The interception of communication in France and Italy – what relevance for the development of English law?

Francesca Galli*

International and European Law Department, Faculty of Law, Maastricht University, The Netherlands

This article examines the distinctive features of the interception of communications regimes in the jurisdictions of France and Italy, focusing only on telephone tapping provisions. This comparative study focuses on the actors involved in the interception of communications either for authorisation or execution purposes, as well as its scope and duration. Finally, the article will attempt to assess the relevance of foreign experiences for the development of English law. The potential use of the information obtained as evidence at trial will be thus particularly relevant to the discussion.

Keywords: interception of telecommunication; terrorism; intercept as evidence

Introduction

This article examines the distinctive features of the interception of communications regimes (as well as envisaged reforms) in the jurisdictions of France and Italy, focusing only on telephone tapping provisions. Most of the provisions under scrutiny existed in principle well before 11 September 2001, but increased concern about terrorism has highlighted their practical importance. This comparative study focuses on the actors involved in the interception of communications either for authorisation or execution purposes, as well as its scope and duration. The potential use of the information obtained as evidence at trial is particularly relevant to the discussion. Finally, the article attempts to assess the relevance of foreign experiences for the development of English law. A particular feature of the scene in the United Kingdom is the fact that under British law intercept evidence is not admissible in criminal proceedings. This potentially makes it harder to prosecute suspected terrorists, which may in turn lead the government to look to administrative measures such as control orders or terrorism prevention and investigation measures (TPIMs) as a means of restraining them. As detailed in the article the growth of these administrative measures has caused some commentators to argue that the ban on the use of intercept evidence at criminal trials ought to be lifted.

The European Convention on Human Rights (ECHR) does not prevent the use of intercept evidence either under article 6\(^1\) or under article 8.\(^2\) Particularly, under article 8, restrictions are explicitly admitted in the name of a public interest in the prevention of the most serious offences, national security, and the protection of other members of society.

---

\(^1\)The article has been drafted in June 2015 and further updates and reform under proposal or negotiation have been only tangentially mentioned in footnote where relevant.

\(^2\)Email: Francesca.galli@maastrichtuniversity.nl

\(©\ 2016\) The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.
Article 8 of the ECHR has had a significant impact on the development of comprehensive statutory regulations of surveillance techniques at the domestic level. States enjoy a certain discretion, subject to article 8(2): the measures have to be in accordance with the law, have a legitimate aim, such as national security, be necessary in a democratic society and strictly proportionate. A crucial factor for proportionality is the existence of sufficient safeguards to ensure that the measures are not carried out in an excessive or arbitrary manner. Domestic legal provisions, written and unwritten, must identify with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities to prevent any misuse of power or arbitrary interferences with the convention’s rights. The European Court of Human Rights (ECtHR) has introduced the two criteria of accessibility and predictability of the law in relation to the right to privacy, pointing out that the restriction of free communication constitutes a direct interference with article 8 of the ECHR. The ECtHR has explicitly accepted the necessity of having some degree of surveillance in order to effectively counter serious threats. However, it has stressed that surveillance techniques must represent the *extrema ratio* and only be permissible if ‘the establishment of the facts by any other method is without prospects of success or considerably more difficult’.

### Interception of communications in France

A preliminary distinction must be drawn between telephone tapping during a judicial investigation for the detection and the investigation of a crime (judicial interceptions), and interceptions authorised by the executive for security reasons (administrative interceptions) called *interceptions de sécurité*. Law 646/91 (as amended by Law 1138/2002, Law 204/2004, Law 64/2006, and Law 1432/2012) provides the legal framework for both judicial (codified under article 100 ff of the French *Code de Procédure Pénale* – CPP-F) and administrative interceptions. Article 1 of the Law 649/91 reaffirms the principle of the secrecy of communications, from which only the public authority can derogate under the circumstances of public interest recognised and restricted by the law. Interceptions are thus forbidden in principle and authorised in exceptional conditions only. For instance, the wording ‘*lorsque les nécessités de l’information l’exigent*’ has been interpreted by the academic literature so as to consider judicial interceptions as an *extrema ratio* where other investigative methods would be unsuccessful or unavailable (under the principle of subsidiarity).

Unlawful interception is a criminal offence. The French *Code Pénal* (CP-F) provides for severe penalties (one to three years imprisonment and a fine of 45,000€) to punish the malicious interception, diversion, use or disclosure of correspondence sent, transmitted or received by means of telecommunication, or the setting up of a device designed to produce such interceptions (arts 226(15) and 432(9) of the CP-F).

In history, the interception of communications in France already took place in the nineteenth century but was never properly ‘framed’ by statute. In the absence of any legislation, the legal regime in respect of interceptions was built on case law. It was generally assumed that a *juge d’instruction* could order an interception as part of that officer’s general evidence-gathering powers, but whether it was legal for the police to do it was uncertain. Then in the *Affaire Baribeau* in 1989, the Assemblée plénière of the Cour de Cassation considered the interceptions of communications during autonomous police investigations (even *in flagrante*) – hence not in connection with a judicial investigation – to be illegal and incompatible with article 8 of the ECHR and with article 66 of the constitution according to which the judicial authority is the guardian of individual freedoms. In its
judgment of 15 May 1990, the Chambre Criminelle of the Cour de Cassation further maintained that:

an interception warrant must be issued by a judge and the measure has to remain under his supervision in order to gather evidence of an offence threatening public order; the interception is to be obtained without any trick or stratagem; and the transcriptions have to be accessible to the parties at trial in the respect to the defence rights (principle of loyalty).20

Subsequently, the French regime was condemned by the Strasbourg Court on the ground that article 8 of the ECHR requires that any interference with private communications be grounded upon legal provisions, which, as French law stood then, they were not.21 As a consequence, parliament was induced to legislate on the matter.22 Debates were hasty and the legitimacy of the interception as such was never questioned (except marginally and in relation to interceptions that were administrative rather than judicial). The regime established in 1991 seems to fulfil the requirements of the ECHR.23

Judicial interceptions

Judicial interceptions were for a long time an informal practice, developed on the basis of article 81 and arts 151–152 CPP-F (framing the scope and implementation of the investigating judge’s powers). Following the enactment of Law 646/91, judicial interceptions are now codified in detail under article 100 and following of the CPP-F. For the judicial investigation (only during the phase of instruction) of the most serious offences (crimes and délits), punishable with a minimum sentence of two years of imprisonment,24 the juge d’instruction may issue a warrant for the interception, recording, and transcription of telephone conversations.

Specific procedural formalities are applicable in this context: the placement of the recordings under closed official seal; the drafting of an official record of both the interception and recording operations (mentioning the date and time where the operation started and ended); the transcription of any correspondence which might be relevant for the investigation25; and the destruction of the recordings upon request of the district/public prosecutor on the expiry of the limitation period for the prosecution.26 When first imposed, an interception cannot last longer than four months. Such an initial period can, however, be extended as long as necessary for investigative purposes.

Over the years the legal regime of judicial interceptions has been considered by some to be too strict and inadequate for the purpose of an effective fight against organised crime. In fact, it only allowed interceptions during the course of judicial investigations — that is to say, cases in which a juge d’instruction was involved.

In response to this difficulty, Law 204/2004 extended the possibility to use judicial interceptions to preliminary and in flagrante police investigations (i.e. to cases where no instruction had yet been instituted) for a limited number of serious offences listed in article 706(73) of the CPP-F (‘organised crime’ offences). They are authorised (and supervised) by the juge des libertés et de la détention on the application of the district prosecutor and cannot last longer than 15 days, once renewable under the same conditions of form and duration.27 The same procedural safeguards applicable to interceptions during judicial investigations on the basis of article 100 and following of the CPP-F are relevant in this context, reinforcing the judicial control on these operations as required by article 706 (95) of the CPP-F.28

The article regrettably does not require informing the judge prior to the interception and hence allows the police to carry out the intercept in the hope of obtaining permission
The effectiveness of such a delayed judicial scrutiny is doubtful. However, the Conseil Constitutionnel has considered the provisions as being in compliance with the right to privacy and all other constitutional principles.

Under the French legal regime, judicially intercepted information is admissible at trial, and nobody has ever suggested that it should not be.

**Administrative interceptions**

The administrative interception of communications, called ‘security interceptions’, represents a traditional practice, which has become particularly important for anti-terrorism purposes. Such interceptions are a preventive instrument, and they are not subject to the commission of an offence. They are considered in compliance with article 8 of the ECHR as Strasbourg case law allows for interferences with private life for the defence of a democratic state.

The current legal regime is regulated under Law 646/91, articles 3–19. Prior to that, the regime of administrative interceptions was vague: no clear list of the grounds for intercepting existed and the risk of arbitrary use was great.

Article 4 of the 1991 Law provides that the prime minister may authorise the interception of communication in order to gather information in relation to national security, the protection of French scientific and economic resources or the prevention of terrorism and organised crime (the latter mostly relating to drug trafficking offences). The information gathered can only serve such purposes. ‘Fishing expeditions’ are prohibited. The prime minister’s authorisation is a written and reasoned warrant which is issued on the basis of the written and reasoned application of the minister of defence, the minister of interior, or the minister of customs. The law has thus strictly limited the number of people who can authorise/apply for an administrative interception. The decision is immediately sent to the Commission nationale de contrôle des interceptions de sécurité (CNCIS), which ensures compliance with procedural rules but most importantly with the right to privacy. As in the case of judicial interceptions, the interception can last for up to four months, renewable under the same condition of form and duration.

The Groupement Interministériel de Contrôle, created in 1960, works under the authority of the prime minister to provide centralised implementation of administrative interceptions within the context of the rules explained in the previous paragraph. With regard to the execution of these means, an interesting feature in France concerns the execution of administrative interceptions and their transcription, which relies upon ‘les personnels habilités’ (authorised personnel) and thus often implies a police officer (not necessarily a member of the police judiciaire).

Since 2002, the recordings themselves have been automatically erased at the latest after ten days following the end of the operation. The transcripts of the recordings are destroyed once their storage is no longer necessary for the previously mentioned preventative purposes. A report of each operation is drafted and mentions the date and time where the interception started and ended.

Finally, the law requires the prime minister to specify a maximum number of intercepts that may take place in the course of the year. Originally resulting from technical constraints, this system is meant to provide a quick removal of less useful interceptions so that preventive interceptions remain an exceptional means of investigation. However, the law in itself does not provide for any overall maximum, and administrative interceptions have been constantly increasing during the last few years. Most operations relate to organised crime (66% in 2012), terrorism (19%) and national security cases. It is mainly in national security cases that renewals are made (42%).
If administrative interception reveals evidence of a criminal offence, the case file is transferred to the public prosecutor (article 40 of the CPP-F). The material so obtained can then justify the issue of a further warrant for judicial interceptions.

Article 6 of Law 64/2006 has introduced a new administrative procedure for the requisition from service providers of technical data of communication (telephone or internet) for the purpose of terrorism prevention. The scope of the requisition does not include the content of the communications. The execution of such a measure is in the hands of authorised police personnel. The Bill mentioned as purposes of the requisition both the prevention and the suppression of terrorism. The Conseil Constitutionnel ruled that a measure under the sole responsibility of the executive power, in the absence of any judicial scrutiny, must only aim at the preservation of public order and the prevention of offences and not at the suppression of terrorism. The provision was subject to a sunset clause and would have elapsed at the end of 2012; Law 1432/2012 made it applicable until 31 December 2015.

Security interceptions have long been controversial due to past political interference. Since 1991, they have thus been placed under the authority of a national commission, the CNCIS, an independent administrative authority. As already mentioned, the CNCIS is in charge of supervising respect for the existing provisions (particularly for the recording, transcription and duration of the interception). It drafts a report each year on the results of its activities and communicates any irregularity to the judicial authority (article 40 of the CPP-F). Individual claimants can address the CNCIS in relation to a specific case or irregularity.

Possible criticisms of the present regulatory regime of administrative interceptions include the following points.

### Table 1. Judicial and administrative interceptions: comparison of powers

| Authority | Grounds | Duration | Renewals |
|-----------|---------|----------|----------|
| **Administrative interceptions**<br>Prime minister (article 3 Law 646/91)<br>i) Prevention of terrorism and organised crime<br>ii) National security<br>iii) Economic protection<br>iv) Outlawed groups<br>**| 4 months | No limits |
| **Judicial interceptions**<br>Juge d’instruction (article 100 CPP)<br>Crimes and délits (max penalty >2 years)<br>** | 4 months | No limits |
| Juge d’instruction (article 80(4) CPP)<br>Suspicious deaths or disappearances<br>** | 2 months | No limits |
| Public prosecutor under the authority of the JLD (arts 74(2), 695 (36) and 696(21) CPP)<br>Hunting of an absconding individual<br>** | 2 months | Renewable three times for délits; no limits for crimes |
| Public prosecutor under the authority of the JLD (article 706(95) CPP)<br>Organised crime<br>** | 15 days | Once renewable |

Source: CNCIS, ‘14e Rapport d’Activité 2005’ (Report) (2006): 18, 54.
First, notions such as ‘national security’, which are used to define the scope of the article, are so vague and broad that they may be subject to misuse in conflict with the principle of legality. However, the CNCIS considers that a mere potential threat to public order or the security of people and goods does not justify the implementation of preventative interceptions.

Second, as for the duration of administrative interceptions, the law regrettably does not provide for a maximum number of renewals.

Third, since it is not admissible as evidence at trial, the retention of the information gathered is not clearly justified for public and testable purposes, despite being prejudicial to individual privacy. By contrast, information gathered during judicial interceptions may be useful for the exercise of defence rights, and it is thus preserved until the prescription of public prosecution.\(^{48}\)

Finally, the CNCIS can only issue non-binding recommendations against a decision of the government. In addition, no judicial figures belong to it, and this body is very close to the political arena so that its real independence is questionable (Table 1).

**Interception of communications in Italy**

The Italian regime partially reproduces the French general distinction between judicial and preventive interceptions.\(^{49}\) However, as underlined in the following paragraphs, preventive interceptions are peculiar in Italy as they are not an administrative prerogative.

**Interceptions post-delictum**

The judicial interception of communications in ordinary cases is regulated by article 266 and following of the Italian *Codice di Procedura Penale* (CPP-I). They are called ‘interception post-delictum’ as in principle they can only be used after an offence has been committed and the preliminary investigations have started. Article 267(1) reads as follows:

> the interception is authorised by a reasoned decision where there are serious grounds (*gravi indizi*)\(^{50}\) for believing that a crime has been committed and it is absolutely indispensable for the purposes of the investigation.\(^{51}\)

The interception warrant is issued by the judge for preliminary investigations (*Giudice per le Indagini Preliminari* – GIP) upon the application of the public prosecutor. This measure is available only for the investigation of the offences listed in article 266(1).\(^{52}\) Interceptions can last up to 15 days, renewable as many times as the reasons grounding the initial decision subsist and upon the authorisation of the judge for preliminary investigations.

Academic commentators consider that the present requirements are too vague. In fact, the judge for preliminary investigations – who is formally in charge of keeping these proceedings under scrutiny – is paradoxically unaware of the facts grounding the investigation. It is thus very difficult for the judge to assess the seriousness of the file.\(^{53}\) It seems pointless to ask a judge to authorise an act potentially interfering with the right to privacy without providing full access to the file.

Exceptional provisions for the interception of communication under less stringent requirements were first enacted by article 13 of Law 203/1991\(^{54}\) for the investigation of organised crime offences.\(^{55}\)

In terrorism cases, the legal regime for judicial interceptions has been amended by article 3 of Law 438/2001. This article applies to terrorism investigations; the special
provisions on intercept evidence were first introduced in relation to organised crime cases and more recently extended to human trafficking by article 9 of Law 228/2003. Three main derogations are thus introduced to the ordinary regime. First, an interception can be authorised where there are sufficient (as against ‘serious’) grounds (sufficienti indizi) for believing that a crime has been committed. Second, interceptions need only to be necessary (rather than indispensable) for investigative purposes. Third, the interception may aim at developing new investigative paths (rather than being merely employed in the course of an already established investigation).

Interceptions in terrorist cases can last for up to 40 days (rather than 15), renewable for subsequent periods of 20 days (rather than 15) when the reasons grounding the initial decision still subsist. No limits exist to the number of renewals available. In case of emergency, the renewal can be authorised by the public prosecutor and then validated by the judge, who has to verify the existence of urgent matters.

As in ordinary cases, the recordings and transcriptions of the interceptions are kept until the final judgment (i.e. one not open to appeal). The intercepted information cannot be used in proceedings other than those for which they have been authorised.

Judicial interceptions under this special regime are available for the investigation of terrorist offences punishable with a term of imprisonment between five and ten years (article 407(2) (a) (4) of the CPP-I). The legislator has also explicitly included in the scope of the provision the offence of ‘assistance to a terrorist group’ (article 270 ter of the CPP-I) punishable with a maximum term of four years of imprisonment.

The communications intercepted cannot be used as evidence when a professional privilege or a state or public secret is involved. In addition, it is noteworthy that interceptions made without complying with the relevant conditions are invalid and cannot be used at trial. This is one of the oldest, and most important, ‘exclusionary rules’ in the Italian system.

The complete re-organisation of the provisions on interceptions is one of the most important features of the new anti-terrorism regime.

The 2001 provisions have been subject to major criticism not merely in relation to the ECHR but also for standing out against domestic constitutional principles such as the right to freedom and secrecy of personal correspondence (article 15 of the constitution) and the right to privacy (article 14 of the constitution). Among the possible criticisms are that the list of offences for the application of this special regime has become too long. For instance, the use of interceptions in cases of assistance to a terrorist group (article 270 ter of the Italian Codice Penal – CP-I) could be disproportionate. Moreover, the vaguely defined concepts of ‘organised crime’ and ‘terrorism’ may entail a further extension by case law of the scope of the current derogations. In any case, such an intrusive method is now available even when it does not represent the ultimate resort as it need only be somehow necessary for the purpose of an investigation.

Preventive interceptions

Preventive interceptions are currently regulated under article 226 disp. att. of the CPP-I, which specifies the authorities entitled to apply for, and issue, interception warrants, the purpose of such application, and its specific content. This provision was at first not clearly drafted, and in consequence was completely rearranged by article 5 of Law 438/2001. This type of interception is permitted when necessary for the prevention of organised crime and terrorism offences. Unlike judicial interceptions, they need not follow the commission of a criminal offence.
Preventive interceptions were first introduced by Law 98/1974, modified by Law 191/1978 in relation to terrorist offences after the kidnapping of Aldo Moro, and further amended by Law 726/1982 specifically dealing with organised crime. Considered of doubtful constitutional legitimacy, the regime was almost completely repealed with the enactment of the new Codice di Procedura Penale in 1988. Nevertheless, article 25 ter of Law 356/1992 reorganised the system to cope with the new Mafia emergency and better specified the legal requirements and the limits for its applicability to concrete situations.

Article 5 of Law 438/2001 differentiates the authorities legitimised to apply for an interception warrant in relation to the two categories of offences. The Ministry of Interior has general competence to apply for an interception of communications for both organised crime and terrorism offences. Here the warrant is issued by the local public prosecutor of the district in which the person to be put under surveillance is resident or where investigative needs have emerged and the operations have to be executed.

In order to allow for systematic scrutiny of the operations, the equipment to intercept the communications is physically located within the office of the Pubblico Ministero (Public Prosecutor) office. Nevertheless, the prosecutor can also authorise the installation of the instruments in other suitable structures, at which point this scrutiny no longer operates.

Operations can last for a maximum of 40 days, subject to subsequent renewals of 20 days each, where the legal requirements still subsist (as underscored by the public prosecutor in his written motivated application). Preventive interceptions must end once a criminal activity becomes manifest (notitia criminis). However, the law does not limit the number of available renewals.

A brief record of the operations carried out and the intercept information is to be made available for scrutiny to the public prosecutor who authorised the activities within five days after their conclusion. Intercepted material and all copies, extracts and summaries which can be identified as the product of an interception must be securely destroyed as soon as no longer needed for any of the authorised purposes.

Possible criticisms of the current legal regime include the following points.

First, from a civil libertarian point of view, the legitimate purpose justifying the use of preventive interceptions is very vaguely defined as ‘acquiring elements for the purpose of the investigation’. This appears to be incompatible with article 15(2) of the constitution requiring a statutory (and precise) identification of any limit imposed upon the right to privacy. The Law Decree previously required mere suspicions to ground an interception warrant. This provision has properly been amended in the final version of the law.

Second, law enforcement authorities might find the law inadequate for their purposes. In fact, as in the case of judicial interceptions, information provided by security services and police informers cannot be used as investigative elements to ground an application for preventive wire-tapping (article 203(1) of the CPP-I). Such a limit might eventually hamper the practical use of this tool, both in anti-organised crime and in anti-terrorist enquiries.

The extension of preventive interception is, in principle, offset by the limit of its use. Information acquired by means of preventive interceptions is not admissible as evidence at trial. As provided by section 17 of the Regulation of Investigatory Powers Act 2000 (RIPA 2000) in the United Kingdom, article 5(5) of Law 438/2001 specifies that preventive intercept evidence cannot be used within the criminal process but only for investigative purposes: they are neither to be mentioned in investigative acts nor to be further disseminated by oral deposition or any other means. According to the Corte di Cassazione, it follows from this that intercepted material cannot be used, for instance, as grounds to justify further preventive interceptions. On the other hand, they can be used as an element of a notitia
criminis on the basis of which a prosecutor can establish an investigation. In addition, although the intercepted material cannot ground any other act or investigative tool, it can lead the police to the development of further autonomous investigations. Revealing this information attracts heavy punishment.

A few problems may occur in the use of the information gathered. As the material is destroyed immediately after the end of the operations, the use of such information would be in the hands of the investigative authorities. This could easily lead to misunderstandings and misleading information.

Here it is certainly arguable that the priority given in this context to the protection of privacy and freedom of expression is disproportionate. The legislator could have nuanced the ban and provided for the partial admissibility of such evidence in specific cases. This is, for instance, the rationale underlying article 191 of the CPP-I: illegally gathered evidence is not admissible at trial, which functions as a deterrent against illegal behaviour. According to some, the complete inadmissibility of intercepted information makes its investigative purposes de facto void and useless. In particular, the specific ban on mentioning intercepted information in any investigative act could hamper further evidence gathering activity. That said, however, it would probably not be desirable to permit material gathered for preventive purposes (under fewer safeguards) to be used, as such, as evidence in a criminal trial.

Other provisions have further amended the regime of preventive interceptions. Law 155/2005 established a wider range of circumstances enabling the relevant authority to implement preventive interceptions. In order to foster investigative and intelligence activities, article 4 gave the heads of security and intelligence services (the Servizio per le Informazioni e la Sicurezza Militare (SISMI) which was replaced in 2007 by the Agenzia Informazioni e Sicurezza Esterna (AISE) and the Servizio per le Informazioni e la Sicurezza Democratica (SISDE) which was in turn replaced in 2007 by the Agenzia Informazioni e Sicurezza Interna) – acting on the instructions of the prime minister – the right to apply to the public prosecutor for an interception warrant ex article 226 disp. att. of the CPP-I whenever deemed to be necessary to prevent terrorist activities or subversion of the constitutional order. The legislator has thus attributed to the executive an important role in the political coordination of intelligence activities (on the model of Law 801/1977 on the security services) unfortunately at the expense of judicial scrutiny, but has also placed a controversial and powerful new instrument in the hands of the security services.

Preventive interceptions need only be ‘necessary for the prevention of terrorist and subversive activities’. The absence of any requirement specifying the seriousness of the offence (or the severity of the penalty) seems to imply that, in referring to terrorist activities, the legal provision includes any offence (or preparatory act) relating to terrorism or the subversion of the democratic structure of the state. Case law will hopefully restrain the applicability of this provision to better balance individual rights and prevention needs.

With regard to the other rules and requirements, the article refers to the regime established by article 226(2–5) disp. att. of the CPP-I. The reasons for any renewal of the measure have to be clearly stated in the judicial warrant. Thus the law underlines even further the need for thorough judicial scrutiny on the matter.

As a result of the political scandal following the discovery of a large amount of illegally intercepted material stored in personal files by secret service agents, Law 281/2006 made significant changes to the use of intercepted material. Article 240(2) of the CPP-I now provides that the public prosecutor may seize any recording, data or documents resulting from an illegal interception of communications. Upon the application of the public
prosecutor, the judge for the preliminary investigations (GIP) holds a public hearing with the interested parties before issuing a warrant for the destruction of the material within 48 hours.

Intercept material that has been illegally obtained cannot be further used in criminal proceedings, even for investigative purposes.\textsuperscript{83} This departs from the long-established distinction in Italian law according to which the inadmissibility of certain findings at trial does not imply that they cannot be used for investigative purposes. The possession of illegally obtained intercepts is sanctioned with a term of imprisonment of between six months and four years (one to five years if the offence is committed by a public official).

Some have argued that the 2006 amendment may hamper intelligence activities pursued by the secret services. However, if an illegal interception provides information concerning a serious offence, it is unlikely that the public prosecutor would not investigate the matter any further, at least for preventive purposes.

**Reform proposal**

In recent years, many other scandals concerning illegally obtained interceptions and their subsequent publication by newspapers have revealed how the current legal regime is too easily subject to abuses. For many years a Bill to reform the law was under discussion, only to be finally abandoned in October 2011.\textsuperscript{84} The most important elements of this proposal were as follows.

In ordinary cases interceptions would have been authorised only when evident suspicions of guilt exist. Interceptions could not have lasted longer than 30 days as a whole (even in non-continuous periods), renewable twice for two consecutive periods of 15 days. Intercepted material would not have been used outside the proceedings for which a warrant had been issued (but this limit would not apply to organised crime and terrorism offences). A judge disclosing the content of an interception which is part of the evidence of an ongoing trial would have had to abandon the case and would possibly be prosecuted for a violation of the secrecy of his role. Interceptions would have been executed in relation to all offences punished with a minimum of five years' imprisonment. Nothing could have been published before the end of preliminary investigations. The publication of illegal interceptions would have been a criminal offence punishable with a term of imprisonment of between six months and three years.

The contents of this proposal have been deeply criticised as it would have allegedly limited the potential use of this crucial investigative tool.\textsuperscript{85}

**Comparisons and conclusions**

In the United Kingdom, telephone tapping has been the subject of controversy, in particular as to whether intercepts should be admissible in evidence in legal proceedings.\textsuperscript{86} Section 17 of the RIPA 2000 provides for a regime of inadmissibility in legal proceedings of intercepted information:

(1): ‘No evidence shall be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of or in connection with any legal proceedings which (in any manner) – (a) discloses, in circumstances from which its origin in anything falling within subsection (2) may be inferred, any of the contents of an intercepted communication or any related communications data; or (b) tends (apart from any such disclosure) to suggest that anything falling within subsection (2) has or may have occurred or be going to occur.’
It the evidence being adduced so that the prosecution and the defence need not even question its provenance. Before the statutory ban was enacted in 1985, intercept evidence was legally admissible, and very occasionally adduced at trial.\(^87\)

This ban has long been the most controversial feature of the interception legal regime. Similar kinds of evidence (from covert agents,\(^88\) bugging and eavesdropping,\(^89\) and CCTV or video surveillance\(^90\)) are already admissible in court, even where not judicially authorised. Civil libertarians would not object to the use of telephone-tap evidence if the process of obtaining it were regulated in a manner that was thought to be rigorous and transparent.\(^91\)

The Joint Committee of Human Rights has repeatedly recommended the admissibility of intercept evidence in criminal trials. Subsequent reports and reviews have indeed advocated an amendment of the legislative framework to achieve this.\(^92\) Moreover, the debate around the possible admissibility of intercept evidence in court is crucial in the framework of terrorism cases. In fact, as explained in detail below, the ban on the use of intercept evidence at trial results in a shortage of evidence which justifies, in the government’s view, the use of administrative measures to get hold of terrorists. Section 17 RIPA 2000 is indeed in conflict with the Birkett Report of 1957, which had indirectly supported that intercept evidence could be revealed and used overtly as evidence when appropriate.\(^93\)

It should be noted that, since 1985, British courts have construed the ban narrowly. For instance, foreign intercepts can be used if obtained in accordance with foreign laws.\(^94\) In addition, following the enactment of the Prevention of Terrorism Act 2005, the use of intercepted material is not banned from the Special Immigration Appeal Tribunal, which deals with both legal issues arising from the expulsion of terrorist suspects and proceedings in relation to control orders and TPIMs.

By contrast, in France and Italy almost all major criminal investigations involve the use of intercepted information, which usually contains abundant and highly probative material to secure the conviction of suspects. Such material seems particularly relevant when the suspect is only involved at a preparatory stage and not in the actual execution of an act. Intercept evidence is routinely used as evidence in legal proceedings. Its admissibility at trial, provided that it is legally obtained, has never been questioned.

The question which arises is why the use of intercept evidence at trial is thought to be appropriate in these two continental jurisdictions but not in England. In this way, it is thus instructive to briefly sketch the relevance of foreign experiences for the development of English law.

First, it is suggested that a useful step in the reform of the current British regime would be to draw a clear line between judicial interceptions for the purpose of evidence gathering to support the prosecution case and preventive interceptions for general purposes of national security. In France and Italy, this obvious distinction has been made and has a clear impact on the subsequent admissibility of evidence at trial. In France, evidence collected as a result of a judicially supervised enquiry is admitted at trial (although it is unlikely that a conviction will be based solely on intercepts). On the other hand, national security interceptions, which are a prerogative of the executive, are not. In Italy, although preventive interceptions are authorised by a judicial authority, they are still excluded from trial as they are obtained following laxer requirements and safeguards. Even the use of intercepted material to ground further investigations is restricted and subject to additional safeguards.

The most important distinguishing feature of the Italian regime of preventive interception is that the warrant is issued by the public prosecutor. Although the public prosecutor is not a completely independent judicial figure (as required by article 15(2) of the constitution), his involvement is striking by comparison to both the English system and the French regime of preventive interceptions, which depend merely upon an administrative
endorsement. In addition, the scope of the provision is clearly defined by reference to articles of the code instead of notions such as ‘national security’.

Another welcome development in English law would be the introduction of a certain level of judicial scrutiny in this context. In France and Italy, as underlined in the previous paragraph, such scrutiny plays a major role in determining which kinds of evidence are to be admitted at trial.\footnote{In English law the issue of an interception warrant is neither entrusted nor supervised by a judicial authority but is in the hands of the executive. Not only non-governmental organisations such as JUSTICE\textsuperscript{96} but also academic commentators\textsuperscript{97} have repeatedly argued in favour of a judicial warrant to be granted for the interception of private communications, preferably through the creation of a delegated judge.}

Finally, one would wish for a clearer definition of the scope of English legal provisions on interceptions and stricter requirements as to the duration of a warrant, and France and Italy again provide useful instruction.

In the United Kingdom, the secretary of state does not have an open-ended discretion in issuing interception warrants, which must be necessary and proportionate to the purpose of the investigation. However, the law does not establish a list of offences or a minimum sentence needed for the use of interceptions. Reference is made only to vague concepts such as the ‘preservation of national security’ or the ‘prevention and detection of serious crimes’. French legislation is stricter: judicial interceptions are available when necessary to the investigations but only for offences punishable with a minimum of two years of imprisonment. Broader discretion is given to the executive in relation to security interceptions. No definition is provided as for the ‘exceptional circumstances’ allowing their use in relation to wide-ranging grounds such as ‘national security’ or the ‘prevention of terrorism and organised crime’. Similarly, in Italy, interceptions post-delictum (available only for a number of listed offences) must not only be necessary for investigative purposes but also be justified by the existence of sufficient grounds for the investigation of a crime. The same requirements exist in relation to preventive interceptions, which are, however, available only for the prevention of organised crime and terrorism, precisely identified by reference to the CP-I.

As for duration, in the United Kingdom interceptions in national security cases can last up to six months, once renewable. In France both judicial and security interceptions can last for four months only. In Italy the period is even shorter as both types of interceptions are available for 40 days only. However, neither the French nor the Italian regime provides a legal limit to the number of renewals available when the reasons grounding the initial warrant still subsist.

In France and Italy, judicial interceptions have long been available for both minor and serious offences. Organised crime and terrorism have played a catalysing effect in the introduction of derogatory provisions and in the expansion of powers of actors involved in either the authorisation or the execution process. The same trend can be easily identified in relation to the provisions on ante-delictum interceptions. In addition, although primarily introduced for the purpose of preventing and investigating terrorism and organised crime, the scope of derogatory provisions was then extended to cover also other types of crimes that are of a less serious nature.\footnote{In the end, from a civil libertarian perspective, the most important shortcoming of the British regime is the inadmissibility of intercept evidence at trial. In fact, this ban significantly increases the difficulty in prosecuting terrorists and thus has provided an excuse for the creation of extra-judicial methods by which terrorist suspects can be locked up indefinitely without the need to have them prosecuted, convicted and sentenced by the criminal courts. A removal of the ban at least in terrorist cases would raise the chances of prosecuting...}
and convicting terrorists under ordinary criminal justice means and on the basis of the available evidence in open court. This would possibly reduce reliance on extra-judicial measures such as administrative detention, control orders and TPIMs, though this potential impact has been denied by successive indendent reviews.\textsuperscript{99} Similarly, it would not be necessary for the police to detain suspects for long periods without charge in order to question them and gather enough other evidence for a charge.

Those who oppose a change in the law would argue that foreign experiences in the interception of communications are irrelevant to English law as they belong to different legal contexts. English rules in relation to the disclosure of evidence to the defence are allegedly more favourable to the defendants than those in France and Italy. The admissibility of intercepted material as evidence at trial, it is claimed, would be detrimental to the efficacy of police and intelligence investigations, alerting suspects to interception methods and capabilities. This argument is based on a misunderstanding of the rules on disclosure. As explained in this article no requirement exists to fully disclose evidence to the defence except in so far as in relation to evidence of innocence. Moreover, methods such as the doctrine of public interest immunity could be used in these cases as a means of protecting sensitive information.

In conclusion, much could be learned from the experiences on the telephone intercptions within some of the leading jurisdictions within Europe. Unfortunately, there is as yet little sign of any willingness to ‘tap’ into this know-how, a situation which seems to be based on an unrealistic primacy given to the existing working practices of the security agencies\textsuperscript{100} and insufficient weighting given to the values of privacy and also due process.

Disclosure statement

No potential conflict of interest was reported by the author.

Notes on contributor

Francesca Galli is an Assistant Professor at the Faculty of Law of the University of Maastricht. She holds a BA and MPhil in Political Sciences (2005) with a specialisation in international and diplomatic studies (Laurea in Scienze internazionali e diplomatiche) at the University of Trieste (Italy), a Masters of Law of the Institut d’Études Politiques de Paris (Master en carrières judiciaires et juridiques, Diplôme de l’Institut d’Études Politiques) (2006) and a PhD in law at the University of Cambridge (2010) entitled Anti-terrorism Legislation in the UK, France and Italy from 1965 Onwards, focusing on selected themes of criminal law and procedures in the area of counter-terrorism legislation and case law. Before joining the Department of International and European Law, she worked as a FNRS post-doctoral researcher at the Institut d’Études Européennes of the ULB in Brussels where she conducted a research project under the supervision of Prof. Anne Weyembergh, entitled: “L’Union européenne et la prévention du terrorisme : impact sur le droit pénal et redéfinition de la relation entre le droit pénal européen et les droits pénaux nationaux” (2010–13). Francesca’s main area of interest is the relationship between European and national criminal law. Her research has developed around the shift towards prevention in the fight against terrorism. She has first analysed the broader picture of developments in criminal justice in recent years from a comparative law perspective and then brought the analysis of current trends to a European dimension. Francesca is a scholar of the Maastricht Centre for European Law, a member of the European Criminal Law Academic Network and a member of the Association Internationale de Droit Penal.

Notes

1. Schenk v. Switzerland, App. No. 10862/84, (1988) 13 EHRR 242; Khan v. United Kingdom, App. No. 35394/97, ECHR 2000-V.
2. *Halford v. United Kingdom*, App. No. 20605/92, (1997) 24 EHRR 523; *Taylor-Sabori v. United Kingdom*, App. No. 47114/99, (2003) 36 EHRR 17; *Uzun v. Germany*, App. No. 35623/05, 2010 EHRR.

3. For instance, the development of a domestic concept of privacy through the Human Rights Act 1998 (c.42), based on art. 8 of the ECHR, might ensure an adequate regulation and control of surveillance activities in the United Kingdom.

4. See *Govell v. United Kingdom*, App. No. 27237/95, (1997) 4 EHRR 438; *PG and JH v. United Kingdom*, App. No. 44787/98, ECHR 2001-IX.

5. S. Van Drooghenbroeck, *La proportionnalité dans le droit de la convention européenne des droits de l’homme. Prendre l’idée au sérieux* (Bruxelles: Bruylant, 2001).

6. *Popescu v. Romania*, App. No. 49234/99, ECtHR, 26 April 2007.

7. *Kruslin v. France*, App. No. 11801/85, (1990) 12 EHRR 547 and *Huvig v. France*, App. No. 11105/84, (1990) 12 EHRR 528.

8. See *Klass and Others v. Germany*, App. No. 5029/71, (1978) 2 EHRR 214.

9. In the aftermath of the successive attacks in Paris in 2015, the government is discussing reforms of the interception regime for enhanced security purposes. At the core of such reform proposals are measures involving bulk data retention provisions being which are not necessarily desirable from a fundamental rights protection point of view. For more information see http://www.gouvernement.fr/conseil-des-ministres/2015-12-23/presentation-du-projet-de-loi-renforcant-la-lutte-contre-le- (accessed on 31 March 2016).

10. F.-B. Huyghe, *Les écoutes téléphoniques* (Paris: PUF, 2010); R. Errera, ‘Les origines de la loi française du 10 juillet 1991 sur les écoutes téléphoniques’, *Revue trimestrielle des droits de l’homme* 55 (2003): 851; C. Guerrier, *Les écoutes téléphoniques* (Paris: CNRS, 2000).

11. *Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques*.

12. *Loi n° 2002-1138 du 9 septembre 2002 d’orientation et de programmation pour la justice*.

13. *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*.

14. *Loi n° 2012-1432 du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme*.

15. The law applies not only to phone tapping but to all means of telecommunications. See J. Pradel, ‘Un exemple de restauration de la légalité criminelle’, *Dalloz* (1992): 49.

16. Freedom of expression is considered of constitutional value. CC Decision No. 84-181DC of 11 October 1984, Rec 78.

17. Pradel, ‘Un exemple’.

18. As for the most recent cases see Crim 9 October 1980 Bull crim no 255; Crim 15 March 1988 Bull crim no 126; Crim 19 June 1989 Bull crim no 261.

19. CC Ass Plén 24 November 1989. See C. Guerrier and M.-C. Monget, *Droit et Sécurité des Télécommunications* (Paris: Springer, 2000), 96.

20. Crim 15 May 1990 Bull crim no 193.

21. *Kruslin v. France* (1990) and *Huvig v. France* (1990). For a comment see Jean Pradel, ‘Une condamnation des écoutes téléphoniques à la française’, *Dalloz* (1990): 353; R. Koering-Joulin, ‘De l’art de faire l’économie d’une loi’, *Dalloz* (1990): 187.

22. See *Schenk v. Switzerland* (1988).

23. *Lambert v. France*, App. No. 23618/94, (1998) ECHR 1998-V 86. For a comment see J.-P. Marguénaut, ‘L’appréciation par la Cour de Strasbourg des efforts d’adaptation’, *Revue trimestrielle de droit civil* (1998): 994. See also *Matheron v. France*, App. No. 57752/00, (ECHR, 29 March 2005).

24. Significantly, this is the same penalty threshold needed for the use of pre-trial detention.

25. The person in charge of the interception has a certain margin of appreciation. However, the juge d’instruction can always obtain the original recordings.

26. Three years for délits and ten years for crimes.

27. Crim 10 May 2012 Bull crim no 116; Crim 27 September 2011 Bull crim no 186; Crim 26 June 2007 Bull crim no 172.

28. Crim 22 November 2011 Bull crim no 234.

29. In this sense see Crim 23 May 2006 Bull crim no 141, (2007) RSC 596.

30. CC Decision no 2004-492 DC of 2 March 2004, Rec 66.

31. Crim 31 January 2007.

32. P. Kayser, ‘La conformité à la CEDU’, *Dalloz* (1991): 17.
33. A fishing expedition is a proactive action by means of surveillance technologies; a speculative demand for information without a suspect, any real expectation about the outcome of the demand or its relevance to the investigation, where there is insufficient evidence to justify the issuing of a search warrant.

34. Art L 242-1 of the Code de la Sécurité Intérieure (CSI).

35. See CSI, Art L.243-1 et seq., Art. R.244-1 et seq. See the reports of the NCIS in La documentation française, http://www.ladocumentationfrancaise.fr/informations/qui-sommes-nous.

36. Art L 242(3) CSI.

37. Art L 242-1 to R242-3 CSI.

38. Art L 242(5) CSI.

39. Art L 242(6) CSI.

40. Art L 242(7) CSI.

41. Art 5 Law 646/91 reads as follows: ‘the maximum number of intercepts carried out at once is fixed by an Order of the Prime Minister’.

42. CNCIS, ‘3e Rapport d’Activité 1994’ (Report) (1995): 16.

43. 6145 administrative interceptions have been requested in 2012 (4022 new interceptions and 2240 renewals). See CNCIS, ‘21e Rapport d’Activité 2012’ (Report) (2013): 59.

44. Ibid., 18.

45. Art L 222(1) CSI.

46. CC Decision no 2005-532 DC of 19 January 2006.

47. See the ‘Affaire des écoutes de l’Elysée’ (1983–1986), a case of illegally obtained interceptions by the Cellule Anti-terroriste de l’Elysée created by President Mitterand in 1982. Around 3000 conversations concerning 150 people were recorded between 1983 and 1986. President Mitterand himself has been considered by the Tribunal Correctionnel de Paris (9 November 2005) to be ‘l’inspirateur et le décideur de l’essentiel’. This cellule was meant to hide a number of embarrassing cases involving the president (e.g. the case of the ‘Irlandais de Vincennes’) and particularly the existence of his illegitimate daughter Mazarine. In 2005 six individuals were found guilty and the Cour de Cassation rejected their appeal in September 2008. See Crim 30 September 2008 Bull crim no 197.

48. There is a maximum time limit after an event that legal proceedings may be initiated as provided by statutes of limitations in common law systems. In civil law systems, similar provisions are typically part of the (civil or criminal) code and are known collectively as periods of prescription.

49. R. Kostoris, ed., Le intercettazioni di conversazioni e comunicazioni. Un problema cruciale per la civiltà e l’efficienza del processo e per le garanzie dei diritti (Milano: Giuffrè, 2009); A. Vele, Le intercettazioni nel sistema processuale penale. Tra garanzie e prospettive di riforma (Milano: Cedam, 2011); C. Marinelli, Intercettazioni processuali e nuovi mezzi di ricerca della prova (Torino: Giappichelli, 2007).

50. On the notion of ‘gravi indizi’ see Cass pen, 7 February 2003.

51. On the need for interceptions for investigative purposes, see Cass pen., IV, 15 giugno 2000.

52. Offences which do not carry a fault element punishable with life imprisonment or a minimum penalty of five years; offences involving drugs, fire-arms or explosives, etc.

53. See D. Siracusano and others, Diritto processuale penale Vol II (Milano: Giuffrè, 2006): 151–2.

54. Legge 12 luglio 1991, n. 203 Conversione in legge, con modificazioni, del decreto-legge 13 maggio 1991, n. 152, recante provvedimenti urgenti in tema di lotta alla criminalità organizzata e di trasparenza e buon andamento dell’attività amministrativa. For an interpretation of the notion of organised crime see Cass Sez Un 31 October 2001 and Cass pen, sezione V, 20 October 2003, sentenza n. 46221; more generally on the issue see also G. Melillo, ‘La ricerca della prova tra clausole generali e garanzie costituzionali: il caso della disciplina delle intercettazioni nei procedimenti relativi a ‘delitti di criminalità organizzata’ (1997) Cassazione Penale 3512.

55. Legge 11 agosto 2003, n. 228 Misure contro la tratta di persone.

56. Note that following the enactment of Law 63/2001 (Legge 1 marzo 2001, n. 63 Modifiche al codice penale e al codice di procedura penale in materia di formazione e valutazione della prova in attuazione della legge costituzionale di riforma dell’articolo III della Costituzione) on due process, information resulting from police informers or security services is not admissible for this purpose ((article 203(1) CPP-I).
58. The defence must be able to listen to the recordings. See Cass pen 7 October 2013.
59. G. Illuminati, ed., Nuovi profili del segreto di stato e dell’attività di intelligence (Torino: Giappichelli, 2011).
60. Art 271 CPP-I.
61. For example, F. Caprioli, ‘Le disposizioni in materia di intercettazioni e perquisizioni’, in Il processo penale tra politiche della sicurezza e nuovi garantismi, ed. Di Chiara Giuseppe (Torino: Giappichelli, 2003).
62. L. Filippi, ‘Terrorismo internazionale’, Dir Pen Pr (2002) 2: 163, 163–4.
63. Ibid.
64. Legge 8 aprile 1974 n. 98 Tutela della riservatezza e della libertà e segretezza delle comunicazioni.
65. Legge 18 maggio 1978, n. 191 Conversione in legge, con modificazioni, del Decreto-Legge 21 marzo 1978, n. 59, concernente norme penali e processuali per la prevenzione e la repressione di gravi reati.
66. Legge 12 ottobre 1982, n. 726 Conversione in legge, con modificazioni, del Decreto-Legge 6 Settembre 1982, n. 629, recante misure urgenti per il coordinamento della lotta contro la delinquenza mafiosa.
67. Legge 7 agosto 1992, n. 356 Conversione in legge, con modificazioni, del decreto-legge 8 giugno 1992, n. 306, recante modifiche urgenti al nuovo codice di procedura penale e provvedimenti di contrasto alla criminalità mafiosa.
68. Alternatively, on his mandate, the central bodies of the police forces, the ‘questore’, the provincial commander of the Carabinieri and of the Guardia di Finanza. From the sole application of the legislation one cannot understand whether these authorities can act autonomously.
69. Whereas the director of the Direzione Nazionale Antimafia has a role limited to organised crime offences; see Decreto-Legge 20 novembre 1991 n. 367 Coordinamento delle indagini nei procedimenti per reati di criminalità organizzata; Legge 20 gennaio 1992 n. 8 recante coordinamento delle indagini nei procedimenti per reati di criminalità organizzata.
70. See M. Caianiello, ‘The Italian Public Prosecutor: An Inquisitorial Figure in Adversarial Proceedings?’, in Transnational Perspectives on Prosecutorial Power, ed. E. Luna and M. Wade (Oxford: Oxford University Press, 2011).
71. For the purpose of increased transparency, the requirement of a written and motivated application represents a novelty of the law, which was not included in the Law Decree.
72. At this point, the file is transferred to the public prosecutor who may decide to open a judicial investigation.
73. Two new criminal offences have been created in order to prosecute individuals who disseminate the intercepted material or the name of the officials involved in the proceedings. See s.19 RIPA.
74. See Cass pen 29 October 1998, no 4977 (unrep); Cass pen 10 November 2000 no 11500 (unrep).
75. J. Vervaele, ‘Special Procedural Measures and the Protection of Human Rights’, Utrecht Law Review 5, no. 2 (2009): 66, 94.
76. For a comparison see the discretionary power of the English trial judge pursuant to the Police and Criminal Evidence Act 1984, s.78.
77. On this point see G. Melillo, ‘Le recenti modifiche alla disciplina’, Cassazione Penale (2002): 904, 911.
78. Legge 8 marzo 2007, n. 124.
79. Legge 24 ottobre 1977, n. 801 Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato.
80. Whereas, art 226 disp att CPP-I provides a very detailed list of offences for which the application can be made and leaves little discretion in the hands of the Ministry of Interior (and the other delegated authorities). In similar cases, the CPP-I normally specifies the minimum penalty for the offence when intrusive measures are applicable.
81. The Scandalo Telecom-Sismi led to the arrest of 21 individuals, including employees of the phone company, carabiniers and policemen. See ‘Intercettazioni illegali, ventuno arresti nell’indagine su security Telecom Pirelli’, La Repubblica (20 September 2006).
82. Legge 20 novembre 2006, n.281 Conversione in legge, con modificazioni, del decreto-legge 22 settembre 2006, n. 259, recante disposizioni urgenti per il riordino della normativa in tema di intercettazioni telefoniche.
83. The word ‘illegal’ is not statutorily defined but is to be interpreted in accordance with the necessary respect of privacy laws.

84. *Disegno di Legge n 1415-B,* ‘Norme in materia di intercettazioni telefoniche, telematiche e ambientali’ (30 giugno 2008). This Bill was a governmental initiative.

85. A further reform is currently under discussion in Italy. In September 2015, the Chamber of Deputies has given mandate to the government to reform provisions on the interception of communications – as part of a general substantive criminal law and criminal procedure reform. In particular the reform would introduce better defined principles to safeguard privacy rights as well as a new offence (punishable with no more than 4 years of imprisonment) for individuals who share the content of conversations illegally bugged for the purpose of fostering a reputational damage. The reform project is currently under examination with the Senate’s Justice Committee. For more information see [http://www.camera.it/leg17/522?tema=riforma_del_processo_penale](http://www.camera.it/leg17/522?tema=riforma_del_processo_penale) and [http://www.senato.it/leg/17/BGT/Schede/Ddliter/46014.htm](http://www.senato.it/leg/17/BGT/Schede/Ddliter/46014.htm) (accessed on 31 March 2016).

86. See Privy Council Review of Intercept as Evidence (London: Cm 7324, 2008); Home Office, *Intercept as Evidence* (London: Cm 7760, 2009); Home Office, *Intercept as Evidence* (London: Cm 8989, 2014).

87. As in *Rumping v. Director of Public Prosecutions* [1964] AC 814.

88. See K. Hyland and C. Walker, ‘Undercover Policing and Underwhelming Laws’, *Criminal Law Review* [2014]: 555.

89. In *R v. Khan* [1997] AC 558, the House of Lords considered the legality of a conviction based on evidence obtained by means of an electronic listening device attached to a private house without the knowledge of either the owners or occupiers. See also *Khan v. United Kingdom*, App. No. 35394/97, 2000-V.

90. See *R v. Rosenberg* [2006] EWCA Crim 6.

91. See JUSTICE, *Intercept Evidence: Lifting the Ban* (London: 2006).

92. There have been eight reports in the last 13 years to government ministers on this issue! See, most importantly, the *Report of the Interception of Communications Commissioner for 2005–2006* (London: HC 315, 19 February 2007); Joint Committee on Human Rights, *Counter-Terrorism Policy and Human Rights: 28 Days, Intercept and Post-charge Questioning* (London: HL Paper 157 / HC 394, 16 July 2007); *Counter-Terrorism Policy and Human Rights: 28 Days, Intercept and Post-charge Questioning* (the government’s reply) (Cm 7215, September 2007); Privy Council Review of Intercept as Evidence (London: Cm 7324, 2008); Home Office, *Intercept as Evidence* (London: Cm 7760, 2009); Home Office, *Intercept as Evidence* (London: Cm 8989, 2014). See also Democratic Audit, *Evidence for Change – Lifting the Ban on Intercept Evidence in Court* (London: March 2007).

93. ‘We are told that in practice the Home Office insists that the power should be exercised for the purpose of detection only, primarily on the ground that the use of the information so obtained, if used in Court, would make the practice widely known and thus destroy its efficacy in some degree. But we do not feel for ourselves that we need to argue the wisdom or otherwise of this practice, although we see no reason why in a proper case the evidence should not be tendered, and the history of the law of evidence is proof enough of the immense care that is taken in the administration of justice to see that the evidence submitted both in civil and criminal cases is evidence that it is proper to admit in all the circumstances of the case.’ See *Report of the Committee of Privy Councillors Appointed to Inquire into the Interception of Communications* (London: Cmd 283, 1957), [152].

94. In *R v. Aujla* [1998] 2 Cr App R 16, the conviction of a defendant charged with conspiracy to smuggle illegal immigrants into the United Kingdom was done on the basis of incriminating telephone conversations intercepted by the Dutch police. The decision was then approved by the House of Lords in *R v. P* [2002] 1 AC 146.

95. In Italy, judicial scrutiny upon any restriction to the right to secrecy and freedom of correspondence is a constitutional requirement (article 15 of the constitution). No use of the information gathered is otherwise allowed at trial.

96. Memorandum from JUSTICE to the Joint Committee on Human Rights, Written Evidence, February 2007.

97. Including F. Galli in *The Law on Terrorism* (Brussels: Bruylant, 2015), Chap 2.
98. C. Cocq and F. Galli, ‘The Catalysing Effect of Serious Crime on the Use of Surveillance Technologies for Prevention and Investigation Purposes’, *New Journal of European Criminal Law* 4, no. 3 (2013): 256.

99. See D. Anderson, *Terrorism Prevention and Investigation Measures in 2012* (London: Home Office, 2013), para. 7.13.

100. An effective veto is accorded by the criteria set by the *Privy Council Review of Intercept as Evidence* (London: Cm 7324, 2008), para. 208.