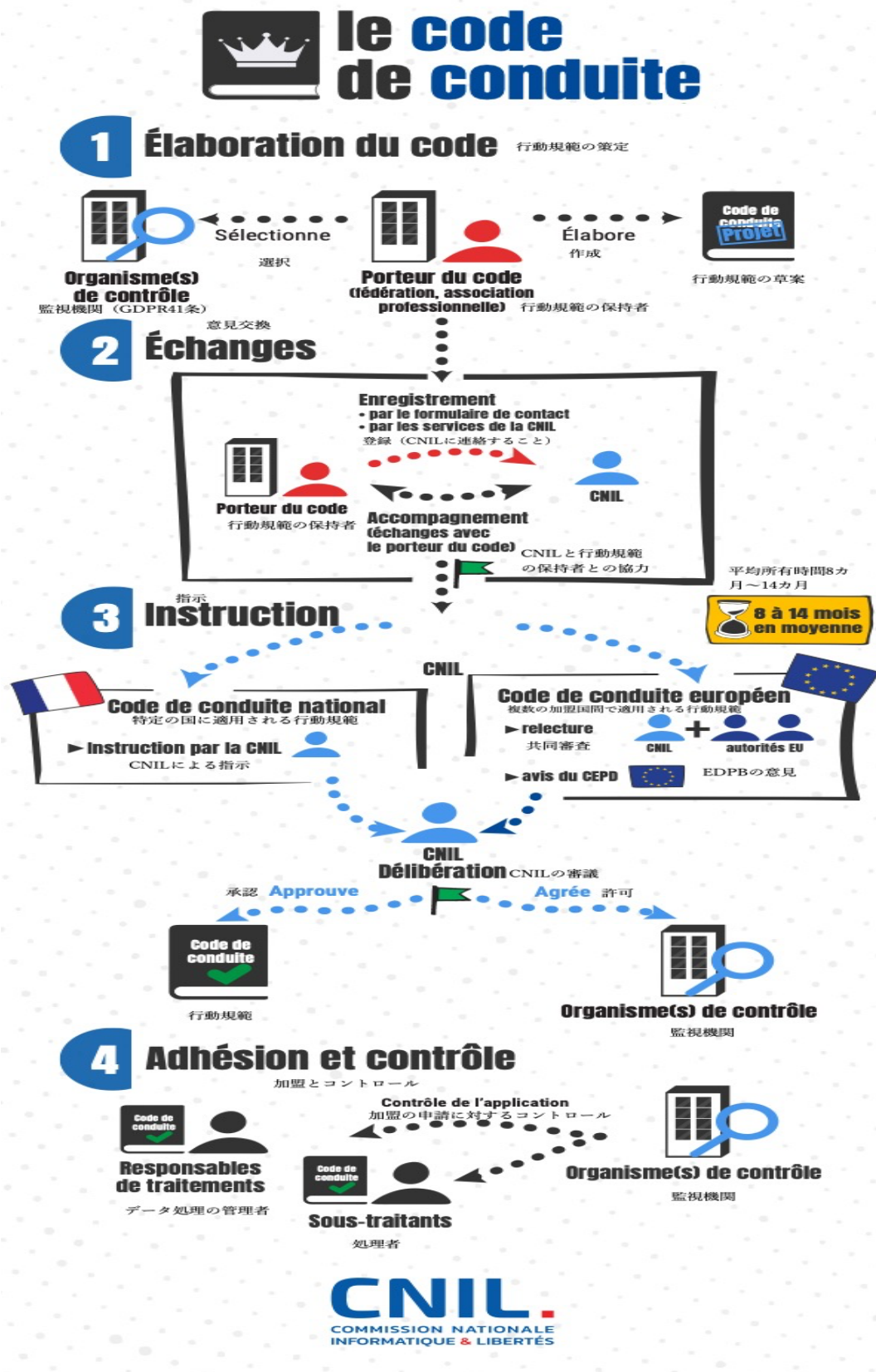
⁴⁷² 前文99項は、「行動規範を策定する際、またはその規範を改正又は追補する際、様々な種類の管理者又は処理者を代表する団体その他の組織は、それが有用であるときはデータ主体を含め、関係するステークホルダーと協議し、そしてそのような協議に応じて申し出や表明された意見を考慮しなければならない」と定めている。

ちに DPA に制裁の経緯を報告しなければならない (GDPR41 条 4 項)。

また、行動規範における監視装置の適用に関する具体例として、CNIL は、監視カメラに関する破毀院の判例法理や CNIL による命令等を中小企業が理解することは困難であることを考慮し、行動規範による対応が有用であるとの意見を示した。例えば、行動規範に監視カメラの設置場所と向き、表示される情報パネルのモデル、画像の保存期間、画像にアクセスする権限を有する者、並びに法的な解釈を含めることにより、監視カメラから生じる問題に対処することができる⁴⁷³。

⁴⁷³ *Ibid.*

図1 行動規範が批准されるまでのプロセス（筆者による一部修正）⁴⁷⁴



⁴⁷⁴ https://www.cnil.fr/sites/cnil/files/2023-06/infographie_le_code_de_conduite.pdf, last visited 5 Dec. 2023.

(4) 新たな監視機関の認定基準

前述のように、保護指令には行動規範の運用状況を監視する組織がなかったため、DPA に承認された後の行動規範のコンプライアンスの問題は主に各国の DPA が策定したガイドラインによって対処されていた⁴⁷⁵。しかし、行動規範の内部運用を監視する機関がない限り、同規範の透明性と実効性は担保されず、その結果、行動規範は事業者がデータ処理に関するアカウントビリティを果たすための有用なツールとはなり得なかった。また、DPA の関与にも限界があったという問題も指摘された⁴⁷⁶。例えば、DPA の執行力は加盟国の財政等の原因によってその状況が異なり、データ処理全般の問題を所管する DPA のリソースが不足していることがしばしば報告されている⁴⁷⁷。このような状況のもとで、DPA の業務量を軽減するという目的も含め、GDPR は新たに行動規範のコンプライアンスや透明性を監視する機関を設けた（GDPR41 条 1 項）。監視機関は、行動規範と同様、管轄権を有する DPA による認定を受けなければならない。GDPR41 条 2 項は、監視機関を認定する基準を一応定めているが、同条 3 項及び 57 条 1 項 (p) ⁴⁷⁸に基づき、各加盟国の DPA は GDPR61 条に基づいて監視機関の具体的な認定基準を EDPB に送付しなければならない。以下では、まず、EDPB のガイドラインを概観し、次に、CNIL が EDPB に送付した基準のうち、特に重要な部分のみを紹介する。

まず、監視機関は管轄権を有する DPA（行動規範の提出先）に対し、①当該機関の独立性、②当該機関と行動規範の加盟者との間に利益相反はないこと、③監視業務を遂行するための専門性を有すること、④確立した監視の手続と構造を有すること、⑤透明性のある苦情処理ができること、⑥DPA とのコミュニケーションを保つ能力を有すること、⑦再審査のメカニズムがあること、⑧法的地位を証明しなければならない⁴⁷⁹。①については、行動規範の保持者は、DPA に対して指定した監視機関の税制状況や組織の構造が、保有者及びその加盟者から独立していることを証明しなければならない。また、監視機

⁴⁷⁵ KUNER ET AL, *supra* note 456, p.727.

⁴⁷⁶ Kamara, *supra* note 438, p.2.

⁴⁷⁷ *Ibid.*

⁴⁷⁸ GDPR57 条 1 項、「本規則に定める他の職務を妨げることなく、各 DPA は、その領土上において…(p) 第 41 条による行動規範を監視するための組織の認定に関する基準及び第 43 条による認証機関の認定に関する基準を策定し、それを公表するものとする」と規定している。

⁴⁷⁹ EDPB, *supra* note 463, pp.21-25.

関が行動規範の保持者の内部機関の場合、保持者は監視機関に雇用される従業員の人事管理を保持者のそれと明確に区別していることを証明しなければならない。②については、行動規範の保持者は、監視機関がその任務と義務を果たす際、保持者またはその加盟者との利害対立が生じないことを証明する必要がある⁴⁸⁰。③行動規範の保持者は、自分が指定した監視機関に専門性、特にデータ保護に関する知識があることを証明しなければならない。④については、指定された監視機関は、行動規範に加盟する事業者（管理者または処理者）の資格を審査し、加盟者が行動規範の規定に従うかどうかを監視し、行動規範全体の運用を調査（例えば、抜き打ち調査や年次定期調査など）するための手続と構造を備えていなければならない。⑤については、監視機関は、データ主体による苦情が公正かつ透明性のある方法で処理し、行動規範の加盟者が同規範を遵守していることを確保するために、効果的な手続と体制を整備する必要がある⁴⁸¹。⑥については、具体例として、監視機関が行動規範の遵守状況に関する定期的な報告書を DPA に提出する義務や同規範に違反した加盟者を制裁した後、速やかに管轄権を有する DPA に報告する義務が挙げられている（GDPR41 条 4 項）。⑦については、法律の適用や解釈の変更、または行動規範の加盟者が実施するデータ処理や、行動規範の内容に影響を及ぼす可能性のある新たな技術的発展があった場合には、それに適応するための監視機関による再審査のメカニズムを導入する必要がある。⑧については、行動規範の保持者は、監視機関が GDPR41 条 4 項に定める業務を遂行するための適切な地位を有していることを保障し、さらに当該監視機関が GDPR83 条 4 項 (c) ⁴⁸²に定める制裁金の対象となる地位を有していることを証明する必要がある。

また、認定された監視機関が適切にその業務を遂行できない場合、GDPR41

⁴⁸⁰ 例えば、行動規範の保持者は、監視機関が自律的に行動する能力を有し、行動規範の保持者及びその加盟者による制裁の対象とならないことを確保するための保護措置を講じていることを証明する必要がある。

⁴⁸¹ 例えば、行動規範の加盟者が同規範に違反した場合、監視機関は当該事業者の権限を一時中止したり、金銭的制裁を科したり、さらにはその加盟者を同規範から排除したりすることができる。See C. KUNER ET AL, *supra* note 456, p.730.

⁴⁸² GDPR83 条 4 項は、「以下の条項違反行為は、第 2 項に従い、1000 万ユーロ以下の制裁金に服するものとし、または、事業の場合、直前の会計年度における世界全体における売上総額の 2%以下の金額、若しくは、いずれか高額の方の制裁金に服するものとする…… (c) 第 41 条第 4 項による監視機関の義務」と規定している。

条 5 項⁴⁸³に基づき、DPA はその認定を取り消すことができる。そのため、一つの監視機関しか含まれていない行動規範の場合、監視機関の認定の取り消しに伴い、その行動規範も一時的に停止されるか、永久的に取り消される可能性がある。さらに、EDPB のガイドラインによると、監視機関の認定が取り消されることは、行動規範の加盟者のレピュテーションや事業利益に悪影響を及ぼし、データ主体やその他の利害関係者の信頼も低下させる結果になりかねないことが指摘されている⁴⁸⁴。

次に、EDPB のガイドラインに基づき、CNIL が策定した監視機関となるための要件に関する審議 (délibération)⁴⁸⁵のうち、特に重要な部分を抽出して検討する⁴⁸⁶。まず、CNIL は監視機関の認定期間を 5 年間とし、5 年ごとの更新が必要であると示した。同審議において、監視機関を認定するための要件を、基本的に上記 EDPB のガイドラインと同様としつつ、EDPB ガイドライン上の一部の要件をより具体化した。例えば、「DPA とのコミュニケーションを保つという要件」について、監視機関が行動規範に違反した加盟者に制裁を科した後、DPA に通知する必要があるという上記 EDPB ガイドラインの内容に加え、CNIL は、DPA が CNIL と定期的に連絡をとることを義務付けている⁴⁸⁷。具体的には、監視機関は、CNIL がいつでもアクセスできるように、講じたすべての措置をまとめた文書を作成しなければならない⁴⁸⁸。監視機関は、その独立性、専門性及び利益相反がないことを疑わせるような重大な変更があった場合には、遅滞なく、書面で CNIL に通知しなければならない⁴⁸⁹。監視

⁴⁸³ GDPR41 条 5 項は、「DPA は、認定の条件が満たされていない場合、若しくは、満たされなくなった場合、又は、当該組織の行動が本規則に違反する場合、第 1 項に規定する組織の認定を取り消さなければならない」と定めている。

⁴⁸⁴ EDPB, *supra* note 463, p.26 (§86).

⁴⁸⁵ Délibération n° 2020-050 du 30 avril 2020 portant adoption d'un référentiel relatif à l'agrément des organismes chargés de contrôler le respect des codes de conduit.

⁴⁸⁶ この審議は、CNIL が 2019 年 10 月 18 日にフランスにおける監視機関を認定する具体的な基準に関する草案を採択し、同月 18 日に EDPB に提出した。EDPB は 2020 年 1 月 28 日に上記草案に対して好意的な意見を発表し、同年 2 月 4 日に CNIL にその意見を通知した。最終的に、CNIL は 2020 年 4 月 30 日の審議において、フランスに適用される GDPR41 条に基づく監視機関の認定に関する具体的な基準を策定した。

⁴⁸⁷ Délibération, *supra* note 485, p. (7).

⁴⁸⁸ *Id.* (7-1).

⁴⁸⁹ *Id.* (7-2).

機関は、行動規範に違反した加盟者に対して規範からの除外や金銭的制裁などの措置を講じた場合には、「制裁の経緯」だけでなく、「当該措置を講じた正当な理由」も CNIL に書面で報告しなければならない⁴⁹⁰。監視機関は、行動規範に違反した加盟者の資格を停止・除外した場合、「停止に関する正当な理由」または「除外に関する正当な理由」を含め、CNIL に書面で遅滞なく報告しなければならない⁴⁹¹。

以上の検討を踏まえると、保護指令の時代における行動規範のコンプライアンスとエンフォースメントが欠如していたとの弊害を打破するために、GDPR は一連の改正、とりわけ GDPR41 条 1 項の監視機関を導入することでこの問題に対処した。監視機関の特徴は、行動規範の内部審査ではなく、同機関の認定段階から任務遂行（場合によっては認定の取り消し）まで、各国の公的機関である DPA が関与していることである。このように、GDPR において新たに導入された監視機関は、従来の行動規範の欠点を克服するだけでなく、その根底にある共同規制の概念をさらに確固としたものになっている⁴⁹²。

（5）行動規範の策定に関するインセンティブ規定

GDPR は、EDPB（GDPR70 条 1 項（n））、加盟国の政府や加盟国の DPA（GDPR40 条 1 項）が行動規範の策定を奨励しなければならないと定めている点は保護指令第 27 条第 1 項と同様であるが、それに加えて、一連の規定を通じて行動規範を策定することを具体的に奨励している。以下では、これらの行動規範を策定するためのインセンティブとなる規定を網羅的に取り上げることとする。

まず、GDPR24 条（管理者の責任）においては、データ処理の性質、範囲、過程及び自然人の権利及び自由に対する侵害の蓋然性と深刻性のリスクを考慮に入れた上で、管理者は、GDPR の規定に従ってデータ処理が遂行されることを確保し、かつそのことを説明できるようにするための適切な技術上及び組織上の措置を実装しなければならないと規定されている。管理者が行動規範に加盟している場合、行動規範は管理者が上記義務を果たしていることを証明するための要素として用いることができる（同条 3 項）。同様に、行動

⁴⁹⁰ *Id.* (7-3).

⁴⁹¹ *Id.* (7-4&7-5).

⁴⁹² EDPB のガイドラインによれば、監視機関は DPA と行動規範の保持者との間のコーディネーターと呼ばれている。EDPB, *supra* note 463, p.25 (§82).

規範は処理者が GDPR 上の義務を遵守していることを証明するための要素として用いることもできる (GDPR28 条 5 項)。

さらに、データ処理のセキュリティのために講じる要件 (個人データの仮名化及び匿名化や技術的なインシデント発生時の対策など) に関する場合でも、行動規範は、事業者が GDPR において定められている要請を満たしているための証明となり得る (GDPR32 条 3 項)。また、事業者は、個人データの処理が自然人の権利や自由に高いリスクを発生させるおそれがある場合、その処理に先立ってデータ保護影響評価 (DPIA) を実施する義務がある (GDPR35 条 1 項)。同条 8 項は、DPIA を実施する際、批准された行動規範の遵守を考慮に入れなければならないと明記している。このほか、最も重要であると考えられているのは、DPA は、事業者が GDPR に違反したとして制裁金を科す場合、当該事業者が加盟した行動規範を遵守しているか否かを考慮し、制裁金の額を調整することができる。具体的には、GDPR83 条 2 項では、「個々の案件において、制裁金を科すか否かを判断する場合、及び制裁金の額を判断する場合、以下の事項を考慮しなければならない」と規定されており、批准された行動規範の遵守はその一つの要素として取り上げられている (同条項 (j))。

(6) 学説上の議論

GDPR 上の行動規範に関する学説上の議論には、制定時から欧州委員会が強調してきた「GDPR の遵守が企業に競争優位性をもたらす」ということを、どのように実現するかに関する Grafenstein の研究がある⁴⁹³。Grafenstein は、データ処理に伴うイノベーションがもたらすリスクを抑えると同時に、イノベーションを促進するためには、共同規制が最も適切な規制手法であると主張している⁴⁹⁴。その理由は、公的機関は産業団体ほどデータ保護の分野に関する豊富な情報と知識を有していないため、具体的で適切な規制を制定することができないからである⁴⁹⁵。Grafenstein の研究によると、GDPR には、データ処理の原則規定 (例えば、GDPR5 条のデータ処理の適法化根拠) や、不明確な法的概念 (例えば、GDPR25 条のデータ保護バイデザイン及びデータ保護バイデフォルト) しか定めていない規定が多く存在しており、GDPR は、

⁴⁹³ Grafenstein, *supra* note 455, p.2.

⁴⁹⁴ *Id.* p.26.

⁴⁹⁵ *Id.* pp.5-6.

このような規定の内容を具体化し、法的確実性を高めるために、ガイドラインや勧告といった従来のアプローチだけでなく、行動規範（GDPR40, 41 条）と認証制度（GDPR42 条）のような方法も利用しているという⁴⁹⁶。このことから、Grafenstein は、行動規範や認証制度を利用する事業者は、それらを利用しない事業者に比べて、法的確実性を得ることによって、GDPR 上の広範で曖昧な規定を企業の競争優位性に転換することができると主張した⁴⁹⁷。もっとも、同氏は、事業者が行動規範の内容について、漠然と GDPR の規定を焼き直しても、前述の競争優位性を獲得することはできないとも指摘している⁴⁹⁸。この点に関して、CNIL も、行動規範が批准されない主な理由の一つに、行動規範の保持者が GDPR の規定を単に繰り返していることを挙げている⁴⁹⁹。

また、日本においては、GDPR 上の行動規範や認証制度を運用する意義に関する山本龍彦の先行研究もある⁵⁰⁰。山本は、GDPR の全体的構造を分析した上で、プロファイリングに関する諸規定を例として、それらの規定の内容が不明確（解釈の不確定性）⁵⁰¹であり、権利侵害及び違法行為を如何にして特定するかも困難であるという問題（同定困難性）に対し、GDPR は行動規範や認証制度などからなる構造統制型規律（ガバナンス・アプローチの規律）という観点から、前述した問題を補完・克服していると指摘した⁵⁰²。上記のGrafensteinと山本の研究はいずれも、GDPR 上の行動規範等の制度を利用することが曖昧かつ広範な法規定の明確性を向上させることができることを示している⁵⁰³。もっとも、Grafenstein の主張は、山本が主張した単なる不明確な規定の具体化ではなく、行動規範等を通じて得られる法的確実性によって、GDPR で強調されている「ビジネス上の競争力の優位性」を獲得することが

⁴⁹⁶ *Id.* p.7.

⁴⁹⁷ *Id.* p.26.

⁴⁹⁸ *Id.* pp.16-17.

⁴⁹⁹ <https://www.cnil.fr/fr/que-doit-contenir-un-code-de-conduite>, last visited 12 Dec. 2023.

⁵⁰⁰ 山本龍彦「『完全自動意思決定』のガバナンスー行為統制型規律からガバナンス統制型規律へ？」情報通信政策研究 3 巻 1 号（2019 年）25 頁以下。

⁵⁰¹ 例えば、GDPR13-15 条では、事業者はプロファイリングを含め、完全に自動化された意思決定を実施する場合、上記プロファイリング等の「結果に関する意味のある情報」をデータ主体に提供することが義務付けられているが、ここでの「結果に関する意味のある情報」が具体的に何を指すかは不明確であると指摘した。同上注、27 頁。

⁵⁰² 同上注、36 頁。

⁵⁰³ 同上注、44 頁。

できることを強調している点に留意しなければならない。

第3節 日本における認定個人情報保護団体

第1款 認定個人情報保護団体の経緯と趣旨

日本の個人情報保護法には、上記 GDPR の行動規範に類似している制度がある。認定団体は、同法制定当初から存在している制度であるが、認定団体に関する学説上の議論は必ずしも多いとは言えない⁵⁰⁴。その一因として考えられるのは、2020 年改正までは、認定団体は、自らが作成した個人情報保護指針（以下では、保護指針と略称する）に違反した対象事業者（認定業務の対象となることに同意した事業者のこと、同法 52 条 1 項）に対して制裁を加える権限を持たなかったため、保護指針の実効性が保障されていなかったということである。

この認定団体の欠陥を是正するため、同法の 2015 年の改正により、認定団体は作成した保護指針を個人情報保護委員会に届け出なければならず、個人情報保護委員会は届け出られた保護指針を公表する義務を負うことが新設された⁵⁰⁵。また、同改正法では、対象事業者に対し、保護指針を遵守させるための必要な指導、勧告その他の措置を講じる認定団体の「努力義務」は「義務」へと変更したとされた（同法 54 条 4 項）⁵⁰⁶。その後、同法の 2020 年の改正では、認定団体に対する認定は、従来の「事業の種類」から「企業の特

⁵⁰⁴ 例えば、穴戸常寿「個人情報保護委員会」ジュリ 1489 号（2016 年）46-47 頁、日置巴美「改正個人情報の保護に関する法律のポイント(第 3 回)匿名加工情報に関する制度および認定個人情報保護団体制度の解説」NBL1087 号（2016 年）

⁵⁰⁵ まず、前者の個人情報保護委員会への届出の義務により、個人情報保護委員会はいかなる認定団体がいかなる保護指針を定めるかを把握することができ、問題のある保護指針の変更その他の必要な措置を命ずることができ（同法 154 条）、逆に、優れた保護指針を認識した時は、それを国の施策に反映したり、ほかの認定団体に情報提供をしたりすることが可能である。一方、後者の個人情報保護委員会の公表義務の義務により、国民は、認定団体が作成した保護指針を容易に認識することができ、さらに、国民が自身に関する個人情報処理について苦情があった場合、苦情の処理を担当する認定団体を容易に特定することができる。瓜生和久『一問一答 平成 27 年改正個人情報保護法』（商事法務、2015 年）139 頁と宇賀克也『個人情報保護法制』（有斐閣、2019 年）143 頁参照。

⁵⁰⁶ この改正は、上記保護指針の届出とそれを公表する個人情報保護委員会の義務に伴い、認定団体の実効性確保の強化を図ろうとしたものであることが指摘された。同上注、39 頁（瓜生）。

分野（部門）」まで拡大されており（同法 47 条 2 項）⁵⁰⁷，認定団体に保護指針に違反した対象事業者を制裁する権限も付与された（同法 52 条 1 項）。この改正の理由として，対象事業者が保護指針を遵守しない場合，認定団体は国民の信頼を失うだけでなく，認定団体による個人情報保護の推進に支障が生じかねないということが指摘された⁵⁰⁸。

次に，認定団体の目的について，事業者間の自主的な取組みを尊重した上で，個人情報保護の水準を確保・向上を図ろうとすること⁵⁰⁹，あらゆる分野を対象として必要最小限度の規制を定める個人情報保護法の上に，さらに分野ごとに取り扱う個人情報の性質や利用方法といった特性に即した規制を設けること，事業者が有する専門性や柔軟性を活用し，基本的な法の履行よりも深化させた自主ルールを策定・運用することが挙げられている⁵¹⁰。また，認定団体の業務は，同法 47 条 1 号～3 号で挙げられているように，①対象事業者の個人情報の取扱いに関する苦情の処理（1 号），②個人情報等の適正な取扱いの確保に寄与する事項についての対象事業者に対する情報の提供（2 号）⁵¹¹，対象事業者の個人情報等の適正な取扱いの確保に関する必要な業務（3 号）である。特に 3 号にいう必要な業務について，個人情報保護委員会が策定した認定団体ガイドラインでは，認定団体は，対象事業者が自らで個人情報の取扱いの透明性等を確保するための説明責任を果たすことができない観点から，対象事業者に対して事前に PIA（privacy Impact Assessment）を含むプライバシー・バイ・デザインの実践や個人データの取扱いに関する責任者の設置（Data protection officer, DPO）などを指導することが望ましいとされている⁵¹²。

なお，個人情報保護委員会が策定した最新の AI を搭載した顔識別機能付きカメラシステムに関するガイドラインでは，認定団体はこのようなシステムを導入する対象事業者に対し，①上記 PIA の実施を勧告すること，②収集し

⁵⁰⁷ 企業の特定分野を新設した理由として，事業分野が幅広い企業の業務全般に適合する認定団体を発見することが困難である一方，認定団体からしても，企業のすべての業務を認定団体に取り入れることは適切ではないからである。岡本・前掲注 30）471 頁。

⁵⁰⁸ 園部逸夫＝藤原静雄『個人情報保護法の解説〔第 3 版改正版〕』（ぎよせい，2022 年）456 頁。

⁵⁰⁹ 石井夏生利ほか『個人情報保護法コンメンタール』（勁草書房，2021 年）752 頁。

⁵¹⁰ 個人情報の保護に関する法律についてのガイドライン（認定個人情報保護団体編，2021 年）2 頁や，園部逸夫＝藤原静雄・前掲注 508）434 頁など。

⁵¹¹ 例えば，前述した保護指針の作成・公表や各業界における利用目的の特定の程度などが挙げられている。同上注（認定個人情報保護団体編，2021 年）7 頁。

⁵¹² 同上注（認定個人情報保護団体編，2021 年）8 頁。

た個人データの保存期間に関する情報の提供、③システム運用のチェック、④対象事業者における利害関係者への意見聴取や第三者委員会設置のサポート、⑤対象事業者における被撮影者等の対応（開示等の請求、苦情処理等）のサポートを指導することが期待されるとされている⁵¹³。

第2款 共同規制の概念に基づく認定個人情報保護団体

認定団体を共同規制の観点から検討する学説は必ずしも多くない⁵¹⁴。前述の認定団体ガイドラインと諸学説は、認定団体を事業者団体による自主的な取組と捉えていることが多く、共同規制という用語はあまり使用されていない⁵¹⁵。しかし、以下で検討するように、認定団体の制度は共同規制の概念を具体化した一形態と捉えることができる。まず、認定団体になろうとする事業者団体は、個人情報保護委員会の認定を受けるために、同法 48 条に定める状況に該当しないことを示す必要があり、その上で、前述した認定団体の①～③の業務を遂行する資格があることを同委員会に証明しなければならない（同法 49 条）⁵¹⁶。個人情報保護委員会から認定を受けた後の段階においては、認定団体は保護指針の作成に努めなければならない（同法 54 条 1 項）。現行法では、保護指針の作成は努力義務にとどまっているが、実際には、個人情報保護委員会が認定したすべての認定団体（2023 年 12 月の時点では、44 団体がある）は保護指針を作成し、公表している⁵¹⁷。また、保護指針を作成する際、認定団体は関係者の意見を聞くことも求められている（同項）。これは、先進国におけるマルチステークホルダープロセスの方式を参考にしたものとして説明されている⁵¹⁸。さらに、同法 54 条 4 項により、認定団体は、対象事業者

⁵¹³ 個人情報保護委員会「犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用について」（2023 年）61-62 頁。https://www.ppc.go.jp/files/pdf/kaoshikibetsu_camera_system.pdf（最終アクセス日 2023 年 12 月 12 日）。

⁵¹⁴ 認定団体の制度を共同規制として捉える学説として、大内・前掲注 429）7 頁がある。

⁵¹⁵ 岡本は、「認定団体の制度は、事業者団体等の自主的な取組を尊重した上で、必要な部分について最小限度の規律を行いつつ政府等が支援（する）」と指摘した。岡本・前掲注 30）470 頁。

⁵¹⁶ また、個人情報保護法の施行令 14 条 1 項の記載事項を満した書類を同委員会に提出する必要もある。例えば、事業者団体の名称や事業報告書、認定業務を適切に行うに足りる知識及び能力を有することを明らかにする書類などがある（詳細は同条項参照）。

⁵¹⁷ 個人情報保護法施行規則 42 条は、認定団体の公表義務を規定している。一方、個人情報保護法 54 条 3 項は、個人情報保護委員会に対し、認定団体が届け出る保護指針を公表することを義務付けている。

⁵¹⁸ 岡本・前掲注 30）477 頁。

に対して保護指針を遵守させるために必要な指導，勧告その他の措置を講じなければならず，さらに同法 52 条 1 項に基づき，保護指針を遵守しない対象事業者を対象業務から除外する権限を有する。一方，公的機関である個人情報保護委員会の関与としては，認定団体になろうとする事業者団体に認定を与えるほか，必要な限度において認定団体に対して認定業務に関する報告を求めること（同法 153 条），認定団体から届け出られた保護指針を審査し，場合によってはその内容の変更を命ずること（同法 154 条），認定団体が上記業務を適切に遂行できない場合と，認定団体が欠格事項に該当する場合にはその認定を取り消すこと（同法 155 条）がある。

以上の検討から，認定団体の制度については，共同規制の観点からはあまり論じられていないが，公的機関である個人情報保護委員会が認定団体のあらゆる段階に関与すると同時に，認定団体には保護指針の届出や認定の証明が義務付けられているとの観点から，認定団体の制度は共同規制の概念を具体化したものと言える。

また，前述したように，GDPR における行動規範を策定する利点は，各分野の特性を考慮した上で，必要最小限度の規制を定めた GDPR の規定をより具体化することで，法的確実性を高めるとする見解があった。このことは，日本の個人情報保護法上の認定団体の制度にも当てはまると考えられる。例えば，個人情報保護委員会は，Q&A において，従来型防犯カメラ（防犯目的で設置されているカメラのうち，撮影した画像から顔特徴データの抽出を行うもの）と，顔識別機能付きカメラを区別し，事業者が前者のようなカメラを利用する際，通知義務の例外（同法 21 条 4 項 4 号，取得の状況からみて利用目的が明らかであると認められる場合）に該当し，本人（データ主体）への利用目的の通知・公表は不要であるという新たな見解を追加した（Q&A1-13）。しかし，両者を区別する基準は曖昧であり，上記の解釈は法的確実性を欠くものである。この問題に対し，認定団体の「公益社団法人日本防犯設備協会」が作成された保護指針においては，対象事業者が「従来型防犯カメラ」を利用する場合でも，「防犯カメラが稼働中である旨の掲示や防犯カメラの設置者を明示するなど，個人情報を取得することを認識させることが望まれる」と記載されている（3 頁）⁵¹⁹。その上で，同保護指針では，「隠し」監視カメラの設置は，防犯設備等に対する国民の理解を深める等の観点から不適切であり，監視の対象となる者が「見落とさないように見やすく工夫すると共に，

⁵¹⁹ https://www.ppc.go.jp/files/pdf/51_ssaj_shishin.pdf（最終アクセス日 2023 年 12 月 12 日）。

ホームページ等で詳しく説明を行う必要がある」とされている（3頁）⁵²⁰。隠しカメラに関する個人情報保護委員会の公式見解がない現状では、同認定団体の上記意見は重要な意義を持つと言える。同様に、認定団体の「工業会日本万引防止システム協会」が作成した保護指針においても、「防犯カメラ（筆者注：上記 Q&A における本人に通知しなくてもよい従来型防犯カメラを指す）が作動中であることを店舗の入り口や設置場所等に掲示する等、本人に対して自身の個人情報が取得されていることを認識させるための措置を講ずるとともに、当該利用目的の範囲内で利用しなければならない」と明記されている（12頁）⁵²¹。

このように、個人情報保護委員会による公式見解がまだ存在しない場合、または同委員会による解釈の内容自体が不明確な場合、認定団体は、その欠如や不明確を補う重要な役割を果たすことができる。

第3款 GDPRの行動規範との差異

GDPR における行動規範の制度と同様、認定団体制度は各分野の特性を反映しつつ、法規定の確実性（法的安定性）を高めるために、公的機関と事業者団体が協力するという点で共通しているが、両制度には質的な違いがある。まず、現行の個人情報保護法では、対象事業者が保護指針を遵守しているか否かを監視する責任は認定団体にあると規定されている。しかし、この制度は、まさにEU1995年のデータ保護指令における行動規範の欠点と同様、監視機関を欠いた状態で、認定団体の透明性と信頼性は如何にして実効的に担保されるかが疑問であり、GDPR は上記の種々の規定を定めることでこの問題を解決した。日本の個人情報保護委員会は、認定団体に対し、認定業務に関する報告をさせる権限と、認定業務の改善等を命ずる権限を有するが、個人情報保護に関する業務全般を所管している同委員会のリソース等の観点からは、認定団体内のガバナンスを第一義に担保する監視機関を設けることが検討されるべきであろう⁵²²。次に、同法の 2015 年の改正と 2020 年の改正によ

⁵²⁰ Ibid.

⁵²¹ https://www.ppc.go.jp/files/pdf/48_jeas_shishin.pdf（最終アクセス日 2023 年 12 月 12 日）。

⁵²² 個人情報保護委員会のウェブサイトを確認したところ、認定団体の資格が取り消された例今のところ 1 件しかなく、同法 153 条に基づく報告の徴収は 2018 年 12 月 10 日付けの「認定業務の適正な実施に関する報告について（個情第 1849 号）」しか見当たらない。
<https://www.ppc.go.jp/personalinfo/nintei/pastinfo/>（最終アクセス日 2023 年 12 月 12 日）。

り、対象事業者に保護指針を遵守させるために認定団体の権限と義務が強化されたが、最も肝心な保護指針の作成は依然として努力義務にとどまっている（同法 54 条）。この点に関して、「民間団体による自主的な取組的な取組を尊重しようとするのが本制度の趣旨であることから、個人情報保護指針の作成については努力義務とされている」という説明⁵²³があるが、各認定団体の特性を反映できる保護指針の重要性や、前述した保護指針に関する認定団体の権限が法改正によって強化されたという観点から、保護指針の作成を義務に変更することが検討されるべきであろう。最後に、GDPR と比べて、個人情報保護法は、事業者が認定団体になることや、事業者が認定団体に加盟することを奨励する規定（インセンティブ規定）が十分ではない。現在では、認定団体に加盟するメリットとして挙げられているのは、主に苦情の処理の補助、情報提供または研修を受けられる等にとどまっている（同法 47 条 1 項、53 条）。テクノロジーの急速な進化に伴って個人情報の処理が高度化・複雑化している中、民間企業と公的機関の協力が必要不可欠という観点から、事業者団体が認定団体になることと、事業者が認定団体に加盟することを奨励する「インセンティブ規定」を定めることが必要不可欠であると思われる。

第 4 節 まとめ

以上、本章では、規制手法のなかで近年脚光を浴びている共同規制を焦点に当てて検討した。共同規制は特に本論文で検討するデータ処理の一態様である監視のような、複雑で流動的かつ革新的な分野において特に効果的である。EU では、1995 年のデータ保護指令のときから、共同規制の概念に基づく行動規範に関する規定を導入したが、監視機関の欠如などの欠陥があったため、その利用は一般的ではなかった。2018 年に施行された GDPR は、上記の欠陥を改善するために、新たな行動規範に関する監視機関や種々のインセンティブ規定を導入した。また、EDPB も学説も、行動規範の策定によって、GDPR 上の広範かつ不明確な法規定について、各分野の特性を反映しつつ、法的確実性を高めることができるという利点を強調している。一方、行動規範と同じ共同規制の概念に基づくとみることができる日本の認定個人情報保護団体の制度は、個人情報保護法の 2015 年と 2020 年の改正により、同認定団体の権限と義務が次第に強化されてきた。個人情報保護の分野においては、その運用が期待されている。しかし、認定団体の制度は、行動規範と比較すると、

⁵²³ 園部逸夫＝藤原静雄・前掲注 508）461 頁。

多くの点でまだ不十分である。特に、現行の制度には GDPR のような監視機関が存在せず、認定団体になることを奨励する「インセンティブ規定」も欠如している。今後、この問題にどのように対処することが重要な課題となる。

第5章 監視に関する規制の構築とその手法

第1節 議論のまとめ

使用者による監視⁵²⁴は、労働者の行動を継続的に把握することにより、労働者のプライバシー・人格権を侵害し、そのストレスを増加させるデメリットがある一方で、例えば、労働者の疲労度を測る目的で従業員が使用するキーボードの動きを監視し、必要な場合には休憩を取るように労働者にメッセージを送ることによって、従業員の健康状態を見守ることができるというメリットもある（当然、使用者も安全配慮義務を果たすことができる）⁵²⁵。このように、監視そのものはメリットもあることから、それ自体を敵視することは適切でなく、監視に関する議論の焦点は、使用者が適正な監視を行えるようにするための判断枠組みをどのように構築するかに置かれるべきである。では、これまでの日本の裁判例において、このような判断枠組みは構築されているのか。この点について、第1章の検討から明らかなように、裁判例では、所持品検査の問題以外、監視に関する明確な判断基準は確立されていないが、裁判所は監視装置の利用に対して全く審査していないわけではない。例えば、監視を通知する前の使用者の通知義務という事実を重視した事件（セコム事件〔プライバシー侵害に基づく損害賠償請求事件〕）、より個人の権利を侵害する度合いが低い手段があったかどうかを重視したもの（目黒高校事件〔解雇事件〕）、監視装置の相当性を重視したもの（奥道後温泉観光バス（配車差別等）事件〔プライバシー侵害・不当労働行為に基づく損害賠償事件〕）などがある。しかし、これらの判決はケースバイケースの判断をしているにとどまり、そこから監視の適法性に関する一般的な判断基準を導き出すことができない状況にあった。加えて、監視に関する裁判例では、監視を個人情報取得の一形態とする意識がまだ不十分である。

一方、学説では、行政解釈の内容に基づき、監視を行う前に使用者は労働

⁵²⁴ 本論文では、監視を、「形態または手段を問わず、使用者が勤務時間に（必要であれば勤務時間外においても）、労働者の業務遂行の状況を確認し、プロファイリング等を通じて業務状況を向上させる目的、または職場の安全衛生、財産を保護する等業務に関連する目的で、従業員の行動、情報を観察・収集することである」と定義している。

⁵²⁵ 大内伸哉『人事労働法－如何にして法の理念を企業に浸透させるか』（弘文堂、2021年）279頁。一方、労働者のキーボードを監視することで、労働者の生産性が低下したり、不正行為（会社の記録を盗むなど）を行ったりする場合に、労働者に警告を発するという使い方もある。R.A Bales & K. V.W Stone, *supra* note 12, p.16.

者に監視に関する詳細な情報を提供する必要があるという見解⁵²⁶、電子メールの私的利用を監視する際に、監視の必要性や目的といった要素からなる判断枠組みが必要であるとする見解⁵²⁷、GPS 機能付き装置を利用する際に従業員の同意と情報提供を求めるとする見解⁵²⁸がある。これらの見解は、上記監視に関する判決の問題点、つまり、監視は個人データの収集にあたるという観点が欠けていることを認識し、情報収集の段階での従業員の同意や通知などの規制を求めているが、監視に関する全体的な問題については本格的な研究はなされておらず、議論は低調であった。また、個人情報保護法は、監視の問題に適用しうる法律ではあるが、労働関係における固有の要請に対応できるものではなかった（第1章第2節第3款参照）。このように、日本では、労働者の監視の適法性について、明確な法的ルールがない状況にあった。その結果、使用者は、デジタル技術が発展するなか、ますます高度化する監視を、明確な行為準則がないままに進めることになる。たしかに、現行法でも、監視によるプライバシー侵害が認められれば、使用者には損害賠償責任が発生するし、プライバシーを侵害するような監視により得た情報に基づき人事上の措置（解雇や懲戒処分など）をとれば、その有効性を問うことはできる。しかし、こうした事後的な処理は、前述のように、明確な判断基準がないなかでのケースバイケースの処理であり、今後、企業内の人事監視における監視の重要性が高まっていくなかでは、こうした状況を放置することは適切ではない。すなわち、ここで求められるのは、使用者による労働者の監視がどのような場合に適法とされるのかについての明確性の高いルールが設けられ、それが使用者への行為準則として機能することである。

加えて、ますます高度化する監視装置、特に、AI を搭載した監視装置の規制に関しては、これらの装置を利用する企業は公的機関よりも、豊富の情報量を有していることが多いことを踏まえると、適正な監視を実施できる判断枠組みを構築することに関しては、法律（国家規制）がその内容を直接規制するのではなく、技術革新の有用性に十分配慮しつつ、労働者の権利を保護できる規制手法が求められる。

⁵²⁶ ①砂押・前掲注 22) 67 頁。

⁵²⁷ 藤内・前掲注 63) 102 頁。

⁵²⁸ ①竹地・前掲注 92) 92-94 頁。

第2節 共同規制の概念を用いた適正な監視を行えるようにするための判断枠組みの構築

第1款 欧州人権裁判所とフランス法上の判断枠組みからの示唆

前述したように、適正な監視を行えるようにするための判断枠組みを構築することは、監視を検討する上で最も重要なことである。第2章の人権裁判所の状況と第3章のフランスの状況は、このような判断枠組みをどのように構築すべきかを考える上で参考になる。

第2章で検討した人権裁判所の判例法では、まず、Halford 事件判決は、監視を行う前に使用者が従業員に通知することを求めており、次に、Köpke 事件（決定）は、監視の適法性を審査するにあたって考慮すべき具体的な要件（監視の対象者、監視の期間・範囲など）を示した。最終的に、Bărbulescu 事件で、大法廷はこれまでの監視に関する判例法の内容を要約し、適正な監視を実施できるための6つの要件（事前通知の有無、私生活に対する侵害の程度、監視を行う正当な理由の有無、代替可能性の有無、監視によって得られた結果の利用結果、侵入的な性質を有する監視の場合、従業員に適切な保護措置が提供されたかどうか）からなるバルブレスク基準を確立した。この基準は、ECHR の締結国の国内裁判所に大きな影響を与え、現在では欧州諸国の裁判所が適正な監視を判断するための実質的な判断基準となっている。また、同基準が世界中の学説で大いに注目されている。その理由は、同基準が、欧州諸国の国内裁判所だけでなく、締結国の企業に対しても、間接的に就業規則などを同基準に沿うように修正することを要請していることである。さらに、López Ribalda et al. v. Spain 事件において、大法廷はバルブレスク基準の事前通知要件を絶対的要件から相対的要件に変更した。この点については、すでに第2章で検討したように、同事件は悪質性の高い集団犯罪であったため、例外かつ特殊なケースとして解釈されるべきであると解する学説が一般的である。実際、後の Florindo de Almedia Vasconcelos Gramaxo v. Portugal 事件判決では、事前通知要件を再び絶対的要件に変更した。以上を踏まえると、人権裁判所が構築したバルブレスク基準は、これまでの人権裁判所の判決の判断に基づいて形成されたものであり、監視が違法であるかどうかを判断する基準であるだけでなく、適正な監視を行うことを可能にするための明確な基準を使用者に提供するものでもある。

第3章で検討したフランスの状況には、上記人権裁判所のバルブレスク基準と同様に、監視の適法性を判断するための判断枠組みがある。破毀院の判例

法理では、主に L.1121-1 条に基づく比例性の審査と L.1222-4 条に基づく事前通知の要件（従業員に事前に通知していない装置を利用して、労働者の個人情報収集してはならない）に基づいて監視の適法性が審査されている。また、破毀院の判例法理の分析から明らかなように、L.1121-1 条は従業員の自由と権利を保護するための「憲章」と理解されているため、従業員の自由が著しく侵害される場合（例えば、労働者の行動を継続的に撮影するような場合⁵²⁹）を除き、破毀院は通常、L.1222-4 に定められている事前通知の要件のみを審査する。また、破毀院の判例法理のもう一つ特徴は、使用者が負う事前通知義務はあらゆる場合に発生するわけではなく、従業員の業務遂行を監視する場合にのみこの義務を課している点である。また、監視の適法性に関する判断枠組みは、前述した破毀院だけでなく、情報と自由法の規定に基づいて監視に関する種々な命令や勧告を策定した CNIL の役割も非常に重要である。このように、フランスでは、使用者による監視に関する具体的な判断枠組みが、破毀院とテクノロジーの発展に精通した CNIL が緊密な協力関係によって形成されてきた。

以上の比較法的検討の結果から、次のような示唆を得た。まず、日本にはまだフランスと人権裁判所のような適正な監視を行えるようにするための判断枠組みがなく、個人情報を所管する個人情報保護委員会の、職場の監視問題への関与もまだ少ないことから、現状では使用者が適正な監視を実施することは非常に困難である。この問題を克服するために、日本も適正な監視を行えるようにするための判断枠組みを導入すべきであると考えられる。では、どのような判断枠組みを導入すべきかが重要な問題となる。結論を先取りすれば、日本の現状に鑑みれば、人権裁判所のバルブレスク基準を導入する方が適切である。その理由はいくつかある。まず、上記フランスの判断枠組みでは、破毀院が使用者に課している事前通知義務を除き、新たな技術から生じる問題に対処する規制のほとんどは CNIL が定めている。監視を情報収集の一態様として明確にした点と、司法機関と CNIL の協力による監視審査の枠組みの確立は、日本にとって示唆に富むものであるが、利用目的中心主義⁵³⁰に基づく日本の個人情報保護法とフランスの情報と自由法には構造的に大きな相違があり、また、すでに監視に関する多くの命令と指針を持っている CNIL とは異なり、発足以来 10 年まだ経っていない日本の個人情報保護委員会が

⁵²⁹ See case *supra* note 378.

⁵³⁰ 第 1 章第 2 節第 3 款参照。

CNIL と同等の役割を果たすことは困難である。したがって、日本に適正な監視を行えるようにするための判断枠組みを導入する際、フランスの方式は必ずしも最善の方法ではないと言わざるを得ない⁵³¹。また、破毀院の判例法理（事前通知義務）のみを日本に導入する意義もさほど大きくないと考えられる。というのも、上記の破毀院の判例法理は、通知の内容について監視の「存在」のみを求めているだけであり、この要件は日本の個人情報保護法 21 条ですでに実現されているからである。これに対して、人権裁判所は、通知内容に関して、監視装置の存在だけでなく、「使用者が行う監視の範囲と性質及び、使用者が通信の内容に直接的にアクセスできる可能性」を含むものを要請している⁵³²。また、バルブレスク基準で定められている要件は、これまでの日本の裁判例では前例がないわけではなく、むしろ既存の判断を統合しつつ、一部新しい要件を追加しているものである⁵³³。したがって、立法論としては、使用者が適正に監視を実施できるようにするために、バルブレスク基準を導入（以下では、日本型監視の適法性に関する判断枠組みと呼ぶ）すべきである。

第 2 款 共同規制方式による規制内容の具体化

バルブレスク基準を参考にした日本型監視の適法性に関する判断枠組みは、監視を実施する企業が、規制の具体的な項目（事前通知の有無、私生活に対する侵害の程度、監視を行う正当な理由の有無、代替可能性の有無、監視によって得られた結果の利用の結果、侵入的な性質を有する監視の場合、従業

⁵³¹ 組織の職員数に関して、2023 年の人口が約 6,700 万人のフランスでは、CNIL の定員は 270 人、人口が約 1 億 2,000 万人の日本では、個人情報保護委員会の定員は 2023 年には 220 人（2022 年には 195 人）にすぎない。

⁵³² See case *supra* note 207, §133. また、拘留室で監視カメラによって撮影されたことが ECHR 8 条に違反したかどうか争われた *Perry* 事件において、人権裁判所は、「申請者が拘留室で作動している監視カメラを認識していたかどうかは別として、申請者が、上記監視カメラによる身元確認手続に使用する目的、および裁判での弁護に不利な証拠となる目的、警察署内で自分の映像が撮影されていることを予想していたことを示す証拠はない」とし、単に監視カメラの存在だけでなく、申請者は当該カメラによって得られた証拠がどのように使用されるかを予測できる必要があると判断した。Perry v. United Kingdom, (App.63737/00), 17 July 2023, (2004) 39 EHRR 76, ECHR 2003-IX.

⁵³³ また、民事事件では、労働事件には見られない、監視カメラの録画の管理方法と保存期間を審査する事件が多くある。例えば、東京地判平 22・9・27 判タ 1343 号 153 頁や東京地判平 27・11・5 判タ 1425 号 318 頁や東京地判平 31・3・14LEX/DB25559868 などがある

員に適切な保護措置が提供されたかどうか)をある程度予測することを可能にするが、この判断枠組みだけでは、規制の具体的な内容は依然として不明確なままである。例えば、具体的にどのような内容を通知要件に含めるべきかは明確ではなく、また、侵入的な性質を有する監視の場合、従業員に適切な保護措置が提供されたかどうかという要件の「適切な保護措置」も明確ではない。加えて、AI など新たな技術を搭載した監視装置については、それを利用する企業は公的機関よりも当該装置に関する豊富な知識と情報量を持っている場合が多いため、日本型監視の適法性に関する判断枠組みの内容に産業団体が関与することは重要である。

以上の問題に対処するために、第4章で検討した共同規制の概念に基づく行動規範と認定団体の制度を用いることが有用であると考ええる。この点について、すでに第4章で検討したように、GDPR上の行動規範と個人情報保護法上の認定団体制度は、各産業団体の分野の特性を考慮しつつ、広範かつ不明確な法規定を明確化できるという利点がある。両制度におけるこのような利点は、日本型監視の適法性に関する判断枠組みにも応用できると考えられる。第4章で取り上げたCNILが示した具体例のように、監視カメラの設置場所、向きや画像の保存期間などを具体的に行動規範に定めることで、行動規範に加盟した事業者が利用する監視カメラはGDPR上の規制を遵守することとなる。実際に、顔認識機能を搭載しない従来型防犯カメラが「利用目的が明らかであると認められる（個人情報保護法21条4項4号）」という例外な場合に該当しても、法的紛争を回避し、消費者の信頼を得るために対象事業者に通知義務を要求することが規定される保護指針が見られる。

また、共同規制の観点から、日本の認定団体制度はGDPRの行動規範の制度と比べ、まだ不十分な点が多いが、個人情報保護法では、認定団体の資格や保護指針の作成などの段階に個人情報保護委員会が関与することから、少なくとも日本型監視の適法性に関する判断枠組みの内容が企業だけに決定されることはなく、公的機関による審査の仕組みも保障されている。加えて、まだ法的拘束力のない個人情報保護委員会の最新の見解を取り入れつつ、新たな技術に適応した判断枠組みを構築できるということも利点である⁵³⁴。こ

⁵³⁴ 例えば、使用者による監視に関するこれまでの判例では、使用者が労働者に事前に通知することなく監視機器を使用したことを違法としたものはないが、個人情報保護委員会が策定した最新の「顔識別機能付きカメラシステムに関するガイドライン」においては、事前通知なしに監視カメラの利用は同法20条1項に違反するとの見解が示されている。前掲ガイドライン512) 38頁。

のように、本論文で主張する日本型監視の適法性に関する判断枠組みは、固定的かつ不変的なものではなく、むしろ前述したバルブレスク基準を土台とし、新たな技術に対応する個人情報保護委員会等の意見⁵³⁵を不断に取り入れながら、その内容を補充するものである。加えて、行動規範と認定団体の保護指針の策定にあたっては、マルチステークホルダプロセスが要求されていることから、日本型監視の適法性に関する判断枠組みの内容を決定する際、従業員や労働組合の意見が適切に反映されることが重要である。

したがって、本論文では、日本型監視の適法性に関する判断枠組みの具体的な内容を決定するにあたっては、各産業団体実態の相違や、監視手段が急速に発展していることなどを考慮し、法律という形で硬直的に定めるのではなく、産業団体と公的機関が継続的に協力しつつ、共同規制の方式によってその内容を決定していくことが適切であると主張する。

第3款 労働者の同意と日本型監視の適法性に関する判断枠組みとの関係

一般的に、労働者の同意は強力な規制と考えられており、日本の学説の中でも、使用者が監視を実施する際に、労働者の同意を得る必要があると主張する見解がある⁵³⁶。しかし、以下の点から、労働者の同意を日本型監視の適法性に関する判断枠組みに組み入れることは適切ではないと考えられる。まず、遠因としては、比較法的観点から、監視を実施する際に、労働者の同意を前提条件とする国は見当たらない。人権裁判所の調査によると、欧州評議会の加盟国における監視に関する大半の法律は、明らかに「行き過ぎた」監視（トイレや休憩室などの場所に監視カメラが設置されている場合や、監視カメラで従業員を間断なく直接撮影する場合など）それ自体を禁止しているか、あるいは監視装置を使用する前に労働力または労働者代表に通知する義務を使用者に課しているという⁵³⁷。ドイツでは、事業所組織法は、監視カメラを

⁵³⁵ 例えば、前述のQ&A5-7では、使用者が監視に関する事項を定める場合には、従業員個人への周知と事前に労働組合等の組織に通知し、必要に応じて協議を行うことが望ましいということに加え、「①モニタリングの目的をあらかじめ特定した上で、社内規程等に定め、従業員に明示すること、②モニタリングの実施に関する責任者及びその権限を定めること、③あらかじめモニタリングの実施に関するルールを策定し、その内容を運用者に徹底すること、④モニタリングがあらかじめ定めたルールに従って適正に行われているか、確認を行うこと（番号は筆者による）」と規定されている。

⁵³⁶ ①竹地・前掲注92) 92頁。

⁵³⁷ See case *supra* note 207, §52-54, See case *supra* note 235, §67-70.

利用する前に使用者と事業者委員会の共同決定が義務付けられているが（同法 87 条第 1 項 6 号）、この共同決定は絶対的なものではなく、共同決定について合意に至らない場合、仲裁委員会（Einigungsstelle）の判断に委ねることとなる（同法 85 条）⁵³⁸。したがって、監視の導入に共同決定を義務づけている上記ドイツの事業所組織法においても、労働者の個別同意は要求されていない。一方、近因としては、日本の学説と前述 EDPB と WP29 が強調しているように、労使間の交渉力の格差と情報の非対称性から、労働者の同意が「真意に基づくもの」であることを証明する困難であるという点⁵³⁹、監視装置の機能が高度化している中で、労働者が監視の目的と収集された情報を利用する結果（特に、AI による分析の場合）を理解することが容易ではないなどの観点から、労働者の同意を求める意義は必ずしも大きいとは言えない⁵⁴⁰。なお、この点に関しては、情報学と憲法学の議論を参照できる。情報学者の松前恵環は、デジタル時代における同意の意義と有効性に疑問を呈し、「単に同意の要件や取得手続を厳格化することは必ずしも情報主体の実質的な意思の反映につながらないおそれもあるため、事業者や情報主体の負担を考慮し、規制の程度を慎重に調整することが不可欠である。また、実質的な同意の確保が困難な現状では、これを実現し得る「環境」を整えることが特に重要である」という重要な点を指摘した⁵⁴¹。また、憲法学の山本龍彦も、デジタル時代におけるプライバシー保護は、個人の同意を求めるよりも、構造的な判断枠組みを通じて審査される必要があると主張している⁵⁴²。

このように、労働法学（労使間の交渉力の格差、情報量の非対称性）、情報学（同意の環境論）、憲法学（構造審査論）の視点を参考にし、本論文で主張

⁵³⁸ L. Middel (trans P. Skidmore), Workplace surveillance in the light of employee data protection, 2019, pp.4-5. available at https://opus4.kobv.de/opus4-euv/frontdoor/deliver/index/docId/462/file/Middel_Lukas_Workplace_surveillance.pdf.

⁵³⁹ また、従業員の所持品検査が違法であるかどうかが争われた前掲のコスモアークコーポレーション事件判決（大阪地判平 25・6・6 前掲注 37）は、所持品検査に対する労働者の同意の有効性について、「雇用契約上の上下関係を背景に、財布や通帳の点検をされると言われた場合、抵抗することなく点検に応じたからといって、真摯な同意があったと認めることは相当でない」とした。

⁵⁴⁰ また、GDPR 6 条において、同意はデータ処理の一つの適法性根拠として挙げられているが、労使の力の不均衡の観点から、同意を監視実施の適法性根拠とすることはできず、同条 6 条 (f) に規定されている使用者の正当な利益を根拠とすべきとする見解が多い。例えば、Komanovics, *supra* note 182, p. 460.

⁵⁴¹ 松前恵環「個人情報保護法制における「同意」の意義と課題」NBL1167 号（2020 年）26 頁。

⁵⁴² 山本龍彦「プライバシーの権利」ジュリ 1412 号（2010 年）81-82 頁。

するような日本型監視の適法性に関する判断枠組みを構築する際に、労働者の同意要件を組み込むことは適切ではないという結論を得た。これは、決して労働者の同意を軽視するものではないが、明確性のある日本型監視の適法性に関する判断枠組みが確立される前に真意性の判断が極めて難しい労働者の同意の有無を求めることは、監視から労働者のプライバシー権等の人格的利益を保護するという目的を達成できない恐れがある。とりわけ、新たなデジタル技術を活用した監視に関して労働者の判断能力に限界がある場合、労働者の同意を求める意義は大きく減殺されていると言える。もっとも、日本型監視の適法性に関する判断枠組みが導入された場合には、労働者の同意は、監視装置に対する従業員の信頼を得るための「グッドプラクティス」として位置づけられることができると考える。

結章

監視は、労働という概念が誕生したときから存在し、監視手段の変容は、中世都市における親方（*maître*）の監視から、18 世紀の工場主による監視、そしてデジタル時代におけるアルゴリズムによる監視（バーチャル監視）に至るまで、テクノロジーの発展とともに変容してきた。このような変容のなかで、監視は次第に舞台裏に潜むようになり、労働者がその存在を察知することが困難になっている一方で、その範囲は個人の言動を四六時中監視できるまでに拡大し、さらにデジタル技術を活用した監視は、従業員の行動を撮影・録画するだけでなく、それによって収集した従業員の個人データを AI で分析し、得られた推知情報（プロファイリング）と従業員本人から提供された情報を混合し、個々の労働者のプロフィールを作成するという新たな機能を有するという点である。従来の監視とは一線を画している。このように、デジタル技術を活用した監視を検討するにあたっては、従来の労働法上の固有の観点だけでは足りず、個人情報保護の観点も視野に入れる必要がある。

裁判例上、プライバシーの権利の侵害をめぐる判決とは異なり、監視に関する従来の判決は、監視を情報収集の一形態としてとらえることはなく、主に監視装置の目的や設置場所といった観点から審査している。一方、学説上、情報収集段階に規制を加える必要があることを意識したいくつかの見解は、監視実施前の使用者による通知や従業員の同意といった要件を求めている。これらの見解は裁判例及び現行法以上の要件を課す点において重要な意義を有するが、こうした要件だけで新たな監視装置に効果的に対処できるか否かは疑問である。この点、デジタル時代における同意の有効性に疑義を呈し、アーキテクチャのような構造的審査や環境の整備に重点を置くべきであると主張する憲法学と情報学上の見解が示唆したように、デジタル技術を活用した監視装置に対しては、労働者の判断能力に限界があり、同意要件の意義が形骸化するおそれがあることを考慮すると、監視に関する判断枠組みによる規制を構築することがより適切であると考えられる。このような判断枠組みがどのように構築されるかについては、第 2 章の人権裁判所によって確立されたバルブレスク基準と、第 3 章のフランス法における CNIL と破毀院の緊密な協力というアプローチを参照できる。この点、第 5 章で検討したように、本論文では、バルブレスク基準の導入は日本の現状に照らして最も妥当であるが、同基準の導入は使用者が適正な監視を実施できるように誘導するための第一歩に過ぎないと主張している。今後より重要になるのは、バルブレス

ク基準を参考にして構築された日本型監視の適法性に関する判断枠組みの内容をどのように明確化し、新たな技術に適応できる内容で補完していくかことである。

また、公的機関が一方的に日本型監視の適法性に関する判断枠組みの内容を決定することは、硬直的な規制や技術の発展に適応しない規制をもたらす問題があるため、公的機関だけでなく、企業側の関与を重要視する必要がある。この関与を可能にしたのは、第4章で検討した共同規制の手法に基づくGDPRの行動規範と、日本の認定団体の制度である。実際、すでに検討したように、個人情報保護委員会による公式見解がまだ存在しない場合、または見解の内容自体が不明確な場合、認定団体は、その欠如や不明確を補う重要な役割を果たしている状況が見られる。さらに、認定団体の保護指針と行動規範は公的機関と産業団体が協力して策定されるだけでなく、その策定にはマルチステークホルダープロセスが要請されている。これによって、行動規範と保護指針の策定における透明性やメンバーの信頼関係を高めることができ、さらに重要な点として、労働組合等の意見をプロセスに反映させることもできる。

最後に、すでに問題所在で述べたように、監視は労働者の人格権やプライバシー権の侵害といったマイナスな面だけでなく、労働者の安全や健康状態を見守る側面もある。また、監視を情報収集の一態様として、適正な監視によって取得された従業員に関する情報をAIで分析することで、労働者の適材適所の実現や、これまで人間が気づかなかった問題点を示すことが可能となる。このように、監視の問題はデジタル時代における新技術がもたらす問題と同様、その評価は使い方次第であり、それゆえ、監視それ自体を敵視すべきではなく、むしろ如何にして使用者が適正な監視を行えるようにするための判断枠組みを整備することに重点を置くべきであろう。

以上の検討から、今後、デジタル技術を活用した監視をどのように規制していくかを考える上で、本論文で主張した共同規制の手法を用いた日本型監視の適法性に関する判断枠組みの構築が必要不可欠であるという結論を得た。なお、すでに述べたように、日本型監視の適法性に関する判断枠組みは硬直的で固定的なものではなく、その具体的な内容は技術の発展に適応できるものでなければならないため、今後、職場における監視を含む情報処理の問題については、個人情報保護の分野に精通している個人情報保護委員会の見解を引き続き注視していく必要がある。