Ⅱ．ハンス・ユルゲン・パピア

予備的データ保存と基本法

倉 田 原 志*（訳）

Ⅰ　情報自己決定権

国勢調査の合憲性に関する1983年12月15日の判決によって，連邦憲法裁判所は，情報自己決定権を承認し，この基本権を基本法秩序の中心，つまり，自由な社会の構成員として自由な自己決定において活動する人の価値と尊厳の中に定着させた[1)]。その保護には，一般的人格権が，しかも住居の不可侵を求める基本権，信書・郵便・電気通信の秘密の保護を求める基本権（基本法13条，10条）のような特別の自由保障と並んで有益である。「国勢調査判決」において新しかったのは，連邦憲法裁判所が一般的人格権[2)]の範囲 Vorgaben を，自動化されたデータ加工という現代的な条件に適応させたことである。人格の自由な発展は，その限りで，個人に関するデータの無限定な収集，保存，利用，提供 Weitergabe に対する個人の保護を前提とする。情報自己決定権は，個人に，自分の個人データの引渡と利用について，原則として自分で決める権限を保障する[3)]。

情報自己決定権への介入 Eingriffe は，十分に特定された法律の根拠を

＊　くらた・もとゆき　立命館大学大学院法務研究科教授

1）　BVerfGE 65, 1 (41 ff.) – Volkszählung.

2）　一般的人格権について，BGHZ 13, 334 (338) – Schacht-Leserbrief ; BVerfGE 34, 269 (281 f.) – Soraya 参照。

3）　BVerfGE 65, 1 (42 f.) – Volkszählung.

必要とする[4]。その際，立法者は，収集されうるデータの利用目的を，領域別に bereichsspezifisch かつ厳密に定めなければならない[5]。データの提供は，原則として，そのデータが収集されるのと同じ目的のためにのみ，考慮に値する。公行政は，その内部で職務共助 Amtshilfe という方法ですべての情報を入手し，異なった行政庁の間で任意に交換することが許される「情報の統一体」Informationseinheit ではない。たしかに，収集されたデータについてのこの目的拘束は，目的の変更を原則として排除するというわけではない。しかし，この目的変更は，憲法に適合した法律の根拠を必要とする。さらに，手続法上の安全対策，たとえば，説明・回答・削除の義務ならびに優先される権利保護のために，独立のデータ保護監察官 Datenschutzbeauftragten の関与が必要である[6]。

Ⅱ　予備的データ保存と通信の秘密

予備的データ保存の場合には，通信の過程が問題となる。通信に関しては，基本法10条は，基本法１条１項と結びついた２条１項にもとづく情報の自己決定を求める一般的基本権を排除し，電気通信の秘密への介入によって獲得されるデータに関する特別の要請を生じさせる，特有の保障を含んでいる。もっとも，その限りでは，連邦憲法裁判所が基本法１条１項と結びついた２条１項から発展させてきた基準は，そのままさらに基本法10条の特別の保障に転用されうる。

1　通信の秘密の保護

基本法10条１項は，通信の秘密を保護する。通信の場合に問題となるのは，個人受領者への通信を使っての情報の無形の unkörperlich 伝達のす

4）BVerfGE 65, 1 (44) – Volkszählung.
5）BVerfGE 65, 1 (46) – Volkszählung.
6）BVerfGE 65, 1 (49) – Volkszählung.

べての過程である。この過程は公権力による閲覧から保護されているべきであり[7]，しかも，通信の内容に関してだけではなく，通信の過程の詳細な状況の秘密に関してもである。この基本法10条によって同様に保護される観点に，連邦憲法裁判所は明文で，「そもそも，いつ，および何回，どのような人あるいは通信設備の間で，通信が行われたかあるいは試みられたか」が属するとしている[8]。

基本法10条の基本権は，通信の秘密を，一方では，通信過程と通信内容を取得する目的の公権力の最初の介入 Eingriff から保護する。他方で，この基本権は，その保護を，通信の秘密への介入を通じて得られたデータの使用および利用というそれに続く措置を考慮しても展開する[9]。「公権力による，通信データのあらゆる閲覧，保存，利用，ならびにその内容の評価あるいはその他の利用のすべてが，基本権への介入である」[10]。したがって，法律によってあるいは法律にもとづく，通信企業に対して通信データを収集，保存し，国家機関に提供することを求める命令のなかには，基本法10条１項にもとづく通信の秘密の保護を求める基本権への介入が存在する。

2　予備的データ保存に関する憲法上の要請

通信の秘密へのこの介入は，「それが正当な公共の福祉 Gemeinwohl の目的に役立ち，その他の点で，比例原則を満たす場合には」合憲である。したがって，この介入は，目的を達成するために，適合し geeignet，必

7）　このこと及び以下のことについては，BVerfGE 125, 260 (309 ff.) – Vorratsdatenspeicherung; BVerfGE 120,274 (306 f.) – Online-Durchsuchung; BVerfGE 106, 28 (35 f.) – Mithörvorrichtung 参照。

8）　BVerfGE 125, 260 (309) – Vorratsdatenspeicherung とそこに挙げられている判決。

9）　BVerfGE 100, 313 (319) – Telekommunikationsüberwachung; 125, 260 (309 f.) – Vorratsdatenspeicherung.

10）　BVerfGE 125, 260 (310) – Vorratsdatenspeicherung.

要で erforderlich，適切なもので angemessen なければならない[11]。

ａ）連邦憲法裁判所は，立法者が，通信履歴データを理由なく anlasslos ６ヶ月間，刑事訴追，危険防止および秘密情報機関の任務の範囲内で限定的に利用するために保存することを規定することは，憲法上可能であるとみなした[12]。そのような規律は，憲法上正当な目的を追求し，その達成のために，６ヶ月間の無条件の保存は，適合し，必要であり，狭い意味で比例的でもありうる。「ここに存在する介入が特に重大であることを十分に考慮した内容形成 Ausgestaltung であれば，通信履歴データの無条件の保存は，それ自体としてすでに，連邦憲法裁判所の判例の意味での予備的データ保存の厳格な禁止に服するわけではない」[13]。

ｂ）刑事訴追，公の安全に対す危険防止ならびに秘密情報機関の任務を果たすことが効果的に実現されるべきことは，通信の秘密への介入をも原則として正当化することができる，国家の正当な任務・目的に属する。このことは，通信履歴データが無条件に予備的に保存される場合にも妥当する。そもそもデータの予備的な収集・保存のすべてではなく，そのようなデータ収集の比例的でない内容形成と特に拡張された目的設定だけが基本法10条の基本権によって禁止される。したがって，個人関連データの予備的な保存は，特に，あまりに不特定でなお特定できない目的を追求する場合に，基本権に反する。それに対して，通信履歴データを，後に条件と関連させて刑事訴追あるいは危険防止の権限をもつ行政庁，あるいは秘密情報機関に提供するために予備的に無条件に保存することは，はじめから比

11） BVerfGE 125, 260 (316) – Vorratsdatenspeicherung とそこに挙げられているこれまでの判決。

12） BVerfGE 125, 260 (316 ff.) – Vorratsdatenspeicherung.

13） BVerfGE 125, 260 (316) – Vorratsdatenspeicherung，ここでは BVerfGE 65, 1 (46 f.) – Volkszählung ; 115, 320 (350) – Rasterfahndung II ; 118, 168 (187) – Kontostammdaten が指示されている。

例的ではないとはいえず，このことで基本権に反するわけではない。もっとも，そのような予備的な通信履歴データの保存の内容形成は，特別の憲法上の要請に服する。このことは，連邦憲法裁判所の判決によれば，特にデータの安全，データ利用の条件と範囲，ならびに透明性と権利保護に関して妥当する[14)]。

ｃ）通信履歴データの保存は，立法者が同時に，データの安全に関する特別の高い水準を保障するときにのみ合憲でありうる。データの安全には，予備的保存の比例性にとっては，大きな意義が当然与えられる，というのは，このように成立するデータのストック Datenbestände は莫大な範囲と相当な潜在的叙述力を獲得するからである。これと関連して，データは，経済性の要求に服し，費用の圧力のもとで行動する，民間のサービス提供者に保存されることにも配慮されなければならない。民間のサービス提供者にとっては，データの安全の保障のための刺激は，限定された程度においてだけ存在する。たしかに，憲法は，詳細にどのような安全措置が要請されているかを個別的に定めることはできない。しかし，結果として，予備的な通信履歴データの保存によって生じるデータのストックがもつ特別な危険の潜在性を顧慮して，相当高い程度の安全を確保する基準が保障されていなければならない。この基準は，専門家の議論の展開状態に適応していなければならず，新たな知識と認識を引き続き受け入れていなければならない。このようなデータのストックに由来する危険の潜在性は，安全の要請を一般的な経済的利益との衡量のもとで相対化することを許さない。それゆえ，データの安全を憲法上十分に保障するために，たとえば，データの分離した保存，高度の暗号化，二人の関与の原則 Vier-Augen-Prinzip を利用したような安全なアクセス体制，ならびに監査可能な記録整備といったものが要求されなければならない[15)]。

14） BVerfGE 125, 260 (325 ff.) – Vorratsdatenspeicherung.

15） BVerfGE 125, 260 (325 f.) – Vorratsdatenspeicherung.

ｄ）そのうえ，通信履歴データの保存の合憲性は，このデータの利用に関する法律の規定に依存する[16]。その際，「関連する法的根拠において，データ利用とその範囲に関する条件は，当該保存の中に存在する介入が重大であればあるほど，狭く限定されなければならない。その際，当該介入の理由，目的および範囲ならびに対応する介入の限界 Eingriffsschwellen は，立法者によって，領域別に，厳密に，規範として明確に規律されなければならない」。[17]

ほとんどすべての通信履歴データの無条件で組織的な保存によって得られたデータあるいはデータのストックが利用されなければならないならば，比例原則は，この利用が特別に高度の公共の福祉の利益に役立つことを要求する。この利用は，ぬきんでて重要な法益保護の任務のためだけになされることが許される。換言すれば，ぬきんでて重要な法益を脅かす犯罪行為の処罰，あるいはそのような法益に関する危険防止が問題となっていなければならない[18]。

(1) したがって，刑事訴追のためのデータ利用は，少なくとも特定の事実によって根拠づけられた，重大な犯罪行為の容疑が存在することを前提とする。個別的にどのような犯罪構成要件がこの「重大な犯罪行為」の範囲に含まれるべきかを，立法者はデータ保存に関する規律といっしょに最終的に確定しなければならない。「重大な犯罪行為」として格付けすることは，当該刑法規定において，たとえばその特別の法定刑 Strafrahmen において，客観的に反映されなければならない。したがって，立法者は，抽象的に当該犯罪行為のカタログを確定しなければならず，さらに，立法者は，予備的に保存された通信履歴データの入手は，個々の場合にも重大な犯罪行為の訴追が問題となっているときのみになされてよいことも確保

16） BVerfGE 125, 260 (327 ff.) – Vorratsdatenspeicherung.

17） BVerfGE 125, 260 (328) – Vorratsdatenspeicherung とそこに挙げられている判決。

18） BVerfGE 125, 260 (328) – Vorratsdatenspeicherung.

しなければならない[19]。

(2) 危険防止のためには，予備的に保存された通信履歴データの入手に関する次のような憲法上の限界が妥当する。つまり，入手は，人の身体・生命・自由，連邦・州の存続ないしは安全に関する危険防止のため，あるいは公共の危険防止のためにだけ許される[20]。このことは，データ保存とデータ利用に存在する介入の重大さと有効な危険防止の意義との間の衡量から生ずる。さらに，法律の授権の基礎は，「少なくとも，保護されるべき法益に関する具体的な危険の事実上の根拠」を前提としなければならない[21]。推測や一般的な経験則は，危険防止のために当該データの入手を正当化するには十分ではない。むしろ，具体的な危険の予測を支える特定の事実が確定されていなければならない。このデータの入手は，重大な基本権への介入である。したがって，事実上の介入の理由は，個々になお予測可能ではない具体的な危険にまで拡大することは許されない。具体的な危険の予測を支えることができ，説得力があると思わせる特定の事実が確定されていなければならない。

(3) 警察による危険防止のためのデータ利用について述べたことは，原則として予防的な目的をもつすべての介入の授権に関して妥当する。秘密情報機関によるデータ利用に関しても，言及した憲法上の要請と限界に注意が払われなければならない[22]。行政庁に関連する区別，たとえば，一方で警察と，他方で憲法擁護庁のような他の予防的な任務を委託されている行政庁の間で，区別の可能性はない。したがって，秘密情報機関による予備的に保存された通信履歴データの利用は，多くの場合にできない。こ

19) BVerfGE 125, 260 (328) – Vorratsdatenspeicherung.
20) BVerfGE 125, 260 (330) – Vorratsdatenspeicherung.
21) BVerfGE 125, 260 (330) – Vorratsdatenspeicherung.
22) BVerfGE 125, 260 (331) – Vorratsdatenspeicherung.

れは，何よりもまず予備的解明 Vorfeldaufklärung の領域で活動する秘密情報機関の任務設定の性質から生じる。このことは，この場合に存在する種類の介入に関する憲法上の条件を引き下げるための正当化理由とはならない。

ｅ）立法者は，最後に，データ利用の透明性ならびに効果的な権利保護と効果的な制裁の保障のための十分な安全措置を講じなければならない[23]。この広範な条件のもとでのみ，予備的に無条件に保存された通信履歴データの保存とその利用が比例原則に適合する。要請される透明性に関して，これが可能である限りにおいて，このデータの利用はオープンに行われなければならない。このことが諸般の状況から判断して考慮されないのであれば，原則として，少なくとも該当者への事後の通知が必要である。例外的にそのような事後通知もされないのであれば，裁判官はこの非通知について判断しなければならない。

(1) 該当者が知ることなくデータが利用されることが憲法上許されるのは，「さもなければ，データ入手が役に立つ捜査の目的が無に帰する場合」だけである[24]。危険防止が問題である限り，このことは原則としてあてはまる。しかしながら，刑事訴追の枠内で，このデータはしばしばオープンにも収集され利用されうる。この場合，秘密に利用することが許されるのは，個々の場合に必要であり，裁判官によって命じられている場合で，その限りにおいてだけである。

(2) 通信履歴データの予備的な保存とその利用は，効果的な権利保護と適切な制裁が，権利侵害の場合に保障される場合にのみ比例原則をみたす

23) BVerfGE 125, 260 (334) – Vorratsdatenspeicherung.
24) BVerfGE 125, 260 (336) – Vorratsdatenspeicherung.

ことができる。この目的のために，このデータの照会 Abfrage ないし提供は原則として裁判官の留保のもとになければならない[25]。重大な基本権への介入をもたらす介入措置の場合には，一般的に憲法から，独立の機関 Instanz を通じた予防的コントロールが要請される。このことは，基本権への介入が秘密のうちに生じ，該当者にとっては直接知覚できないときには特にあてはまる。これは，このような措置は原則として裁判官の命令の留保のもとにおかれなければならないことを意味する。というのは，裁判官だけが「その人的および客観的独立性と法律だけに拘束されることを根拠として，個々の該当者の権利をもっともよく，確実に確保する」ことができるからである[26]。

その他，データ利用の事後的なコントロールのための権利保護手続も存在しなければならない。該当者が措置の実施の前に自分の通信履歴データの利用に対して，裁判所で防禦することができないのであれば，該当者には事後的な裁判所によるコントロールが開かれていなければならない[27]。

(3) 最後に立法者は，違法なデータ利用の場合の有効な制裁を規定しなければならない。ここで問題としているデータの権限のない獲得あるいは利用に通常存在する人格侵害の特別の重大さは，刑法，刑事訴訟法，民法の損害賠償法において十分に考慮されなければならない。この場合には，刑法上の利用禁止ならびに非財産的損害に対する損害賠償責任も考えられうる。

3 ドイツの法律規定の合憲性

ドイツ法の争われている法律規定における，データの安全に関する法律上の基準ならびにデータの利用に関する規定は，連邦憲法裁判所の見解に

25) BVerfGE 125, 260 (337) – Vorratsdatenspeicherung.
26) BVerfGE 125, 260 (338) – Vorratsdatenspeicherung.
27) BVerfGE 125, 260 (339) – Vorratsdatenspeicherung.

よれば，憲法上の要請を満たしていなかった[28]。したがって，同時に，保存義務自体にも憲法上必要とされる正当化が欠けていた。それゆえ，予備的データの保存についての規定全体が基本法10条１項にもとづく通信の秘密の保護を求める基本権と適合しなかった。これらは連邦憲法裁判所によって無効と宣言された。他方，連邦憲法裁判所は，特別に厳格な条件を確保すれば，通信履歴データに関する無条件の予備的保存は憲法と合致しうるということを排除しなかった。もっとも，立法者は今日まで新たな規定をつくっていない。これは，とくに，キリスト教―自由連合の内部で，予備的データ保存の導入が全体として争われていることによる。

連邦憲法裁判所は，通信履歴データの予備的保存についての判決で，憲法上の「境界標柱 Grenzpfahl」に到達した。つまり，市民のほとんどすべての活動を再現可能とするデータの，広範で予備的な入手と保存は，情報自己決定権と合致しない。このような国家のデータ収集はもしかすると追加的な程度の安全を意味するかもしれない，しかし，これは自由行使をはなはだしく制限するであろう，市民の完全な監視という負担でなされてはならない。

Ⅲ　基本権保護に関する新たな挑戦

1　新たな脅威――新たなテクノロジー

情報自己決定権は，1983年12月15日の国勢調査判決の時代と比べると，新たな挑戦を受けている。新たな挑戦の根拠は，特に，さし迫った危険の種類にある。2001年９月11日のアメリカ合衆国における，および2004年３月11日のマドリッドにおけるテロ行為の後，ドイツにおいて，およびヨーロッパ連合のレベルで，たとえば，いわゆる「普段は普通の生活をしているテロリスト Schläfern」をさがすための予防的な警察による網目スク

28）BVerfGE 125, 260 (347 ff.) – Vorratsdatenspeicherung.

リーン犯罪捜査[29]，「オンライン捜索」[30]，あるいはここですでに述べたような通信履歴データの予備的保存といった，新たな措置が実施ないし議決された。

しかし，これらの新たな挑戦は，その根拠をさし迫った危険の種類にだけおくのではなく，情報・コミュニケーション技術のまさに革命的な変化にもおいている。国家は，一方では―市民の身体，生命，自由の保護のための基本権による義務を果たすために―この技術的な変化を，危険防止と犯罪行為の訴追の際には，配慮しないままでいることは許されない。他方，自由と安全のバランスをとることに関連して，重点を根本的に自由の負担になるように移動させることは許されない。

2　比例性と人間の尊厳の保護

情報自己決定権への新たな介入に関する憲法上の判断の際には，比例原則が，保護されるべき法益の重要さならびに危険の種類と強さに関する要求を出す。さらに，究極的には人間の尊厳から導かれる私的な生活形成の核心領域も，国家による監視措置によって侵害されてはならない[31]。人間の尊厳と個別の自由権のなかに含まれる人間の尊厳の内容は，連邦憲法裁判所の確立した判例によれば，他の自由権とそれから生じる国家の保護義務に対して，衡量できない，あるいは，全く「衡量から免れている」のである。たしかに，実際には，データ収集の前には，そのデータが私的な生活形成の核心領域に関わるものであるかどうかが全く明らかにならないという問題はしばしば生じる。この状態に関しては，収集と利用の段階の区別を要求する二段階の保護構想が妥当するが，それについて，ここでは詳細に立ち入ることができない。

29）　このことについては，中でも，BVerfGE 93, 181 (186 ff.) – Rasterfahndung I; BVerfGE 115, 320 (341 ff.) – Rasterfahndung　II 参照。

30）　BVerfGE 120, 274 (302 ff.) – Online-Durchsuchung 参照。

31）　このこと及び以下のことについては，特に，たとえば BVerfGE 109, 279 (311 ff.) – Großer Lauschangriff 参照。

いずれにせよ，結論として，国家の安全保障法上の活動に関する基本権上の限界に照らせば，国家が「オーウェルが描いたような Orwellscher Prägung」監視国家へと変化する可能性はたいへん遠く離れたものであるということが固く保持されることができる。法治国家的な共同体 Gemeinwesen は，われわれがドイツにおいても最近の歴史から知っているように，自らを全体主義的な監視国家から区別する，法治国家的および民主的なコントロールメカニズムをもっている。

3 私人による脅威

a）われわれの心配としては，国際的な規模の私人による監視社会に変貌する可能性があることが，今日ではより問題であると言われているが，このことは一定程度，自発的にも生じている。情報・コミニュケーション技術の絶え間のない技術的な進歩と，情報手段の国際的なネット化によって，市民は国勢調査判決の時代に比べて，信じがたいほど多くの新しい行動可能性をさらに獲得した。たしかに，世界のどこかでわれわれについて保存されている情報のすべてが集められれば，各人の「人格のプロフィール」が，たやすく作成されうる。もっとも，このことは「データ保護の想定不可能な大事故 Super-Gau」であろうが，それは，国家によってではなく，私人の手によって引き起こされるものである。

b）基本権は一般的に，情報自己決定権は特に，市民に有利になるように国家の保護の最低基準を要求する[32]。というのは，基本権は国家に，競合する自由権との調整の上で，適切な保護システムと保護水準を創設し貫徹すること，ならびに，国際的なレベルでそのようなシステムのために尽くすことを義務づけもするからである[33]。換言すれば，国家は，私人に

32） 基本権からの客観的保護義務の導出について，たとえば BVerfGE 39, 1 (36 ff.) – Schwangerschaftsabbruch; BVerfGE 115, 118 (152) – Luftsicherheitsgesetz 参照。

33） Hoffmann-Riem, JZ 2008, 1009 (1011 f., 1013); ders., AöR 123 (1998), 513 (524 ff.); Petri,↗

よる介入に対しても効果的な保護を確保しなければならない。その際，国家は，私人に自己拘束を課すことだけで甘んじることはもはや許されず，基本権の価値秩序を私法関係においても有効なものとするために，国家は自ら拘束的な秩序をつくり出さなければならない。情報自己決定権の基本権としての保護委託は，技術の絶えざる進歩に照らせば，決して完了させられうるものではないことから出発することができる[34]。このことは，最近再び，誰にでもアクセスでき，街全体について詳細にありのまま，三次元の表示を可能にするインターネット・プログラムである「グーグル・ストリートビュー」をめぐる議論で示された[35]。

私は，すでにたびたび引用した，1983年12月15日の連邦憲法裁判所の国勢調査判決のなかのある命題で締めくくることとしたい。すなわち，「情報自己決定権は，市民が自らについて，誰が何をいつ，およびどのような機会に，知るかをもはや知ることができない社会秩序とこれを可能とする法秩序とは相容れないであろう。」

↘ DuD 2008, 443 (446 f.); Hassemer, FAZ vom 5. Juli 2007, S. 6; Ronellenfitsch, RDV 2008, 55 (58) も参照。

34） データ保護法の根本的な改革の必要について，たとえば，Kutscha, ZRP 2010, 112 ff.; Kühling/Bohnen, JZ 2010, 600, 601 (607 ff.) 参照。

35） たしかに，民間企業のグーグル社は，特に，家の所有者と借り主が異議申し立てすれば，その建物を表示しない準備があることはすでに明らかにしている。これについては，自らに対する義務づけの表明である，“Zusagen von Google zum Internetdienst Google Street View”（http: //www. hamburg. de/datenschutz/aktuelles/1569338/google-street-view-zusage.html で閲覧可）参照。しかし，今日のドイツの法的状況によれば，当該写真の公表に対して有効な論拠があるかどうかは，少なくとも争われている。これについては，たとえば，Caspar, DÖV 2009, 965 ff.; Spiecker gen. Döhmann, CR 2010, 311 ff.; Lindner, ZUM 2010, 292 ff. 参照。