論題 Title	フランスにおける偽装携帯電話基地局を使用した通信傍受法制
他言語論題 Title in other language	Legislation on Interceptions by Cell-site Simulators in France
著者 / 所属 Author(s)	川西　晶大（Kawanishi, Akihiro） / 国立国会図書館調査及び立法考査局　行政法務課長
雑誌名 Journal	レファレンス（The Reference）
編集 Editor	国立国会図書館 調査及び立法考査局
発行 Publisher	国立国会図書館
通号 Number	794
刊行日 Issue Date	2017-03-20
ページ Pages	49-64
ISSN	0034-2912
本文の言語 Language	日本語（Japanese）
摘要 Abstract	テロが頻発したフランスにおいて整備された偽装携帯電話基地局を用いた通信傍受法制について、偽装携帯電話基地局の意義、法制度の内容等を概観する。

フランスにおける偽装携帯電話基地局を使用した通信傍受法制

国立国会図書館　調査及び立法考査局
行政法務課長　川西　晶大

目　　次

要　旨

① 犯罪捜査、情報活動等のために、公の機関が偽装携帯電話基地局を使用して利用者契約番号、端末機器の位置情報、通信内容等の情報を取得する事例が各国で見られる。偽装携帯電話基地局を使用した情報収集は、対象者以外の通信も傍受され、傍受者以外に傍受を知られる可能性が極めて低い点に特徴がある。

② フランスにおいては、2015 年及び 2016 年に偽装携帯電話基地局を使用したデータの取得及び通信内容の傍受が法制化された。法制化に至る背景として、1990 年の欧州人権裁判所の判決において、通信傍受に当たっては、欧州人権条約第 8 条の私生活及び通信の尊重に係る規定に適合するよう、明確な法の規定が必要であるとされたことがある。1991 年に、刑事訴訟手続における通信傍受及び行政が行う通信傍受の法制化が図られ、その後、通信傍受の範囲が拡大している。

③ フランスにおける偽装携帯電話基地局の使用については、2015 年に行政が行うデータの取得及び通信内容の傍受について、2016 年に刑事訴訟手続におけるデータの取得及び通信内容の傍受について、それぞれ立法が行われた。これらの法制においては、偽装携帯電話基地局を使用する場合について、既存の技術を使用する場合と比べて、許可期間、データの消去等の面でより慎重な取扱いを定めている。

④ 通信手段の発達に伴い、安全の保障のために新しい捜査手段の導入が求められているが、それが私生活の尊重の不当な侵害をもたらしてはならないため、新しい捜査手段の導入と統制については極めて困難な考察を要する。

はじめに

2015年、パリは2度の大きなテロ事件に見舞われた。1月7日のシャルリ・エブド事件と11月13日のコンサート・ホール「バタクラン」ほかで起きたパリ同時多発テロである。シャルリ・エブド事件では12人が、パリ同時多発テロでは130人以上が死亡した。

フランスは、2005年のロンドン同時多発テロ以来、頻繁にテロ対策立法を行っており、2014年11月にも「テロリズムの対策に関する措置を強化する2014年11月13日の法律第2014-1353号」(1)を制定したところであった。政府は、テロ対策の中でも、部分的にしか法整備が進んでいない情報活動については強化の余地があると考え(2)、2015年3月には情報活動について包括的に規定する法律案を国民議会に提出し、同年7月には「情報活動に関する2015年7月24日の法律第2015-912号」（以下「2015年情報活動法」という。）(3)として成立した。同年11月のパリ同時多発テロの後には、緊急状態(4)が宣言され、数度の延長を経て、現在では2017年7月まで延長されている。そのような中で、2016年6月には「組織犯罪、テロ及びこれらの資金調達への対策を強化し、刑事司法の実効性及び保証を改善する2016年6月3日の法律第2016-731号」（以下「2016年テロ対策強化法」という。）(5)が制定された。

2015年情報活動法及び2016年テロ対策強化法等の制定に当たっては、人権擁護機関等から様々な点が指摘された(6)が、中でも通信の監視、プロバイダにおける「ブラックボックス（boîte noire）」(7)の設置並びに偽装携帯電話基地局（cell-site simulator）を利用した接続データの取得及び通信傍受については、私生活及び通信の尊重といった人権を不当に害するおそれがあるとして、大きな批判があった。

偽装携帯電話基地局を利用した接続データの取得及び通信傍受に関する法制度については、フランスのほか、米国、ドイツ等でも議論が行われているが、本稿では、このうち、我が国での紹介がまだ少ないフランスについて取り上げる(8)。

＊　本稿におけるインターネット情報は、2017年2月16日現在のものである。

(1)　Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.

(2)　“Projet de loi relatif au renseignement,” N° 2669, Assemblée nationale, 19 mars 2015, p.4.

(3)　Loi n° 2015-912 du 24 juillet 2015 relative au renseignement.

(4)　État d’urgence. フランスの緊急事態制度には、憲法に規定する大統領の非常権限及び戒厳の制度と、法律に根拠を置く緊急状態の制度があり、2015年以降適用されているのは後者の制度である。「緊急事態」と訳す例もあるが、ここでは、憲法上の制度と区別する意味で、「緊急状態」と訳す例に倣った。フランスの緊急事態制度及び緊急状態法について、矢部明宏「フランスの緊急状態法―近年の適用事例と行政裁判所による統制―」『レファレンス』748号, 2013.5, pp.5-26. <http://dl.ndl.go.jp/view/download/digidepo_8206691_po_074801.pdf?contentNo=1> 参照。

(5)　Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et ameliorant l’efficacité et les guaranties de la procédure pénale.

(6)　例えば、“Avis sur le projet de loi relatif au renseignement dans sa version enregistrée le 1er avril 2015 à la Présidence de l’Assemblée nationale,” 1 avril 2015. Commission nationale consultative des droits de l’homme website <http://www.cncdh.fr/sites/default/files/15.04.16_avis_pjl_renseignement_0.pdf>

(7)　インターネット上の通信に係る情報を自動的に解析する装置。

(8)　日本語で主に米国の事例について論じた資料として、指宿信「偽装携帯基地局を用いた通信傍受」『法学セミナー』No.730, 2015.11, pp.1-4がある。

Ⅰ　偽装携帯電話基地局

1　概要

偽装携帯電話基地局とは、携帯電話基地局を装い携帯電話端末からの無線通信を傍受する装置である。携帯電話の契約者を一意に識別する識別子であるIMSI（International Mobile Subscriber Identifier）を把握できるものであることから「IMSIキャッチャー」、また、著名な商品名から「スティングレイ（Stingray）」とも呼ばれる。

携帯電話は、電波の強い基地局を自動的に選んで接続する。偽装携帯電話基地局は、これを利用して、傍受対象者の端末が偽装携帯電話基地局への接続を選択するように仕向けるものである。携帯電話が使用中ではない場合にも基地局との通信は行われるため、偽装携帯電話基地局によって携帯電話の情報を取得することが可能となる。このほか、類似の監視技術として、携帯端末に働きかけずに飛び交っている電波を受信する方法もある。この方法は、偽装携帯電話基地局のように電波を発しないため秘匿性が高いが、傍受対象者の端末が現にデータを送信しているときに近くに設置する必要がある。(9)

偽装携帯電話基地局は、次のような機能を有する。第一に、対象者の所在がわかっている場合には、IMSIその他の対象者の携帯電話端末及び契約に関する識別番号を取得することができる。第二に、IMSIその他の識別番号がわかっている場合には、対象となる携帯電話端末の所在を特定することができる。第三に、行われている通信の相手先や通話時間といった通信の接続に関する技術的データ（以下「接続データ」という。）を取得することができる。第四に、通話や送受信されたメッセージ、接続したウェブサイトのアドレス等の通信内容自体を傍受することができる。(10)第五に、特定の端末ごとに、又は接続しようとした相手方の番号等により通信を止めることも可能である(11)。

偽装携帯電話基地局が使用され始めた時期は明らかではないが、米国の軍や情報機関では少なくとも1990年代初めから携帯電話監視技術が使用されていたといわれている(12)。

2　特徴

偽装携帯電話基地局による通信傍受は、通信会社の設備等を用いた従来の通信傍受と異なる考慮を必要とする。その要因は、次の2点にある。

第一に、偽装携帯電話基地局により通信が傍受された場合であっても、通信は正常に行われるので、利用者は通信が傍受されたことに気がつかない。また、無線通信を傍受するものであるので、傍受に当たって通信会社の設備を利用する必要がない。このため、傍受を実施する者以外が傍受に気付くことは困難である(13)。

---

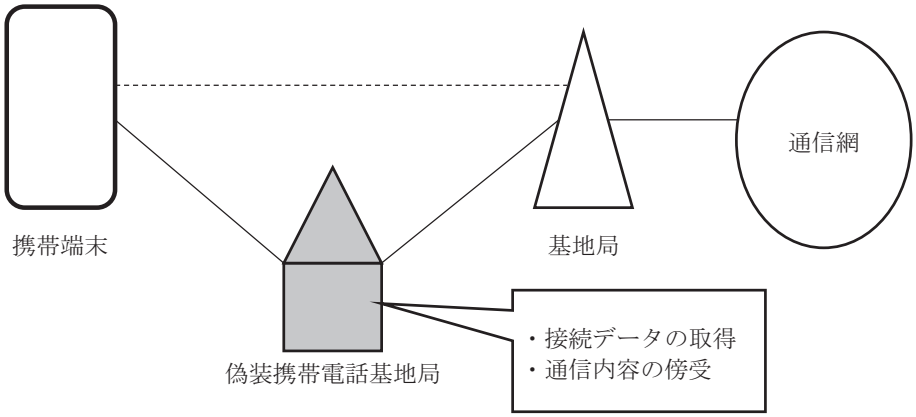
(9)　Stephanie K. Pell and Christopher Soghoian, “Your secret stingray’s no secret anymore,” *Harvard Journal of Law & Technology*, 28(1), Fall 2014, pp.9-13.

(10)　Linda Lye, *Stingrays: The Most Common Surveillance Tool the Government Won’t Tell You About*, ACLU of Northern California, 2014, pp.2-3. <https://www.aclunc.org/sites/default/files/StingRays_The_Most_Common_Surveillance_Tool_the_Govt_Won%27t_Tell_You_About_0.pdf>; “Cell-Site Simulators.” Electronic frontier foundation website <http://www.eff.org/sls/tech/cell-site-simulators>

(11)　Pell and Soghoian, *op.cit.*(9), p.18.

(12)　*ibid.*, pp.9-12.

図　偽装携帯電話基地局の概念



（出典）筆者作成。

第二に、偽装携帯電話基地局は、傍受対象端末だけから接続できるわけではなく、通常の基地局と同様に、他の基地局よりも電波強度が強い範囲にある他の同様の端末からも接続されることになる。このため、傍受対象者とは関係のない通信も傍受されてしまう。(14)

Ⅱ　フランスにおける通信傍受関連法制の変遷

フランスにおいては、2015 年及び 2016 年に偽装携帯電話基地局を使用したデータの取得及び通信内容の傍受が法制化された。これらの法制度について、通信傍受関連法制がどのように成立してきたかという観点から概観する。

現在、フランスにおける通信傍受法制には、刑事訴訟手続の一環としての捜査において行われる司法傍受に関するものと、行政機関が行う行政傍受(15)に関するものがある。前者は刑事訴訟法典（Code de procédure pénale）により、後者は国内安全法典（Code de la sécurité interieure）により規律されている。

1　クリュスラン事件判決

かつて、フランスには通信傍受に関する明確な法律の規定がなく、刑事訴訟手続における電話の傍受は、予審判事の権限である「真実の発見のために有用と思料する一切の予審処分」（刑事訴訟法典第 81 条）に含まれるものとして行われてきた(16)。また、情報機関等によって行われる治安のための傍受には、法律上の明文の根拠はなかった(17)。この点に関して、ヨーロッパ人

---

(13)　*ibid.*, pp.10-11. 一方で、偽装携帯電話基地局を探索するスマートフォンアプリも開発されている等、偽装携帯電話基地局に対する対抗技術も進展しているとの指摘もある。*idem.*, pp.73-75.

(14)　C. Justin Brown and Kasha M. Leese, “Stingray devices usher in a new fourth amendment battleground,” *Champion*, 39(5), June 2015, p.14.

(15)　フランス法では interceptions de sécurité（治安傍受）と規定されているが、日本語文献では「行政傍受」又は「行政盗聴」と訳されることが多い。

(16)　クリュスラン事件判決以前の判例及び実務に関する詳細については、小木曽綾・只木誠「フランスの電信・電話傍受法制」『法学新報』101(11・12), 1995.8, pp.81-135.

(17)　Roger Errera, “Les origines de la loi du 10 juillet 1991,” *Commission nationale de contrôle des interceptions de sécurité - 10e rapport d’activité: 2001*, 2002, p.49. <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/024000296.pdf>

権裁判所は、1990年のクリュスラン事件判決[18]において、このような刑事訴訟手続における盗聴の実務はヨーロッパ人権条約（European Convention on Human Rights）第8条に違反すると判示した。

同条は、私生活、家族生活、住居及び通信（correspondence）の尊重に関する権利を定めたものであり、その第2項では、国の安全保障、公共の安全等の一定の目的のために法に従って（in accordance with the law）行われ、かつ、民主的社会に必要とされる場合を除き、この権利の行使に対する公の機関による干渉を禁じている。

同判決では、同条第2項の「法に従って」という要件を満たしているかが問題となった。

争点となったのは、まず、フランス法に同条第2項の「法」が存在するかどうかである。原告は、刑法典第368条が原則として電話盗聴を禁じているにもかかわらず、刑事訴訟法典第81条は明示的に電話盗聴を認めているものではないので、同条約第8条第2項に規定する「法」は存在しないと主張した。一方、フランス政府は、刑事訴訟法典は、捜査方法を網羅的に列挙したものではなく、判例により補充されるものであると主張した。これに対し、裁判所は、「法」とは実質的な法を指すのであって、イギリスのようなコモンローの国々だけではなく、フランスのような大陸法系の国であっても、判例法も含まれるとの判断を示した。また、同項の「法に従って」の解釈に当たっては、法へのアクセス可能性が問題となるが、本件ではこの点は問題ではないとした。

次いで争点となったのは、法の「予見可能性」である。裁判所は、1984年のマローン判決[19]を引いて、同条約第8条第2項は、国内法があれば十分というものではなく法の質を問うているのであって、「（ヨーロッパ人権条約第8条）第1項により保護される権利に公的機関が任意に干渉することに対して、国内法に法的保護の措置を置かなければならないことを意味している」[20]と判示した。すなわち、法は、任意の干渉に対して適切な保護が与えられるよう、「権限ある当局に付与された裁量の範囲及びその行使の方法を十分明確に示さなければならない」[21]というのである。

裁判所は、この規準に照らして、刑事訴訟法典の規定及び判例法は、公的機関による裁量の行使の範囲及び方法を合理的に明確に示しているとはいえないと判断した。なお、裁判所が不明確であるとして例示したのは、電話盗聴の対象となる人物のカテゴリー、盗聴の対象となる犯罪の性質、傍受した会話を含む調書の作成手続、裁判官又は弁護側による取調べの際に録音物を改変なく完全な形で伝達するために採られる予防措置及び弁護側による録音物の消去又は破棄の条件である。

また、本稿との関係では、クリュスラン事件判決が「利用し得る技術的な処置は絶えず改良されていくのであるから、この点に関する明白かつ詳細な準則の存在は不可欠である」[22]と、通信傍受に関する新技術の開発と法による準則の設定の必要性を関連付けて論じている部分が注目される。

---

⑱ European Court of Human Rights, Kruslin v. France, 24 April 1990, Series A no. 176-A. 同判決の解説として、白取祐司「電話盗聴と手続法定原則」『ジュリスト』No.977, 1991.4.15, pp.54-58; 永野貫太郎「ヨーロッパ人権裁判所判決と電話盗聴」『国際人権』No.6, 1995.11, pp.74-75.

⑲ European Court of Human Rights, Malone v. The United Kingdom, 2 August 1984, Series A no. 82.

⑳ *ibid*., § 67.

㉑ *ibid*., § 68.

㉒ 白取　前掲注⑱, p.56の訳による。European Court of Human Rights, *op.cit.*⑱, § 33.

2　1991 年通信傍受法

クリュスラン事件判決を受けて、1991 年 7 月に「遠隔通信手段により発信された通信の秘密に関する 1991 年 7 月 10 日の法律第 91-646 号」（以下「1991 年通信傍受法」という。）[23]が制定された。同法の第 1 章では司法傍受について、第 2 章では行政傍受について、それぞれ規定されている。第 1 章は、刑事訴訟法典を改正するものである。[24]以下、同法の概要を紹介する。

まず、司法傍受制度について説明する。傍受、録音及び反訳を命ずることができる権限を有するのは、予審判事であり、傍受の決定は書面で行われる。この決定に対する上訴は認められない。対象となる犯罪は、重罪及び法定刑が 2 年以上の拘禁刑である軽罪である。傍受の決定の有効期間は、決定から最長 4 か月であり、傍受の形式及び期間のいずれも同一の場合には更新することができる。予審判事又は予審判事の嘱託を受けた司法警察員（officier de police judiciaire）（以下「予審判事等」という。）は、通信業者等に傍受装置の設置を委託することができる。傍受及び録音の措置は、その開始及び終了の日時とともに予審判事等が調書に記載する。また、予審判事等は真実の発見に有用な通信を反訳し、調書に記載する。傍受により作成された録音物は、封印され、公訴時効期間が満了したときに、共和国検事（procureur de la République）[25]又は検事長（procureur général）[26]の請求により廃棄される。

次に、行政傍受制度について説明する。傍受の目的は、国の安全保障に関する情報を収集すること、フランスの科学的及び経済的潜在能力に関する不可欠な情報を保全すること、テロリズム及び組織犯罪を防止すること並びに「武装集団及び民兵に関する 1936 年 1 月 10 日の法律」[27]により解散された集団の再結成や維持を防止することである。傍受は、国防大臣、内務大臣若しくは税関を所管する大臣又はこれらの者から特に委任を受けた者の書面による提案に基づき、首相又は首相により特に委任された 2 人の者のうちの 1 人の書面により許可される。許可の際には、同時に実施可能な傍受件数を定める。許可は、最長 4 か月間有効であり、同一の条件で更新可能である。傍受で得た情報はこの法律に規定された目的以外に使用することはできないが、刑事事件捜査に関する共和国検事の権限は妨げられない。国家行政傍受監視委員会（Commission nationale de contrôle des interceptions de sécurité: CNCIS）が独立の行政機関として設立される。CNCIS の委員長は、コンセイユ・デタ（Conseil d'État）[28]の副院長及び破棄院長が共同で作成した 4 人のリストから大統領により任命される。委員長の任期は 6 年である。CNCIS の主な権限は、傍受の決定の通知を受けて傍受の合法性に疑義があると思われるときに 7 日以内に見解をまとめ、傍受がこの法に違反して実施されたと判断するときは首相に対して中止を勧告すること、また、職権又は利害関係者の請求により傍受の合法性の審査を行い、違反していると判断するときは首相に対して中止を勧告することである。

⑵3　Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications.

⑵4　同法について、小木曽・只木　前掲注⑴6。また、第 1 章に係る邦訳としては、『フランス刑事訴訟法典』（法務資料 459 号）法務大臣官房司法法制調査部司法法制課, 1999, pp.57-59 がある。以下の記述は、これらを参照したものである。

⑵5　大審裁判所（原則として県庁所在地に所在する第一審の普通法上の裁判所）の検察の長の地位にある検察官。

⑵6　破毀院又は控訴院の検事局の長の地位にある検察官。

⑵7　Loi du 10 janvier 1936 sur les groupes de combat et milices privées.

⑵8　国務院と訳されることもある。最高行政裁判所であり、同時に法的問題に関する政府の諮問機関でもある。なお、院長は形式上首相とされており、副院長がコンセイユ・デタ全体の責任者である（滝沢正『フランス法　第 3 版』三省堂, 2008, pp.202-203）。

接続データの取得については、明記されていない。接続データの取得に関係する規定としては、第3章（共通規定）の第22条において、予審裁判所、首相、国防大臣又は内務大臣は、通信事業者に対して、この法律に定める傍受に必要な情報及び文書の提供を求めることができることとされているにとどまる[29]。

行政傍受制度に関する第2章は、2012年に国内安全法典の法典化が行われた際に、その第2編（公の秩序及び治安）第4章（行政傍受）に加えられた。

3　組織犯罪に係る通信傍受

司法傍受に関しては、「犯罪の進展への司法の対応に関する2004年3月9日の法律第2004-204号」[30]により、組織犯罪（Ⅲ2（1）参照）に関する現行犯捜査又は予備捜査[31]において行い得る通信傍受に関する規定が置かれた。これまで予審段階で行われることになっていた司法傍受を、一定の対象犯罪に限り予審の前の捜査においても行うことができるようにしたものである[32]。これは、自由・勾留裁判官（juge des libertés et de la détention）[33]が共和国検事の請求に基づき許可するものである。許可期間は、最長15日（2011年に1か月に延長）であり、1度に限り同一条件で延長することができる。

4　接続データの取得

行政による接続データの取得に関しては、「テロ対策並びに治安及び国境管理に関する2006年1月23日の法律第2006-64号」（以下「2006年テロ対策法」という。）[34]及び「2014年から2019年までの軍事プログラム並びに国防及び国内治安に関する2013年12月18日の法律第2013-1168号」（以下「2013年軍事プログラム法」という。）[35]において法整備が行われた。

2006年テロ対策法は、インターネット通信の接続を提供する事業者に通信記録を保存する義務を課し、国家警察及び憲兵隊のうち、テロ防止に関する任務について個別に任命され、正規に授権された警察職員に対し、テロ行為を未然に防止するために通信記録のデータを要求する権限を与えた。この法により要求できるデータは、通信の内容自体ではなく、電子通信サービスへの加入又は接続の番号の同定に関する技術的なデータ、特定の人物の加入又は接続の番号の全ての明細目録、利用された端末の位置に関するデータ、受信先又は送信先の番号リスト、通信の時間及び日時に係る加入者の通信に関する技術的なデータに限定された。このデータの

---

[29] Oliver Gohin et Xavier Latour (directeurs de publication), *Code de la sécurité intérieure 2016*, 2e éd, Paris: LexisNexis, 2016, p.342.

[30] Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité. 治安を重視した刑事司法立法であると評価されている。白取祐司『フランスの刑事司法』日本評論社, 2011, pp.91-97; 末道康之「フランス刑事立法の動向―Loi Perben 2について―」『南山法学』29(2), 2006.1, pp.123-165.

[31] 予審開始前に警察又は憲兵隊が職権で又は検察官の請求により行う捜査（『フランス法律用語辞典　第3版』三省堂, 2012, p.182）。

[32] 末道　前掲注[30], p.145.

[33] 2000年に設置された地位。それまで予審判事が行っていた未決勾留に付す旨及び更新の決定を行う。また、テロ犯罪のための警察留置の延長等の人身の自由に関する決定権限を有する。白取　前掲注[30], pp.75-76参照。

[34] Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

[35] Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

要求は、内務大臣直属の担当官の許可に従って行われる。担当官の任命は、内務大臣の提案に基づきCNCISが行う。CNCISは、データの伝達の方法について検査する権限を持ち、違反や権利侵害があったときは内務大臣に勧告を行う。(36)これらの規定について、憲法院（Conseil constitutionnel）(37)は、適用範囲を「司法機関の指揮又は監督の下で行われるのではない行政権の責任のみにおいて行われる純粋に行政的な警察の手段」に限定する判決を下した(38)。

2013年軍事プログラム法は、通信記録のデータの提供に関する規定について、2006年テロ対策法で定めた行政権限を拡大するものであった。すなわち、提供の要求の目的をテロ行為の防止から、1991年通信傍受法における行政傍受の諸目的に拡大すること、アクセスできる権限を有するのは国内治安、防衛、経済及び予算を担当する大臣部局の職員のうち行政傍受の任務について個別に指定され適法に授権されたものとすること、及び保存された情報だけではなくリアルタイムでのデータへのアクセスを認めることである。(39)

一方、司法手続における接続データの取得に関しては、2016年テロ対策強化法の制定までは、明確な規定はなく、以下のように様々な規定が適用されていた(40)。

まず、司法警察員は、郵便電子通信法典（Code des postes et des communications électroniques）L.第34-1条の規定に基づいて、犯罪の調査、確認及び追跡のために、通信事業者に対して最長1年の間、専ら利用者の特定、通信の技術的性格及び端末機器の位置情報に係るデータを保存するよう求めることができる。また、司法警察員は、現行犯捜査においては刑事訴訟法典第60-2条の規定により、予備捜査においては同法典第77-1-2条の規定により、共和国検事の請求に基づく自由・勾留裁判官の許可の下、通信事業者に対し、1年を超えない範囲で、当該事業者のサービスの利用者が閲覧した情報内容の保存のため適切な全ての措置を採るよう求めることができる。証拠調べにおいても、同法典第99-4条により、同様の請求を予審判事の許可により行うことができる。

5　2015年情報活動法

（1）制定の経緯

2015年3月19日に、情報活動政策に関する原則及び目的を定めることに加え、総合的な法の枠組みを作り、情報機関の活動を保障するとともに、統制を強化することを目的として(41)、情報活動に関する法律案が国民議会に提出された。

法案は、国民議会、元老院及び両院協議会の審議により修正が加えられた後、2015年6月23日に元老院において、同月24日に国民議会において、それぞれ可決された。7月23日、憲法院は、緊急時に首相の許可等なしに位置情報の取得又は通信傍受のための技術装置の設置及び利

---

(36)　詳細については、高山直也「フランスのテロリズム対策」『外国の立法』No.228, 2006.5, pp.113-132. <http://dl.ndl.go.jp/view/download/digidepo_1000363_po_022807.pdf?contentNo=1>

(37)　法律の憲法適合性を審査する憲法裁判所である。法律の議会での議決後、大統領が審署するまでの間に事前審査を行う権限を有する（滝沢　前掲注(28), pp.210-211）。

(38)　Conseil constitutionnel, Décision n° 2005-532 DC du 19 janvier 2006; Gohin et Latour (directeurs de publication), *op.cit.*(29), p.342.

(39)　詳細については、情報セキュリティ大学院大学「インターネットと通信の秘密」研究会『インターネット時代の「通信の秘密」各国比較』2014, p.74.（曽我部真裕執筆部分）<http://lab.iisec.ac.jp/~hayashi/2014626%20revised.pdf>

(40)　“Rapport fait au nom de la commission des lois constitutionnelles, de la législation et de l’administration générale de la république, sur le projet de loi (n° 3473),” N° 3515, Assemblée nationale, 18 février 2016, pp.95-96.

(41)　“Projet de loi relatif au renseignement,” *op.cit.*(2), pp.3-5.

用を可能とした規定並びに外国と送受信する通信データの取扱いに関する規定を違憲としたものの、その他の規定については合憲と判断した(42)。大統領の審署を経て、7月25日に、違憲と判断された条項を除いた法律が成立した。

なお、違憲とされた外国と送受信する通信データの取扱いに関する規定については、修正の上、憲法院の判決を経て、「国際電子通信の監視措置に関する2015年11月30日の法律第2015-1556号」(43)として成立している。

（2）主な内容

まず、情報活動の原則を定める（国内安全法典L.第801-1条）。私生活の尊重は法律によって保障されると述べ、公的機関が私生活の尊重を侵すことができるのは、法律が定める公益上の必要がある場合であり、法律に規定する範囲内において、比例原則(44)を遵守したときに限るとする。

法律により特定された技術による情報収集が認められる目的は、次の7項目の保護又は促進であると規定された。①国の独立、領土の保全及び国防、②対外政策における重大な利益、ヨーロッパ及び国際的な取決めの履行並びにあらゆる形態の外国の干渉の防止、③フランスの経済、産業及び科学技術に関する重大な利益、④テロの防止、⑤共和政体に対する攻撃、戦闘集団、民兵等として解散された集団の再結成若しくは維持又は公安に重大な攻撃をもたらす性質の集団的暴力の防止、⑥組織犯罪の防止、⑦大量破壊兵器の拡散の防止（同法典L.第811-3条）。

法律により特定された技術による情報収集には、アルゴリズムを用いてテロの脅威を監視する装置の使用（同法典L.第851-3条）、偽装携帯電話基地局のような会話の遠隔探知やコンピュータデータの取得が可能となる装置による接続データの収集（同法典L.第851-6条）等が新しく加えられた。偽装携帯電話基地局は行政傍受に使用することもできることとされた（同法典L.第852-1条Ⅱ）。

情報収集技術の使用に関し首相が許可をするに当たっては、緊急の場合を除き、事前に新設される国家情報技術監視委員会（Commission nationale de contrôle des techniques de renseignement: CNCTR）の意見を求めることとされた。首相の許可及びCNCTRの意見は、通信内容の傍受だけではなく、接続データの収集を行うためにも必要となった。（同法典L.第821-1条）

CNCTRは、CNCISに代わって設置される独立の行政機関であり、国民議会及び元老院の議員各2人、コンセイユ・デタの構成員2人、破毀院（Cour de cassation）(45)の司法官2人、電子通信・郵便規制機関（Autorité de régulation des communications électroniques et des postes）の長の提案に基づき任命される電子通信分野の有識者1人の計9人の委員で構成される（同法典L.第831-1条）。CNCTRは、前述の意見の提出要求による事前統制のほか、事後の適法性審査及び中止勧告の権限を有する。また、事後統制に係る新しい制度として、コンセイユ・デタが、この法律に定める国の情報活動による利害についての提訴を受けて審査を行うこととされた（同法典L.第841-1条）。(46)

---

(42) Conseil constitutionnel, Décision n° 2015-713 DC du 23 juillet 2015.

(43) Loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales.

(44) 目的と手段の均衡を要求する法原則（高橋和之ほか編『法律学小辞典　第5版』有斐閣, 2016, p.1118）。

(45) 司法系統における最上級審の裁判所（「破毀院の役割」Cour de cassation website <https://www.courdecassation.fr/cour_cassation_1/in_six_2850/26085_26412_35486_3727/38498_12398_17652.html>）。

６　2016 年テロ対策強化法

2015 年 11 月のパリ同時多発テロ後、フランスでは緊急状態が宣言された。政府は、緊急状態のような臨時的な措置のほか、テロに対応した恒久的な制度改革が必要であるとして、2016 年 2 月にテロ対策強化法案を提出し、同年 6 月 3 日に 2016 年テロ対策強化法として成立した。

法案の目的は、次の 3 点である。①組織犯罪対策、特にテロ対策の実効性の強化、②刑事訴訟手続の間、特に捜査及び予審の間の保護の強化、③刑事訴訟手続の簡素化。提案理由説明では、これらの目的は、行政手続と司法手続の間の均衡を強化し、「2015 年 7 月 24 日の法律により情報活動に関して許可された捜査手段が司法に関しても利用できることを許容する」と書かれている(47)。

2016 年テロ対策強化法は、捜査手段の強化策として、刑事訴訟手続において偽装携帯電話基地局等を使用した接続データの取得を認めるほか、予備捜査及び予審の段階の夜間における家宅捜索、探知機の設置によるデータの取得等を認めている。(48)

Ⅲ　フランスにおける偽装携帯電話基地局に関する法制

１　行政による使用

（1）概要及び目的

行政による偽装携帯電話基地局の使用については、2015 年情報活動法により規定が加えられた国内安全法典に規定されている。

偽装携帯電話基地局の使用により端末機器若しくは利用者契約番号を特定する接続データ、又は使用されている端末機器の位置に関するデータを取得することができ（同法典 L.第 851-6 条）、また、通信内容を傍受することができる（同法典 L.第 852-1 条Ⅱ）。

接続データの取得、通信内容の傍受のいずれについても、使用目的は、①国の独立、領土の保全及び国防、②テロの防止、③共和政体に対する攻撃、戦闘集団、民兵等として解散された集団の再結成若しくは維持又は公安に重大な攻撃をもたらす性質の集団的暴力の防止に限定される。他の情報収集技術の使用目的である経済的利益の保護等は含まれない。

なお、偽装携帯電話基地局は、国内安全法典において「刑法典第 226-3 条 1° に規定する機器又は技術装置」と規定されているものに含まれる。具体的には、刑法典第 226-3 条 1° に基づく同法典 R.第 226-1 条により授権された首相の命令（アレテ）において規定されている、同法典第 226-15 条第 2 段落に規定する犯罪（電子回線上の通信の傍受等又はそのような傍受を行うことができる機器の設置）を構成し得る操作である、電子情報通信網上で発信され、伝達され又は受信される通信の傍受、盗聴、分析、再送信、記録又は処理を行うために作られた機器（ハードウェア及びソフトウェアを含む。）に該当する(49)。

---

(46)　詳細について、齊藤笑美子「フランス　情報活動に関する法律（海外法律情報）」『論究ジュリスト』No.16, 2016.冬, pp.102-103; 豊田透「【フランス】国による情報監視技術の使用を規定する法律」『外国の立法』No.265-1, 2015.10, pp.10-11. <http://dl.ndl.go.jp/view/download/digidepo_9514875_po_02650105.pdf?contentNo=1>

(47)　“Projet de loi renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l’efficacité et les garanties de la procédure pénale,” N° 3473, Assemblée nationale, 3 février 2016, pp.5-6.

(48)　2016 年テロ対策強化法の詳細について、豊田透「【フランス】2016 年テロ対策強化法」『外国の立法』No.268-2, 2016.8, pp.8-9. <http://dl.ndl.go.jp/view/download/digidepo_10168961_po_02680204.pdf?contentNo=1>

(49)　Arrêté du 4 juillet 2012 fixant la liste d’appereils et de dispositifs techniques prévue par l’article 226-3 du code pénal, Annexe I, 1.

（2）実施主体

偽装携帯電話基地局を使用した措置の実施の許可を受けることができる機関は、コンセイユ・デタの議を経るデクレ(50)で指定された情報専門機関（国内安全法典 L.第 811-2 条）及び CNCTR の意見を受けてコンセイユ・デタの議を経るデクレで指定された機関とされている（同法典 L.第 811-4 条）。

情報専門機関として指定されているのは、対外安全保障総局（Direction générale de la sécurité extérieure: DGSE）、国防警備保安局（Direction de la protection et de la sécurité de la défense: DPSD）、軍事情報局（Direction du renseignement militaire: DRM）、国内治安総局（Direction générale de la sécurité intérieure: DGSI）、関税情報調査局（Direction nationale du renseignement et des enquêtes douanières: DNRED）及び資金洗浄対策情報局（Traitement du renseignement et action contre les circuits financiers clandestins: TRACFIN）である（同法典 R.第 811-1 条(51)）。

CNCTR の意見を受けてコンセイユ・デタの議を経るデクレで指定された機関については、実施理由及び実施可能な技術がそれぞれデクレにより指定される。L.第 811-4 条により偽装携帯電話基地局の使用の許可を受けることができる機関として指定されたものは、国家警察の一部機関、国家憲兵隊（gendarmerie nationale）の一部部局、地方警察の一部機関及び国防省の下にある各憲兵隊である（同法典 R.第 851-4 条(52)）。

（3）実施の許可

実施の許可の申請は、国防大臣、内務大臣又は経済・予算・関税担当大臣が行う。この申請には、以下の事項を明記する。①実施する技術、②申請部局、③目的、④措置の理由、⑤許可の有効期間、⑥関係する人、場所、乗物。（同法典 L.第 821-2 条）

使用の許可は、CNCTR の意見を受けて首相が行う（同法典 L.第 821-1 条）。絶対的緊急性がある場合には、首相は CNCTR の意見をあらかじめ得ることなく許可することができる。この場合、首相は、許可から 24 時間以内に、絶対的緊急性があると判断した理由を含め、許可について CNCTR に届け出るものとする。（同法典 L.第 821-5 条）

許可請求は、CNCTR の委員長に伝えられ、その後 24 時間以内に首相に意見が提出される。ただし、CNCTR の総会又は小委員会(53)が審査を行うときは、72 時間以内とする。この時間を過ぎて意見の提出がなかったときは、意見の提出があったものとみなす。（同法典 L.第 821-3 条）

許可の期間は、接続データの取得については、最長 2 か月間とし、同一の期間で更新することができる（同法典 L.第 851-6 条Ⅰ）。通信内容の傍受については 48 時間とし、更新可能である（同法典 L.第 852-1 条Ⅱ）。

（4）機器の使用制限

偽装携帯電話基地局は、CNCTR において管理する特別登録簿に登録される。同時に使用す

---

(50) デクレ（Décret）は命令の一種である。このうち、コンセイユ・デタの意見を徴することが義務付けられているデクレを「コンセイユ・デタの議を経るデクレ」という。

(51) Décret n° 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement により制定。

(52) Décret n° 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure により制定。

(53) 国民議会及び元老院議員である委員以外の委員による会議。国内安全法典 L.第 831-2 条

ることができる偽装携帯電話基地局の数は、CNCTR の意見を受けて首相が決定する。（同法典 L.第 851-6 条Ⅱ及びⅣ）

（5）対象者以外による通信の内容の傍受

許可対象者の周辺人物（entourage）である 1 又は複数の者が許可の目的に関する情報を提供している疑いがあると信ずる確実な理由があるときは、通信内容を傍受することができる（同法典 L.第 852-1 条Ⅰ）。この規定は、偽装携帯電話基地局を使用する場合に限らず、行政傍受全般に適用される。

（6）データの保存及び破棄

首相の部局[54]は収集した情報又は文書を集中的に管理する。具体的には、接続データについては、使用の許可に関連するものであれば、収集してから 4 年間保存し（同法典 L.第 851-6 条Ⅲ、L.第 822-2 条Ⅰ 3°）[55]、使用の許可と無関係であることが判明したときは、収集から 90 日を上限として、直ちに破棄する（同法典 L.第 851-6 条Ⅲ）。傍受した通信内容のデータについては、収集してから 30 日以内に、また、通信内容が傍受の許可と無関係であることが判明したときは直ちに破棄するものとする（同法典 L.第 852-1 条Ⅱ、L.第 822-2 条Ⅰ 1°）。集中管理の規定及び許可と無関係であることが判明した際の破棄の規定は、偽装携帯電話基地局を使用した場合に特有の規定である。

２　刑事訴訟手続における使用

（1）概要

刑事訴訟手続における偽装携帯電話基地局の使用については、2016 年テロ対策強化法により規定が加えられた刑事訴訟法典に規定されている。

偽装携帯電話基地局の該当する概念については、国内安全法典と同様である。

偽装携帯電話基地局の使用により端末機器若しくは利用者契約番号を特定する接続データ、又は使用されている端末機器の位置に関するデータを取得することができ、また、通信内容を傍受することができる（刑事訴訟法典第 706-95-4 条及び第 706-95-5 条）。

偽装携帯電話基地局を使用することができるのは、組織犯罪に係る特別手続[56]の対象となる犯罪に関して、捜査のため必要があるとき（同法典第 706-95-4 条）及び予審の証拠調べのため必要があるとき（同法典第 706-95-5 条）である。対象犯罪は、同法典第 706-73 条及び第 706-73-1 条が適用される犯罪であり、故殺罪、組織的集団による拷問、略取又は誘拐の罪、資金洗浄罪、テロ犯罪、薬物の取引の罪等がこれに含まれる[57]。

54　具体的には、閣僚間統制団（Groupement interministériel de contrôle: GIC）を指す（国内安全法典 R.第 851-7 条）。GIC の任務は、同法典 R.第 823-1 条に規定されている。

55　L.第 851-6 条Ⅲ 1°は、「L.第 822-2 条に規定する条件において保存する」と規定するが、L.第 822-2 条は複数の消去期間を定めているため、ここで記したように L.第 822-2 条Ⅰ 3°が適用されることは、必ずしも文理上明らかとはいえない。本稿の記述は、L.第 822-2 条Ⅰ 3°は接続データの収集に関する総則である L.第 851-1 条に規定する情報及び文書の消去期限を 4 年と定めていることから、L.第 851-6 条Ⅲ 1°についても同様に解されるとする以下の解説による。Gohin et Latour (directeurs de publication), *op.cit.*㉙, p.329.

56　2004 年に新設された手続。この手続においては、特別裁判所が裁判管轄を有し、大幅な捜査権強化が図られている。白取　前掲注㉚

（2）使用の許可

捜査のため必要があるときは、自由・勾留裁判官が共和国検事からの申請により司法警察員に偽装携帯電話基地局の使用を許可する。接続データの取得に関する許可の期間は、最長1か月であり、同一条件により1回更新することができる。通信内容の傍受に関する許可の期間は、最長48時間であり、同一条件により1回更新することができる。証拠の滅失等（dépérissement）又は人若しくは財産に対する重大な侵害のおそれが切迫している緊急の場合には、これらの許可は共和国検事が行うことができる。この場合、24時間以内に自由・勾留裁判官の確認を得なければならない。（同法典第706-95-4条）

予審の証拠調べのため必要があるときは、予審判事が共和国検事の意見を受けて司法警察員に偽装携帯電話基地局の使用を許可する。接続データの取得に関する許可の期間は、最長2か月であり、同一条件により合計6か月を超えない範囲で更新することができる。通信内容の傍受に関する許可の期間は、最長48時間であり、同一条件で1回更新することができる。（同法典第706-95-5条）

これらの許可は、書面の、かつ理由を付した（motivée）命令の対象となる。この命令は裁判行為ではなく、上訴の余地はない。（同法典第706-95-6条）

（3）通信傍受に係る規定の準用

通信内容の傍受に関しては、通常の通信傍受に係る刑事訴訟法典の以下の規定を準用する（同法典第706-95-4条Ⅱ及び第706-95-5条Ⅱ）。

①予審判事（捜査のため必要があるときは自由・勾留裁判官。以下同じ。）又は司法警察員は、傍受及び録音の各措置を調書に記録し、録音は封印すること（同法典第100-4条）、②予審判事又は司法警察員は、真実発見に有用な通信を反訳し、調書に記載すること（同法典第100-5条）、③公訴時効期間が満了したときは、録音物は、共和国検事又は検事長の請求により廃棄すること（同法典第100-6条）、④国民議会議員、元老院議員、弁護士の回線に関する特例（同法典第100-7条）。

なお、取得した接続データに関しても、①、②と同様の取扱いをすることとされており（同法典第706-95-9条）、③に関しては、公訴時効期間の満了時又は確定判決が出された時に消去することとされている（同法典第706-95-10条）。

（4）目的の限定

接続データの取得及び通信内容の傍受は、許可及び許可をした判事の監督の下で有効であり、許可の対象である犯罪の調査及び確認以外の目的で行った場合には無効となる。一方、接続データの取得及び通信内容の傍受が許可決定の対象以外の犯罪に関連していたとしても、そのことがその犯罪に係る手続の付帯的無効原因とはならない(58)。（同法典第706-95-7条）

---

(57) 刑事訴訟法典第706-73条が適用される罪の詳細について、末道　前掲注(30), pp.142-143参照。同法典第706-73-1条が適用される罪には、組織的集団による詐欺罪、個人情報を扱うシステムに対する侵害罪、組織的集団による逃走罪等がある。

(58) 1991年通信傍受法の適用において、A犯罪事実のための通信傍受において、別のB犯罪事実に関する会話が傍受されたときに、これを公判に提出できるかという問題があった（白取祐司「フランス」奥平康弘・小田中聰樹監修, 右崎正博ほか編『盗聴法の総合的研究』日本評論社, 2001, pp.344-345）。この問題に対してB犯罪事実に関する傍受が付帯的である限り有効であるとするものである。許可を得て行う捜査関係手続が許可対象犯罪以外の犯罪に係る手続の付帯的無効原因とならないとする規定は、刑事訴訟法典第78-2条（身分検査）等にも見られる。

（5）情報機関との関係

共和国検事、予審判事又は司法警察員は、デクレに列挙する内務大臣管轄下の各機関の権限ある職員に偽装携帯電話基地局の使用のための要求をすることができる（同法典第 706-95-8 条）。

（6）傍受する通信内容の限定

傍受する通信内容は、許可の対象となる者又は許可の対象となる通信（liaison）に関するものに限る（同法典第 706-95-10 条）。

３　携帯電話基地局に関する法制の特徴

他の方法による接続データの取得及び通信傍受と比べ、偽装携帯電話基地局を用いる方法による場合の規定の特徴は、次のようにまとめられる。

①使用目的が限定されている。行政による使用ではテロ防止等の 3 目的に、刑事訴訟手続における使用では組織犯罪を対象とした場合に限られている。②許可の期間が短い。③行政による使用においては、データの保存期間が短くなる可能性がある。

これらは、携帯電話基地局による接続データの取得及び通信傍受が、多くの種類の情報を広い範囲で収集できるものであり、より私生活及び通信の尊重への影響の大きい手段であることを反映したものである。

４　実施状況

CNCTR は、2015 年 12 月 12 日に発表した第 1 回の年次活動報告において、2015 年 10 月 3 日から 2016 年 10 月 2 日までの 2015 年情報活動法による監視対象者数は 20,282 人であり、その 47％に当たる 9,624 人がテロ防止の目的での監視対象であったと明らかにしている(59)。また、コンセイユ・デタには、2015 年情報活動法に規定する情報技術又は国の安全に係る情報ファイルに関する提訴を受けて審査を行う特別部（formation spécialisée）が設けられた。この特別部は、2016 年 10 月 19 日に初めて 15 の判決を出した(60)。

おわりに

通信手段の発達は、テロリストや犯罪者にも新しい、より秘匿された情報交換の方法を提供している。捜査機関や情報機関は、新しい捜査手段を与えられなければ、通信手段の発達がなければ捕捉できたであろうテロリストその他の犯罪者を取り逃がすおそれもある。それは、単に捜査機関や情報機関の不利益となるにとどまらず、捜査機関や情報機関が目的とする国・国民の安全をも脅かすものである。

他方、新しい捜査手段は、従来の捜査手段にはなかった問題点を伴うこともある。偽装携帯電話基地局の場合には、標的とする人又は情報の範囲にとどまらない広範な情報収集能力と、

---

(59) Christophe Cornevin, “20.282 personnes espionnées en un an sur le territoire français,” *Le Figaro.fr*, 13 décembre 2016. <http://www.lefigaro.fr/actualite-france/2016/12/13/01016-20161213ARTFIG00102-20282-personnes-espionnees-en-un-an-sur-le-territoire-francais.php>

(60) “Contrôle des techniques de renseignement,” 19 octobre 2016. Conseil d’ État website <http://www.conseil-etat.fr/Actualites/Communiques/Controle-des-techniques-de-renseignement>

捜査の不可視性が問題となっている。前者により、厳密な審査による令状の発行等で事前に統制したとしても、機器の特性上、対象者以外の一般の人の通信も傍受してしまうことになり、目的外の傍受を厳重に監視しない限り、必要以上の私生活及び通信の尊重への侵害を引き起こすおそれがある。また、後者により、仮に不当な手続により傍受をされていたとしても、傍受された側はそれを知る方法がないため、傍受する側において十分な統制が働かなければ、私生活等への侵害の有無すらわからない不安定な状態に置かれる。

クリュスラン事件判決においても明らかなように、厳重な統制の仕組みが明確にされることは、これらの問題点を解決し、人権を保障するための1つの有効な方法であるが(61)、反面、捜査機関や情報機関の活動を制約するものでもある。

それでもなお、この方法に対しても懸念が示される(62)のは、仮に統制の仕組みがあったとしてもなお、新しい捜査手段によって、安全の保障による利益よりも重大な人権等に関する不利益が生ずることがあるのであれば、そもそも新しい捜査手段に関する権限を付与すべきではないといえるためである。

また、捜査や治安に係る情報収集の実態は、性質上明らかにされることが少ない。このような条件下で、新しい捜査手段の導入と統制をどのように行うのが適当かを判断することには、極めて困難な考察を要するものであり、さらに様々な立法事例を検討する必要がある。

（かわにし　あきひろ）

---

(61) 2015年情報活動法について、情報活動の技術手段の拡大に対応した法的枠組を設定し、統制できるようにしたと評価したものとして、Oliver Desaulnay and Romain Ollard, “Le renseignement français n’est plus hors-la-loi,” *Droit Pénal*, 27(9), Septembre 2015, pp.6-12.

(62) 2015年情報活動法について、市民の基本的な権利、私生活の尊重を侵害するものであり、テロから守るはずの民主主義をかえって覆す危険性もあるとの懸念を示したものとして、Nicolas Catelan, “Cadre juridique du renseignement: un moindre mal?” *RSC: revue de science criminelle et de droit pénal comparé*, 2015(4), octobre-décembre 2015, pp.922-940.