翻　訳

「オンライン捜索」についての連邦憲法裁判所判決(1)

――二〇〇八年二月二七日第一法廷判決――

アルプレヒト・レスラー
鈴木秀美／訳

一　イントロダクション――一般的人格権

ドイツでは、一九七〇年代にデータ処理の際の個人データの保護のための立法が始まった。州では、一九七〇年のヘッセン州をかわきりに州データ保護法が発効し、一九七七年に連邦データ保護法が発効した。

一九八三年の国勢調査に関する連邦憲法裁判所の判決が、データ保護法のその後の発展に指針を与えた。「国勢調査判決」(2)において、連邦憲法裁判所は、情報自己決定についての主観的権利を保障した。連邦憲法裁判所は、この権利を（基本法一条一項と結びついた二条一項の）憲法上の一般的人格権の直接の刻印であると考えている。それによると、各人は、自己に関するデータの放棄や利用について原則として自ら決める権利を有する。コミュニケーション技術の急速な発展（デジタル化）は、個人データを簡単に把握し、処理し、提供することを可能にし、そ

れによって私的領域にとっての潜在的危険を高めた。私たちは、それがどれくらい危険なものかを、いまだ見通すことができない。このため、まさに最近になって、データ保護についての連邦憲法裁判所の重要な幾つかの判決が下された。例えば、二〇〇八年には自動車のナンバーの自動読み取り機についての判決や、通信記録の保存（Vorratspeicherung）についての仮命令が下されている。(3) ただし、本日はこれらの判決に言及することはできない。

ここでは、公法上の一般的人格権の根拠が基本法二条一項と、補足的に一条一項にあるということを再度指摘しておくことが有益である。(4) 一般的人格権は、連邦憲法裁判所によれば、基本法の個々の自由の保障対象ではないが、その構成的な意義は劣らない、人格の要素を保護することを保障する。(5) その防禦機能において、一般的人格権は、直接に国家に対して適用される。この点が、私法上の一般的人格権との違いである。私法上の一般的人格権は、既に一九五〇年代に連邦通常裁判所の判例によって裁判官による法形成に基づいて導入された。私法上の一般的人格権は、抽象的に保護された権利である。すなわち、この権利は、誰に対しても、そして、他の抽象的な法益（生命、健康、財産等）と同様に、第三者によるその侵害および違法な介入から保護される（民法典八二三条一項、一〇〇四条一項）。私法上の一般的人格権の法源は直接憲法にあるのではなく、原則として立法者の意のままになる。一般的人格権は、憲法上の権利であれ、私法上の権利であれ、今日のメディア市場においては（データ保護も含めて）、非常に重大な意義をもっている。一般的人格権は、判例により、時の経過にともない、一定の形態（「小グループ」）によって具体化されている。憲法上の一般的人格権の分野では以下のような形態が認められている。(6)

――内密領域、私的領域、秘密領域の保護

――人格的名誉権

――自己の人格の外部に対する描写についての決定権

――肖像権
――発言した言葉についての権利
――執筆した言葉についての権利
――発言の歪曲や捏造に対抗する権利
――氏名権
――犯罪との関連で無限定の報道に対抗する権利
――情報自己決定権

連邦憲法裁判所は、二〇〇八年二月二七日の「オンライン捜索」判決において、このカタログに、また新たな保護の方向性を追加した。それは、「情報技術システムの信頼性と不可侵性の保障」についての権利である。この基本権は、情報自己決定権がこれまでに及ぼしてきたのと似たような照射効を立法や法の適用に及ぼすであろう。

二　連邦憲法裁判所の「オンライン判決」の事実と概要

この度の判決は、ノルトライン・ヴェストファーレン州の憲法擁護に関する法律の個々の規定に対する憲法異議に基づくものである。憲法異議申立人は以下の通りであった。

――主としてインターネットで活動している女性ジャーナリスト一名
――さらに、「左派党」という政党で積極的に活動している党員一名。この政党は、連邦議会といくつかの州議会に議席を持つが、憲法擁護のための監視を受けている(7)。
――法律事務所を共同経営している弁護士二名。この弁護士らの依頼人にはクルド労働党の指導的な党員も含ま

れている。クルド労働党は憲法擁護のために監視されている。

憲法異議申立人らが具体的に問題にした規定は、憲法擁護庁が情報技術システム（コンピュータとネットワーク）からデータを収集する権限であり、収集したデータの行政機関による取り扱いに関するものであった。ただし、憲法異議申立人の誰からも、かつてそのようなデータの収集が行われたことはなかった。

問題とされた、データ収集に関するノルトライン・ヴェストファーレン州憲法擁護法（ＶＳＧ）の規定[8]は、憲法擁護庁の捜索手段について二つの異なる形態を含んでいた。それは、①行政機関によるインターネットの密かな監視と②情報技術システム（ネットワーク、コンピュータ）への密かなアクセスである。

密かな監視の場合、行政機関は技術的にそのために定められた方法でインターネットによるコミュニケーションの内容を把握する。すなわち、行政庁は「ネットサーフィン」を行い、例えば、誰でもアクセス可能なワールドワイドウェブ上のウェブページにアクセスする。また、行政機関は、仮名を用いて誰でもアクセス可能なチャットまたは交換掲示板（Tauschbörsen）に参加することもできる。「監視」には、行政機関がある情報提供者のパスワードを使って、「なりすまし」によって電子メールによるコミュニケーションに参加する場合も含まれる。行政機関が試行錯誤によってパスワードを見つけ出すことも監視にあたる。これに対して、二つ目の形態は、特定の情報技術システムへ潜り込むことを意味する。潜り込むこと（侵入）というのは、ある特定の情報システムの利用を監視すること、保存媒体（例えばパソコンのハードディスク）を見張ること、それどころかそのシステムを遠隔操作することも意味している。行政機関はその際、その手段として、このために自ら開発した監視プログラムを用いるか、あるいは目標となったシステムのセキュリティシステムの欠陥を利用する。この二つめの形態（アクセス）が、「オンライン捜索」（または「オンライン監視」）と呼ばれている。

「オンライン捜索」の権限には、憲法擁護法によって、以下のような要件が結びつけられている。まず、データの収集によって憲法擁護に関連する活動を認識すること、ないしそのような認識のために必要な情報源を獲得することができることが一般的に必要である。さらに、憲法擁護法によれば、信書、郵便または通信の秘密への侵害となる措置、または方法や程度がそのような侵害と同じになる措置は、信書、郵便または通信の秘密の制限に関する法律（「一〇条法」[9]）に定められた付加的な特別の要件の下においてのみ許される。基本法一〇条法は、自由で民主的な基本秩序または連邦と州の存続と安全を脅かす危険に対抗するために役立つ場合には、憲法擁護庁に電気通信の監視および録音を認めている。この法律は、さらに、郵便サービスと電気通信サービスの事業者に、憲法擁護庁に対する義務を含んでいる。前述した行政機関による制限のための要件は、――ここでは単純化して説明するが――監視対象者が、法律のカタログに列挙された特別に重大な犯罪（例えば、反逆、民主的法治国家を脅かすこと、テロ組織の設立）を計画し、遂行し、あるいは遂行したことについての嫌疑について事実上の手がかりが存在していることである[10]。その際、もちろん、すべてのその他の捜索手法が尽くされていること（最後の手段であること）が必要である。一〇条法は、さらに手続的要請も含んでいる[11]。さらに、制限措置を命じる権限は、最上級の州行政機関、さもなければ連邦首相から任命された連邦大臣にある[12]。制限措置は、それが終了した後に本人に通知されなければならない。これはもちろん、制限の目的が脅かされる可能性があるときは必要ではない[13]。これについては特別な委員会が判断する。この法律の執行については議会の監視委員会が監視を行う[14]。

ノルトライン・ヴェストファーレン州憲法擁護法は、これまでに「オンライン捜索」を明文で規定したドイツで唯一の法律であった。ただし、最近、連邦政府が連邦刑事局の権限拡大のための法案を連邦議会に提出した。それには「オンライン捜索」も含まれている[15]。この立法計画は、世間で激しく議論されている。連邦刑事局がかつて

「オンライン捜索」を行ったことが明らかになっている。それがどれくらい頻繁に行われたかは、もちろん明らかにされていない。[16] とはいえ、連邦通常裁判所刑事部が、「オンライン捜索」は刑事訴訟法の被疑者に対する捜索についての規定によってカバーされていないと判断した後、遅くとも二〇〇八年二月までに、すべてのそうした捜索措置は暫定的に中止された。[17]

三　判決理由について

1　憲法異議の適法性

ここではいくつかの観点のみに言及したい。

（1）当事者適格

連邦憲法裁判所は、インターネットの監視とオンライン捜索を定めた憲法擁護法の規定に関連して、すべての憲法異議申立人に当事者適格を認めた。連邦憲法裁判所は、基本権侵害の可能性を前提とした（「可能性理論」）。

異議申立人の女性ジャーナリストは、さらに、「個別に、金融機関において、……支払流通への関与に関する情報および金銭の動きに関する情報を」収集することができるとする憲法擁護法の規定も問題にした。[18] 連邦憲法裁判所は、この点についての憲法異議を不適法とした。なぜなら、この女性ジャーナリストは、自分が当該規定によって自己の基本権を侵害される可能性があることを明らかにしなかったからである。行政機関がこのジャーナリストの口座データに関心を持つとは認められないとされた。「左派党」の積極的な党員の場合、連邦憲法裁判所は、これとは別だと考えた。なぜなら、この憲法異議申立人は、インターネットに接続した彼のパソコンを彼の政治的活動にも使っていたからである。

（2）憲法異議の補完性

この原則によれば、憲法異議は、憲法異議申立人が期待可能な方法で通常の裁判所へ提訴することによって権利保護を得ることができる時には不適法となる。これによって、憲法裁判所が不確定な事実の基礎と法律の基礎に基づいて、すべての法共同体にとって広範に及ぶ意義のある判断を下すことが回避される。[19]

二名の憲法異議申立人は、この法律がもはや必要ではなくなった収集されたデータを行政機関が保存すると定めていることを問題にした。もちろん、憲法異議申立人らが主張するように、データ消去が本当に排除されていると、この法律から解釈によって明らかに読み取れるわけではなかった。連邦憲法裁判所は、この問題を判断したくなかったので、その点については憲法異議を不適法とした。この解釈問題をとりあえず専門裁判所に解決させるということは憲法異議申立人らにとっても受け入れられると考えられた。

（3）申立期間

一九九四年に旧憲法擁護法に採用された規定によれば、憲法擁護庁は、厳密な要件の下で、住居内で話された言葉を技術的手段によって密かに傍受し、記録することができる。[20] 二人の憲法異議申立人はこの規定も問題にした。連邦憲法裁判所は、この主張を期間経過後にされたものと判断した。法令に対する憲法異議の申立期間は、当該法律の施行後一年である。[21] 連邦憲法裁判所は、確立された判例を通じて、問題とされた規定が改正の枠内（憲法擁護法は二〇〇六年に改正された）で受け継がれた場合にもこの本来の期間が妥当することを確認してきた。旧規定の申立期間は、改正によってスタート地点に戻らなかった。[22]

2　憲法異議の認容性

専門家にとって連邦憲法裁判所が「オンライン捜索」に関する憲法擁護法の規定を違憲としたことは驚きではなかった。これに対し、連邦刑事局法の改正のための最近の企図との関係では、大きな緊張とともに、連邦憲法裁判所の「オンライン捜索」の要件についての判断への期待が高まっていた。いわゆるリモート・フォレンジック・ソフトウェア・ツール（「連邦の木馬」、「バックドアの木馬」）を用いることを、連邦政府、連邦刑事局、秘密情報機関[23]は、テロとの戦いのための不可欠の手段とみていた。

（1）「情報技術システムの信頼性と不可侵性の保障」についての基本権――保護領域

連邦憲法裁判所は、憲法上の人格権の継続形成と解する新しい基本権（基本法一条一項と結びついた二条一項）を提供した。それは、「情報技術システムの信頼性と不可侵性の保障」についての権利である。

この主観的権利は、その保護が他の基本権によってすでに保障されていないその範囲で、情報技術システムへの侵害からの保護を与える。既存の基本権としては、とくに信書、郵便、通信の秘密（基本法一〇条）、住居の不可侵（基本法一三条）、情報自己決定権（一般的人格権の形成）がある。

連邦憲法裁判所は、最初に、情報技術における近年の発展によって、情報技術システムが今日ではすべての生活領域において――とりわけ私的な日常における生活の形成の際にも――ユビキタスなものとなり、人格の発展にとってますます重要な意義を獲得していると確認する。連邦憲法裁判所は、ここから、人格にとってのチャンスと、しかしまたまったく「新しいかたちの危険」が生じることを強調する[24]。コンピュータがユビキタスなものとなったことにともなう潜在的危険は、以下の観点から明らかとなる。

――情報技術システム（私的なパソコンも）には、今日、多様な利用可能性がある。それは、個人データの作成、

処理、保存と結びついている。当該データから、「利用者のプロフィール」が作成され、当事者の人格を逆推論することが可能になる。

――こうした「利用者プロフィール」が権限無く第三者によって収集される危険は、情報システムのますます複雑な網目状の結合（例えば、インターネットを介して）によって、ドラマチックに拡大した。こうして、個人データの見張りまたは操作のためのアクセス可能性が生じた。このような侵害に対して、本人が自己防衛できるのは限られた場合だけである。

このように特殊な、かつては未知だった危険から、基本権上の、重要な保護の必要性が生じる。連邦憲法裁判所は、憲法上要請されている、人格権の完全な保障に基づいて、補足されるべき保護の欠如を認識している。「情報技術システムの信頼性と不可侵性の保障」についての基本権はこれに役立つ。

もちろん、すでに伝統的に認められてきた基本権保障の観点から、保護の欠如の承認が本当に説得的なものか否かも問題となる。そこで、以下では、基本権競合の問題を詳しく論じることにしたい。

(a)　情報自己決定権との区別

前述の通り、情報自己決定権は、個人に、自己データの放棄および利用について決定する権限を保障している。これに対して、――連邦憲法裁判所も述べる通り――情報技術システム利用者の法的に保護された利益は、私的領域のデータに限定されない。そのようなシステムの複雑さが、私的なデータと、非私的なデータの明確な区別をしばしばほとんど不可能にする。連邦憲法裁判所によれば、「データ自身からは、それが本人にとってどのような意義をもち、他の文脈と結びつけることによりどのような意義を獲得できるか、読み取れない」[25]。

ある情報技術システムへの侵入によって、すべてのデータへのアクセスが可能になる。そこから、利用者の「全

体像」が明らかになりうる。ここに、特別な、人格に関連する潜在的危険がある。連邦憲法裁判所は、同時に、新たなひとつの法概念を生み出した。それは、「情報技術システム」である。連邦憲法裁判所が述べるように、この新しい基本権の保護領域によって把握されるのは次のような情報技術システムだけである。それは、「単独で、あるいはその技術的（網目状の）結合の中で、当事者の個人データを一定の範囲および一定の多様性において含むことができるシステムである。そこでは、システムへのアクセスが、ある人物の生活形成の本質的な部分を覗き見ることを可能にするか、あるいは人格の印象的なイメージを獲得することを可能にする」。このようなシステムとして典型的には、デスクトップパソコン、あるいはモバイルパソコンがある。それが、私的にあるいは仕事で使われているかは問題ではない。さらに、携帯電話または電子手帳もある。(26)

新しい基本権の保護法益は、情報技術システムによって生み出され、処理され、保存されたデータの信頼性についての利用者の利益である。保護する価値のある信頼性と不可侵性への期待は、当事者が、その情報システムを自己のものとして利用していることを前提としている。なぜなら、――連邦憲法裁判所も抑制的なのだが――そのような場合にのみ、当事者は、彼がシステムを媒介として、単独または他の利用資格のある人物とともに、自己決定的に利用するということを前提とすることができる。(27)彼の情報技術システムが、彼には利用権限のない他の情報技術システムと網目状に結合する場合、保護領域は、この別のシステムにも拡大する。

基本権への侵害は、とくに、情報技術システムへの密かなアクセスの場合に生じる。この「アクセス」は、それによって第三者がそのシステムの能力、機能、保存内容を利用する技術的可能性が生じるという点に特徴がある。永続的に保存されたデータだけでなく、単に一時的に保存されたデータ（ハードディスク、作業用メモリー）も保護されている。例えば、データ処理プロセスが、ハードウェア・キーロガー（Hardware-Keyloggern）(28)の利用によ

って把握される場合、またはデータ収集が、コンピュータのディスプレイないしキーボードの電磁信号の測定によって行われる場合にも、アクセスが認められる。

要約として、連邦憲法裁判所の判決文を引用することにより、情報技術システムの信頼性と不可侵性の保障についての基本権なくしては明らかにはならなかった保護の欠如を指摘したい。

「情報自己決定権は、個人が、自己の人格の発展のために情報技術システムの利用に依存していること、そしてその際にシステムに個人データを任意に、あるは強制的に提供することから生じる人格にとっての脅威を十分には考慮に入れていない。（第三者の）アクセスの当事者の人格にとっての深刻さは、情報自己決定権がそれに対抗して保護している、個々のデータの収集の場合をはるかに超える」[29]。

(b)　電気通信の秘密との区別

（基本法一〇条の）電気通信の秘密は、電気通信による交流を用いて、情報が個々の受信者に無形のまま伝達されることを保護する（すなわち、インターネットにつながることで行われる情報技術システムを解した遠隔コミュニケーションもそれにあたる）。基本法一〇条は、これに対して、情報技術システムの信頼性と不可侵性を保護していない[30]。国家による監視措置が、コンピュータネットワークにおいて現に行われている電気通信の内容と範囲を収集し、収集されたデータを分析することに限られているその範囲内であれば、連邦憲法裁判所は、電気通信の秘密のみを審査するであろう。言い換えれば、保護の欠如がなければ、情報システムの信頼性と不可侵性についての基本権を援用することはできない。

しかし、行政機関による監視が、情報技術システムそれ自体に関連している限り（すなわち、現に行われているコミュニケーションの範囲外の内容に）、電気通信の秘密の適用可能性がないため、情報システムの信頼性と不可

侵性についての基本権が適している。これは、「オンライン・アクセス」によって収集されたデータが電気通信網を介して行政機関に伝達される場合にも妥当する。

ここで、通信の秘密の保護領域についていくつか具体的な説明をしておきたい。

通信の秘密は、通信行為が終了した後の時間帯に、通信の当事者の支配する領域に保存された内容と状況を保護していない。この場合は、当事者が、密かなデータへのアクセスに対抗する自己防衛策をとることができる。なぜなら、そこでは、連邦憲法裁判所の見解によれば、第三者によって秘密を把握されるところにある遠隔通信に固有の危険は存在しない(31)。

連邦憲法裁判所がさらに強調するように、通信の秘密によって保護されているのは、ある個人の関与した通信が、第三者によって認識されないことについてのその当事者の信頼である。これに対して、この［新しい基本権による］保護は、通信当事者間の信頼性、とりわけその特定性についての観念には関連していない(32)。例えば、閉鎖的な「チャット」のある参加者が、憲法擁護庁に任意に、アクセスキーを委ねたとき、行政機関はその権限によって当該通信に関与する。ここでは、当事者は、通信の相手方の同一性についてのみ欺かれているため、通信の秘密の保護領域への侵害は生じない。これは、当事者が一般にアクセス可能なウェブページまたは開放されたディスカッションフォーラムを覗き見る場合にまさに妥当する。もちろん、行政機関が、通信当事者の意思がないのに、またはその意思に反して、通信へのアクセスを行った場合なら、事情は異なる。すなわち、例えば、電子メールボックスや閉鎖的なチャットをみるためにキーロギング（Keylogging）によってアクセス権を獲得した場合である。ここでは、通信の関与者によって、通信の秘密が無権限に侵害される。

(c)　住居の不可侵の権利との区別

基本法一三条一項において保障されている基本権は、私生活にとっての空間を保護するためのものである。「住居」の概念は、私的空間だけでなく、仕事のための空間を含むことができる。保護の効果は、物質的な侵入からの保護に限定されない。保護領域にとって問題となるものとして、例えば、音声および視覚による住居の監視[33]または住居内の情報技術システムの利用によって外部から監視される電磁信号の測定がある。基本法一三条は、さらに、行政機関の職員が、監視のための装置の付いた技術的情報システムを設置するために住居に侵入する場合にも対抗する[34]。その他の例として、行政機関は、インターネットを通じて、住居内のコンピュータにアクセスし、住居を密かに撮影し、盗聴するために、そのパソコンに設置されたカメラまたはマイクを操作する。この場合にも、住居の不可侵に対する侵害が生じる。

それにもかかわらず、基本法一三条の、空間に関連している保護がすでに事実上の理由によって実現されない多くの場合がある。とくに、住居の外で利用される、（ラップトップ・コンピュータ、ＰＤＡ携帯情報端末、携帯電話といった）移動可能な、技術的情報システムがそうである。しかしながら、技術的情報システムが住居内に存在している場合でさえ、この基本権は、情報技術システムへの侵入のさまざまな可能性に対して包括的な保護を与えていない。連邦憲法裁判所の判例によれば、コンピュータの保存用メディア内のデータだけを探知するために、標的とされたシステムへのアクセスが、コンピュータの接続を介して生じる場合には、住居の不可侵は問題にならない[35]。

2　新しい基本権の限界

(a)　「オンライン捜索」の原理的違憲性の否定

連邦憲法裁判所は、「情報技術システムの信頼性と不可侵性の保障」についての基本権への侵害が、犯罪の予防のためにも、犯罪捜索のためにも正当化することが可能であると明らかにしている。[36] 侵害は、憲法に適った、法律の権限の根拠を必要とする。その際、とりわけ、規範の明確性と特定性についての法治国家的要請が妥当する。権限の根拠および具体的な措置の比例性（適切性、必要性、期待可能性）も入念に顧慮されなければならない。憲法異議によって問題とされた憲法擁護法は、この基準を満たさなかった。私は、その詳細を説明するのではなく、かわりに判決の原則的な中心となる説示を取り上げたい。それは、情報技術システムの行政機関による探知についての権限の比例性についての説示である。

(b)　具体化――比例原則に関する要請

連邦憲法裁判所は、平和および秩序に関する権力としての国家の安全ならびに、身体、生命および自由に対する危険から住民を保護する国家の義務が、その他の高い価値がある法益と同じ次元にある、憲法上の価値であると述べる。[37] 国家の任務には、テロリズムと急進主義に対する実効的な対策も含まれる。その際、それに関連する集団が、ますます、現代的な情報技術を利用していることが考慮されなければならない。情報技術システムへの密かなアクセスは、憲法擁護という憲法に適った目的に適切に役立つ。連邦憲法裁判所は、「オンライン捜索」の適切性についての判断における立法者の評価の特権を強調する。[38] 連邦憲法裁判所は、それによって、専門家の間の一部にあった、「オンライン捜索」は当事者が技術的自己防衛の可能性によってそれに対抗できるため、一般的に役に立たないとの批判を退けた。連邦憲法裁判所は、アクセスの必要性も肯定した。それは、立法者が、彼の評価特権の枠内

において、そのようなシステムに保存されたデータを収集する、より緩やかな手段が存在しないと認めることができる、と判断されたためである。

それにもかかわらず、最も重要な説示が、狭義の比例性（均衡性、期待可能性）についてなされている。連邦憲法裁判所は、全体的な衡量の枠内で、侵害の重大さが、それを正当化する理由の重要性と均衡しているか否かを審査する。連邦憲法裁判所は、ここで、侵害の特別な重大性を強調する。「オンライン捜索」の侵害の高い強度は、遠隔コミュニケーションの接続データの把握が、市民の国家による監視に対する恐怖をつのらせ、自然になされる個人のコミュニケーションを阻害する可能性があるため、それによってますます高まる。最終的に、侵害の重大性にとって特徴的なことは、アクセスの結果として、アクセスされたコンピュータの不可侵性にとっての危険と、当事者と第三者の法益にとっての危険が生じることである。(39)

このように強い基本権侵害は、とりわけ、法律によって規定された契機が、十分な重要性をもたない場合には、比例的とはいえない。立法者は、一方では、基本権侵害の方法と強さを、他方では、正当な、法律上の構成要件要素の侵害のバランスを保たなければならない。連邦憲法裁判所は、それを二つめの判決要旨において次のように定式化している。

「システムの利用を監視し、その保存メディアを解読することによる情報技術システムへの密かな侵入は、優越する、重要な法益にとっての具体的な危険についての事実上の手がかりがある場合に限り、憲法上許容される。優越的に重要であるのは、人々の身体、生命および自由であり、それが脅かされると人間の存在の基礎にかかわる公衆の諸利益である。特定の事実が、個々の場合に特定の人物によって脅かされる危険に基づき、優越的で、重要な法益に差し迫る危険を指し示すその限りにおいて、十分な蓋然性によって、危険が近い将来生じることがまだ確認

されない場合にも、措置の正当化は可能である」。

情報技術システムへの密かなアクセスについての法律上の権限付与は、さらに、当事者の権利の手続法上の保障のための規律を含まなければならない。とくに、アクセスは、裁判官の命令に留保されなければならない[40]。独立した機関によるそのような予防的監督が行われないとしたら、当事者は、保護されない状態に置かれる。連邦憲法裁判所は、立法者が、裁判官と同じく独立性と中立性が保障される場合に限り、他の機関に監督を委ねることができると強調している。もちろん、特に緊急の場合（「危険が差し迫っている場合」）には、中立の機関による監督が事後に確保されているときには、事前の命令が無くてもアクセスを行うことができる。

密かな監視措置がタブーとされる領域は、絶対的に保護されている「私生活の形成の核心領域」である[41]。この領域は、基本法一条一項によって不可侵とされている人間の尊厳の保護領域に含まれる。そこに、私的な利益と公衆にとっての利益を衡量する余地はない。「私生活形成の核心領域」には、連邦憲法裁判所の判例によれば、「感覚や感情、考慮、見解、経験といった、きわめて個人的な、内面的な経過を、国家によって監視される不安無く、表現できる可能性も含まれる」[42]。具体的な例は、日記のような記述や、電話又は電子メールによって伝えられる「きわめて個人的な体験」についての発言である。立法者が、国家機関に「オンライン捜索」の権限を付与しようとするときには、立法者は、私的な生活形成の核心領域が、できる限り侵されない状態に置かれるための明確な予防措置を講じなければならない。連邦憲法裁判所は、オンライン捜索の際に、実務においてしばしば、核心領域の基準による分析が可能になる以前に、きわめて私的な領域の情報も知ることになることは不可避であると認めている。このような場合のために、立法者は、分析の段階における有効な保護を行わなければならない。行政機関は、例えば、その核心領域との関連性をはじめに審査することができない外国語による会話の内容を、全般的に把握することも、

次のような場合に限って許される。それは、優越的で、重要な共同体の利益にとっての具体的危険の事実上の手がかりが存在している場合であり、かつ、分析の段階においてきわめて個人的なデータを事後的に選別し、消去する相応の仕組みが保障されている場合である。

まとめると、以上のことから、二段階の核心領域保護コンセプトが明らかとなる(43)。

第一段階――立法者は、核心領域に関連するデータの収集が可能な限り行われないよう、明確に定めなければならない。

第二段階――核心領域との関連性がデータ収集の前ないしその間に明らかにできない状況は、法律で規律されなければならない。そのためには、核心領域への侵害の強度が可能な限り低く抑えられることを保障することに適した手続規定が必要である（例えば、データの即座の消去またはデータの提供や利用の禁止についての規定）。

四　結びにかえて――いくつかの未解決の問題

いくつかの未解決の問題を指摘して結びにかえたい。

一　「オンライン捜索」判決は、「情報技術システムの信頼性と不可侵性の保障」についての基本権の国家に対する防禦機能を取り扱った。そこから、私人による攻撃に対抗する基本権を保障する国家の保護義務を導き出すことはできるのか。

二　この新しい基本権は民事法関係においていかなる効力を発揮するのか。この判決から、いかなる帰結が明らかになるのか。とくに、企業の情報技術システムが問題になる。例えば、経営者は、「彼の」コンピュータに保存されたデータを好きなように調べることができるのか。

三　この新しい基本権は、「通信記録保存」についての規律に関してどのような意味を持つのか。

〔追記〕　本稿は、二〇〇八年九月五日、大阪大学において行われた法学会スタッフセミナーにおけるアルブレヒト・レスラー（Albrecht Rösler）氏の講演を訳出したものである。ドイツ連邦共和国イルメナウ工科大学経済学部法学研究所研究員であるレスラー氏は、二〇〇八年八月と九月の二ヶ月間、外国人研究員として大阪大学に招かれ、日本の通信放送法制について調査・研究された。

オンライン捜索とは、いわゆる「トロイの木馬」を用いた犯罪捜査である。そのためのソフトウェアは、連邦内務省では「リモート・フォレンジック・ソフトウェア」と呼ばれているが、一般には「連邦の木馬」（Bundestrojaner）という名称で知られている。オンライン捜索については、山口和人「海外法律情報ドイツ――『オンライン捜索』の合憲性をめぐる争い」ジュリスト一三四六号（二〇〇七）七頁、同「海外法律情報ドイツ――オンライン捜査に違憲判決」ジュリスト一三五九号（二〇〇八）六六頁がある。小山剛「監視国家と法治国家」ジュリスト一三五六号（二〇〇八）四八頁以下も参照。

本稿でも言及されているように、二〇〇八年六月、連邦刑事局の権限を拡大し、オンライン捜索を可能にするための法案が連邦議会に提出された。この法案をめぐっては、連立与党間で激しい議論が続いていたが、二〇〇八年一一月一二日、ようやく意見の調整がつき、連立与党の賛成によりこの法案が連邦議会で議決された。なお、この法案は、連邦刑事局のオンライン捜索の権限に、二〇二〇年末までという期限を設けた。この法案については、与党の一部や野党になお強い反対があり、修正なしで連邦参議院の同意を得ることは難しいとみられている（Peter Carstens, Auf dem Weg in den Vermittlungsausschuss, Frankfurter Allgemeine Zeitung v. 17. 11. 2008）。

（1） 1 BvR 370/07, 1 BvR 595/07, BVerfG NJW 2008, 822. 以下では、「本判決・欄外番号」と表記する。

（2） BVerfGE 65, 1 ff.

（3） 自動車ナンバー自動読み取りについての判決（1 BvR 2074/05, 1 BvR 1254/07）と通信記録の保存についての仮命令（1 BvR 256/08）は、二〇〇八年三月一一日に下された。

（4） これに対し、死者の人格権は人間の尊厳（基本法一条一項）のみをその根拠としている。Vgl. BVerfG, 1 BvR 932/94（二〇〇一年四月五日の「ヴィルヘルム・カイゼン」についての第一法廷第一部決定・欄外番号一八）.

（5） 本判決・欄外番号一六九。

（6） 例えば、Frank Fechner, Medienrecht, 8 Aufl. 2008, Kapitel 4, Rn. 11 ff. を参照。

（7） 「左派党」（Die Linke）という政党は、「労働と社会正義――選挙の選択肢」（WASG）の「民主社会党・左派党」（PDS. Linkspartei）への参加によって二〇〇七年に誕生した。民主社会党（Partei des Demokratischen Sozialismus）は、旧東ドイツのドイツ社会主義統一党（Sozialistische Einheitspartei Deutschlands）の直接の権利承継人だった。とりわけ旧西ドイツ地域で行動しているWASGは、ドイツ社会民主党（Sozialdemokratische Partei Deutschlands）の元党員と労働組合員によって、とりわけ「アジェンダ二〇一〇」（一九九八年から二〇〇五年まで続いたゲルハルト・シュレーダー政権下での社会国家改革）に対する抗議のために組織された。

（8） 二〇〇六年一二月二〇日の憲法擁護法五条二項一一号（Gesetz- und Verordnungsblatt Nordrhein-Westfalen S. 620）。

（9） 二〇〇一年六月二六日の基本法一〇条法（BGBl. I S. 1254, 2298）。最終改正は二〇〇七年一二月二一日の法律（BGBl. I S. 3198）五条による。

（10） 一〇条法三条一項。

（11） とりわけ、記録・削除の義務。一〇条法四条。

（12） 一〇条法一〇条一項。

（13） 一〇条法一五条。

（14） 一〇条法一四条、一六条。

（15） 連邦内閣は、二〇〇八年六月、連邦刑事局の権限を改正するための法案（Bundestag-Drucksache 16/10121 vom 13.

August 2008）を決定した（http://dip21.bundestag.de/dip21/btd/16/101/1601 21.pdf）。二〇〇六年の連邦制改革の枠内で、基本法七三条九 a号として連邦に新たな排他的権限が与えられた。それによると、「複数のラントに及ぶ危険が存する場合、一のラント警察官庁の管轄権が認められていない場合、又は、ラントの最高官庁が要請している場合における、連邦刑事警察庁による国際テロリズムの危険の予防」は連邦の専属的権限である。

(16) 二〇〇五年六月から一一月の期間、連邦情報局（BND）が、アフガニスタンのアミン・ファルハン通商産業大臣を「オンライン捜索」によって見張っていたことが明らかになった。その際、ファルハン大臣と雑誌シュピーゲルの女性ジャーナリストとの間で交わされた、表向きは私的ないし内密な内容の電子メールのやりとりも見張られた。連邦情報局長は、二〇〇八年四月、この監視措置について謝罪した。

(17) BGH StB 10/06（二〇〇八年一月三一日の決定）。それによると、刑事訴訟法一〇二条は、被疑者に対し公然とされる捜索の権限のみを付与しており、密かに行われる捜索の権限を付与してはいない。

(18) 憲法擁護法五 a条の「特別な権限」。

(19) Vgl. BVerfGE 79, 1 (20) ; 97, 157 (165).

(20) 憲法擁護法七条二項（「公共の安全にとって差し迫った危険に対する防禦のため」の傍受）。

(21) 連邦憲法裁判所法九三条三項。

(22) BVerfGE 11, 255 (259 f.) 以降。

(23) ドイツでは、秘密情報機関（情報機関）として、①国内情報機関である連邦の憲法擁護機関（連邦内務省の管轄下にある連邦憲法擁護庁）と各州の憲法擁護機関がある。さらに、②連邦情報局（連邦首相府に属する国際情報機関）および③連邦国防省の軍事保安局（MAD）がある。

(24) 連邦憲法裁判所は、「人格にとっての危険」（“Gefährdung der Persönlichkeit” ないし “Persönlichkeitsgefährdung”）という言葉を何度も用いている。しかし、用語法としては、おそらく「人格の発展にとっての危険」（Gefährdung der Entfaltung der Persönlichkeit）のほうがより適しているだろう。

(25) 本判決・欄外番号一九七。

(26) 本判決・欄外番号二〇三。

(27) 本判決・欄外番号二〇八。

(28) 「キーロガー」とは、コンピュータ利用者のキーボード入力を記録することができるハードウェアまたはソフトウェアのことである。キーロギングによって、例えばパスワードが突き止められる。「ハードウェア・キーロガー」は、キーボードとコンピュータの間に取り付けられるものであり、そのためにはコンピュータに直接に物理的にアクセスする必要がある。

(29) 本判決・欄外番号二〇〇。

(30) 本判決・欄外番号一八二以下。

(31) 本判決・欄外番号一八五。「接続データ」についてのBVerfGE 115, 166 (183 ff.) が参照されている。

(32) 本判決・欄外番号二九〇、二九一。

(33) BVerfGE 109, 279 (309, 327).

(34) 連邦憲法裁判所においてITセキュリティの専門家として意見を述べたディルク・フォックス (Dirk Fox) の鑑定書の見解によれば、標的とされたコンピュータに捜索用のソフトウェアを手動でインストールすることによってのみ、第三者のシステムへの侵害を回避することが可能になる。しかしながら、この方法は、二〇〇八年四月に行われた、連邦刑事局の権限を新たに規律するための法案作業の枠内では放棄された。

(35) 本判決・欄外番号一九五。住居の捜索および刑事訴追の枠内での押収（刑事訴訟法一一条）についての判決において、連邦憲法裁判所は、「弁護士事務所の捜索」に関連して、二〇〇五年四月、次のような判断を示した。それによると、住居の捜索からただ間接的に生じる押収は、基本法一三条の保護領域にはもはや含まれない。これに対して保存されたデータの押収は、情報自己決定についての基本権を侵害する。BVerfGE 113, 29 (45).

(36) 制約の問題については、本判決・欄外番号二〇七以下。

(37) 本判決・欄外番号二一〇。

(38) 本判決・欄外番号二一一以下。

(39) 本判決・欄外番号二三九以下。

(40) 本判決・欄外番号二五九以下。二つ目の判決要旨。

（41）確立された判例。本判決・欄外番号二七一。とりわけ大盗聴（Großer Lauschangriff）事件判決BVerfGE 109, 279（313）が参照されている。

（42）本判決・欄外番号二七一。大盗聴事件判決 BVerfGE 109, 279（314）が参照されている。

（43）本判決・欄外番号二八〇以下。