TILT LAW & TECHNOLOGY
WORKING PAPER SERIES

Criminal Investigation and Privacy in Italian Law

Bert-Jaap Koops

Tilburg University, TILT
e.j.koops@tilburguniversity.edu

Version 1.0, December 2016

citation: B.J. Koops, *Criminal Investigation and Privacy in Italian Law*, TILT Law & Technology Working Paper Series, version 1.0, December 2016, available at https://ssrn.com/abstract=2888422

Abstract

The law regulating criminal investigation both legitimates and limits the government's use of power, and privacy is one of the most prominent issues in this process. This paper analyses criminal investigation in relation to privacy in Italian law, with particular focus on privacy-related safeguards and limitations to criminal investigation. As part of a large-scale project on privacy protection in the 21st century, together with similar country studies, it will facilitate comparative legal analysis of criminal investigation, and help to better understand privacy, as the forms and scope of privacy protection in criminal investigation law tell us something about how privacy is conceptualised. After an introduction on Italian criminal procedure, investigation powers are discussed that reflect limitations grounded in the protection of places, persons, things, and data, with particular attention for search and seizure, covert online searches, visual observation, and location tracking.

The overview demonstrates that criminal investigation powers are largely under-regulated in statutory law, which has to be compensated for by case-law and triggers extensive doctrinal debates. What emerges from case-law and particularly the doctrinal debates on privacy protection is a strong emphasis on the capacity of individuals to shield parts of their private life from others' access or cognition. The cornerstone of this protection is the home, as spatial projection of the person, but it also comprises, for instance, protection of conversation space. While some authors emphasise a shift in importance from secrecy or seclusion (through access control) to reserve (through broader mechanisms of regulating information flows), the former remain important. The paper concludes that doctrinal debates on topical investigation methods demonstrate a continuous search for a sustainable normative framework to assess the intrusiveness of criminal investigation in a world of increasing mobility and datafication. Through proposals for new normative concepts such as informatic privacy and a right not to be localised, in combination with strengthened attention for the right to anonymity, Italian doctrine seeks to help protect the underlying value that people should be able to develop and manifest their personality without undue constraints, which is ultimately what, in the Italian normative framework, privacy protection seeks to achieve.

Keywords
privacy, criminal investigation, constitutional law, investigation powers, search and seizure, surveillance, online searches, location tracking

Criminal Investigation and Privacy in Italian Law

Version 1.0, 21 December 2016

Bert-Jaap Koops[1]

[1] Bert-Jaap Koops is Professor of Regulation and Technology at TILT – Tilburg Institute for Law, Technology, and Society, Tilburg University, the Netherlands, and Distinguished Lorentz Fellow 2016/17 at the Netherlands Institute for Advanced Study in the Humanities and Social Sciences and the Lorentz Center. The research for this paper was made possible by a grant from the Netherlands Organisation for Scientific Research (NWO), project number 453-14-004. I thank Alessandro Bruno, who provided valuable research assistance for this paper.

Abbreviations

Cass.	(Corte Suprema di) Cassazione (Italian Supreme Court)
Corte cost.	Corte costituzionale (Italian Constitutional Court)
Cost.	Costituzione (Constitution)
c.p.	Codice penale (Italian Criminal Code)
c.p.p.	Codice di procedura penale (Italian Code of Criminal Procedure)
disp. att. coord. c.p.p.	Norme di attuazione, di coordinamento e transitorie del codice di procedura penale (Legislative Decree on Implementation, Coordination and Transitional Norms of the Code of Criminal Procedure)
Sez.	Sezione (Section of the criminal division of the Italian Supreme Court)
Sez. Un.	Sezioni Unite (United Sections of the criminal division of the Italian Supreme Court)

1. Introduction

Criminal investigation law legitimates the government's use of power by providing a legal basis for law enforcement authorities to intrude upon individuals' rights and liberties, and at the same time limits the government's use of power by setting conditions for these intrusions. Privacy is one of the most prominent issues to be considered in establishing and limiting investigation powers. It is therefore interesting to analyse how criminal procedure law regulates the use of investigation powers in light of privacy protection. This facilitates comparative legal analysis of criminal investigation (a still rather under-researched field), and it helps to better understand privacy, as it shows how privacy is conceptualised by legislators and how and to what extent different types of privacy are protected by law. In that light, this paper aims to analyse criminal investigation in relation to privacy in Italian law, with particular focus on privacy-related limitations and safeguards in the regulation of criminal investigation powers. It is part of a large-scale project aiming to understand how privacy protection can be shaped sustainably in light of 21st-century challenges,[2] and is complemented by a number of similar country studies,[3] which jointly will serve as a basis for future comparative analysis.

As criminal investigation involves a large number of investigation powers, an in-depth analysis is not feasible in a single paper. Rather, this paper focuses on search and seizure powers, in relation to both traditional places and computers, and zooms in on a number of topical and often-debated surveillance measures, in particular online (covert) computer searches, visual observation, and location tracking. Other investigation powers are briefly mentioned to provide an overview of how criminal investigation powers are regulated.

Several limitations apply. First, the report is limited to criminal investigation powers; other parts of criminal procedure in which privacy play a role (e.g., restraining orders) are not discussed. Second, the overview is limited to general criminal investigation, as regulated in the Code of Criminal Procedure (*Codice di procedura penale*); investigation powers in special legislation (e.g., drugs or organised crime laws) are not mentioned, unless they contain exceptions that are particularly salient from the perspective of privacy protection..

Criminal investigation powers can be classified in different ways. The structure of the paper is based on the typology of privacy that was developed in the larger project,[4] which does not only distinguish between different types of privacy (such as bodily, spatial, communicational, behavioural, and informational privacy), but also between types of privacy-related rights, based on constitutional classifications of privacy.[5] The latter is used here, as the constitutional forms of privacy protection (focusing on different objects, such as homes or bodies) are closely connected to the legal limitations that constrain investigation powers. Thus, after an introductory section on Italian criminal procedure (s. 2), investigations powers will be discussed that reflect limitations grounded in the protection of places (s. 3), persons (s. 4), things (s. 5), and data (s. 6). Throughout the text, references to legal provisions (e.g., art. 189) are to the Code of Criminal Procedure, unless otherwise noted. Paragraphs of criminal provisions are not numbered; for readability, I have used [i], [ii] etc. to indicate the paragraphs of provisions. All translations are mine.

2. Background: the contours of criminal procedure and privacy protection[6]

2.1. A brief history of criminal procedure[7]

The first Italian Criminal Procedure Code (*Codice di procedura penale* or C.p.p., hereinafter: CPC), after the unification of Italy in 1859, dated from 1865. It was a modified version of

[2] See http://www.privacyspaces.org.
[3] To be published on http://www.privacyspaces.org/publications/.
[4] Koops et al. 2016.
[5] See Koops et al. 2016, part III(H).
[6] This section offers a succinct, simplified sketch of Italian criminal procedure, which leaves out many details and exceptions. The aim is to give the reader a bird's-eye view that helps to understand how the provisions discussed in the subsequent sections fit within the general system of criminal procedure.
[7] This section is based on Tonini 2015, p. 24-44. See also Chiavario 2012, p. 33-53.

Piemonte's Criminal Procedure Code of 1859, which, like its predecessor of 1848 and many other European codes of the time, was modelled on the Napoleonic *Code d'instruction criminelle* of 1808. It was a 'mixed' system, a combination of the accusatorial and inquisitorial ideal types of criminal procedure, with largely inquisitorial elements in the preliminary stage of investigation, and largely accusatorial elements in the subsequent stage of the trial.

The CPC was replaced in 1913 by a Code that was still a mixed system, but which introduced more accusatorial elements in the preliminary stage of the instruction (*istruzione*); it also introduced a lay jury in trials of serious crimes. After the First World War and the rise of fascism, the CPC was replaced in 1931 by a new Code, called the Rocco Code (*Codice Rocco*) after the then Minister of Justice, which was much more inquisitorial. Rights of the defence during the instruction stage were abolished (while the results of this secret stage could be used during trial), and the Public Prosecutor obtained coercive powers for investigation in parallel to the powers of the examining judge (*giudice istruttore*) during the instruction. The lay jury was abolished; instead, a Court of Assizes (*corte d'assise*) was introduced for the most serious crimes, comprised of two magistrates and five citizens.

With the post-World War II demise of fascism and the liberal Constitution of 1948, the Rocco Code remained in place but was gradually deprived of many of its inquisitorial traits. The Constitutional Court declared around a hundred provisions of the CPC unconstitutional over time, and the legislator – partly as a response to the Constitutional Court's judgements – modified the law in many ways since the 1950s. A major reform in 1955 reintroduced many of the more rights-guaranteeing elements of the 1913 Code, including active participation of the defence during the instruction stage. The Public Prosecutor did retain the power to conduct an investigation, with coercive powers, on its own initiative (a 'summary instruction'), in parallel to the instruction conducted by the investigatory judge; and all records (*verbali*) of the instruction stage could be used during trial, including witness statements on which the defence had had no influence during the instruction. Nevertheless, the end result of all reforms by the late 1980s was a mixed system with largely accusatorial traits.

In the mean-time, since the early 1960s, initiatives had been taken to create a new Code. An extensive draft, based on a delegation law (*legge delega*) of 1974 and presented in March 1978, aimed to introduce an accusatorial model, while retaining structural elements of the mixed model. Its adoption was stalled, however, by the kidnapping of former Prime Minister Aldo Moro by the Red Brigades and the subsequent climate of anti-terrorist politics. It took until 1988 for a new draft to be developed and adopted: the new, and current, Code of Criminal Procedure was promulgated in October 1988 and entered into force on 24 October 1989. This Code is based on the accusatorial system, with a stricter separation between the investigation and trial stages and a stricter functional separation of the roles of judge and prosecutor during the investigation stage. The instruction (investigation at the initiative of the examining judge) was abolished and replaced by a stage of preliminary investigations (*indagini preliminari*), where the judge no longer had investigation powers himself but, as a judge of preliminary investigations (*giudice degli indagini preliminary*, hereinafter: investigatory judge), served to decide on the use of (the most infringing) investigatory powers by the public prosecutor. The strong emphasis on the trial stage, in which time-consuming oral debate – cross-examination – is the main organising principle, was mitigated by the introduction of several shortened procedures.

Since 1989, the Code has been changed several times, partly by legislative responses to social developments (such as the anti-organised crime efforts and murder of anti-mafia judges in the early 1990s) and partly through interpretations by the Constitutional Court. Many changes relate to more or less strict interpretations of the accusatorial nature of the criminal procedure, with its emphasis on oral contestation during trial, and whether and to what extent pre-trial statements (including those from co-defendants or defendants in other trials) could be used as evidence. In 1999, Parliament adopted a constitutional amendment involving the right to a fair trial, to emphasise the strong contradictorial character of the criminal procedure (see s. 2.2.1 below on art. 111 Constitution). Altogether, the 1989 Code can be seen as an almost pure form of the accusatory model, albeit that several subsequent modifications have diluted it somewhat to off-set some disadvantages of a purely accusatorial system.

2.2. Constitutional law, principles of criminal procedure, and privacy protection

2.2.1. The constitutional grounding of criminal procedure

Italian criminal procedure is strongly grounded in constitutional law. Article 25 Constitution (*Costituzione*) establishes the legality principle, both substantive (no punishment without a prior law) and procedural (no-one can be subjected to a security measure except in cases foreseen by law) (art. 25[2-3] Cost.); and no-one can be kept from the relevant judge prescribed by law (art. 25[1] Cost.). The inviolable right to defence, in every stage of the proceedings, is guaranteed by article 24[2] Cost. Article 27 Constitution contains the presumption of innocence ('The accused is not considered guilty until the definitive conviction', para. 2) and a prohibition of the death penalty (para. 4); it also stipulates that punishments cannot consist of unhuman treatment (literally, treatments against the sense of humanity) and should aim at re-educating the convict (para. 3). The law shall also establish the conditions and modes for repairing judiciary errors (art. 24[4] Cost.). Article 102[3] calls for the legislator to regulate the direct participation of the people in the administration of justice, which for criminal procedure has been implemented through the Court of Assizes (art. 5 CPC), which consists of two professional and six lay judges.[8]

Important norms for the criminal trial are found in article 111, as amended in 1999. It stipulates a fair trial (*giusto processo*), albeit not in the form of an individual right to a fair trial but in the form of a duty for the legislator to regulate the fair trial (para. 1). The following paragraphs emphasise the accusatory, contradictoriness-based model of the criminal trial:

> '[2] Each trial takes place in the contradictoriness between the parties, on an equal footing, before a third and impartial judge. The law assures its reasonable duration.
>
> [3] In the criminal trial, the law ensures that the person accused of a crime is, as quickly as possible, informed confidentially [*riservatamente*] of the nature and motives of the accusation against him; has at his disposal the time and necessary conditions for preparing the defence; has the right to interrogate, in front of the judge, the persons who provide statements against him, to obtain the calling and interrogation of persons for his defence under the same conditions as the accusation and the acquisition of any other means of evidence in his favour; is assisted by an interpreter if he does not understand or speak the language employed in the trial.
>
> [4] The criminal trial is governed by the principle of the contradictoriness in the establishment of evidence. The culpability of the accused cannot be proven on the basis of statements by someone who, by free choice, has always voluntarily detracted himself from the interrogation by the accused or his defence.
>
> [5] The law regulates the cases in which the establishment of evidence does not take place in contradictoriness by consensus of the accused or by an ascertained impossibility of an objective nature or by effect of a proven illicit conduct.
>
> [6] All judiciary measures have to be motivated.
>
> [7] Against the sentences and against the measures involving personal liberty pronounced by the ordinary or special judiciary organs, recourse in Cassation for violation of the law is always admitted. Derogation of this norm is only possible in military tribunal cases in times of war.'

While these norms largely fulfil the individual-protective function of the constitution, the community-protective function is reflected in the principle that the Public Prosecutor (*pubblico ministero*) has the 'obligation to exercise penal action' (*obbligo di esercitare l'azione penale*). In other words, Italy applies the legality principle that requires all crimes to be prosecuted (similarly to, e.g., German law, and in contrast to, e.g., Dutch law that applies the opportunity principle). This serves to reinforce the values underlying the substantive legality principle of article 25[2] (no punishment without a prior law) but also, more importantly, to reinforce the equality principle embedded in article 3 of the Constitution: the public prosecutor cannot be selective in whom to prosecute.[9]

[8] Law of 10 April 1951, n. 287.

[9] Gaeta 2015, p. 156. To be sure, not all crimes can be prosecuted in practice, leading some critics to argue that the result of this legality principle is the opposite of what it is supposed to ensure, namely, complete discretionary power of the prosecutor to prioritise cases in practice; on this discussion, see ibid., p. 170-171, with references.

While these form the main constitutional principles governing criminal procedure, they are supplemented by the norms of international treaties, most importantly the European Convention of Human Rights and the International Covenant on Civil and Political Rights. These treaties, like the EU communitarian order, restrict, along with the Constitution, the legislative power of the Italian legislator (art. 117[1]).[10] Moreover, the rights stipulated in international treaties can also be used to fill in the open-ended rights clause of article 2 Constitution ('The Republic recognises and guarantees the inviolable human rights (…)').

2.2.2. Constitutional privacy protection

The Constitution contains three major privacy-related rights: liberty of the person (art. 13), inviolability of the home (art. 14) and liberty and secrecy of correspondence and of all other forms of communication (art. 15). Infringements of these rights are possible, under different conditions. Personal liberty can be limited only with court authorisation:

> 'No form of detention, personal inspection or search is admitted, nor any other restriction of personal liberty, except by motivated act of the judiciary authority and only in the cases and modes foreseen by law.' (art. 13[2] Cost.)[11]

Pre-trial detention is allowed, but the law shall impose maximum limits on its duration (art. 13[5] Cost.). Moreover, 'every physical and mental violence against persons, however subjected to restrictions of liberty, shall be punished' (art. 13[4] Cost.). It can be seen as comprising the right to personal intimacy.[12]

In contrast, infringements of domiciliary privacy do not necessarily require judicial authorisation:

> 'Inspections or searches or seizures cannot be executed, except in the cases and modes established by law, according to the guarantees prescribed by the protection of personal liberty.' (art. 14[2] Cost.)[13]

The constitutional protection of the home safeguards 'a type of spatial projection of the person',[14] which is a necessary spiritual breathing space for the human person.[15]

Restrictions to the liberty and secrecy of correspondence can only take place on the basis of motivated acts by a judiciary authority and with the guarantees established by law (art. 15[2]).

Also the presumption of innocence (art. 27[2]), family rights (art. 29[1]) and freedom of expression (art. 21, which includes the right *not* to manifest one's thoughts[16]) are considered to (also) protect aspects of privacy.[17] The right to health (art. 32) is privacy-related as well, as the law cannot impose forced treatment that would disrespect the human person (which amounts to a prohibition of violating personal intimacy).[18] Although not usually included in catalogues of privacy-related rights, article 16 Constitution is also relevant for criminal procedure in that it sets limits to the restrictions of movement that can be imposed on citizens (e.g., through restraining orders), and thus safeguards an aspect of behavioural privacy: 'Every citizen can circulate and stay freely in any part of the national territory, subject to limitations established by law in general for reasons of health or security. No restriction can be determined by political reasons' (art. 16[1] Cost.).

Since the 1950s, privacy has been discussed extensively in the literature, which gradually recognised an overarching general right to privacy as an important and protection-worthy good, although it had no explicit constitutional basis. In the 1970s, such a general right to privacy was

[10] See Corte cost. [Italian Constitutional Court], judgements 348/2007 and 349/2007; Conso, Grevi & Bargis 2014, p. LXII.
[11] In exceptional cases, temporary measures can be imposed by public security authorities (art. 13[3] Cost.).
[12] Bonetti 2003, p. 56.
[13] Art. 14[3] stipulates that special laws shall regulate the verifications and inspections [of homes] for reasons of health and public safety or for economic or fiscal reasons.
[14] Bonetti 2003, p., 56, quoting Amorth (1948), *La Costituzione italiana. Commento sistematico*, Milano, p. 62.
[15] Bonetti 2003, p., 56, referring to Pisani (1967), 'La tutela penale della "riservatezza": aspetti processuali', *Riv. it. dir. e proc. pen.*, p. 788 and others.
[16] Mantovani 2013, p. 588.
[17] Mantovani 2013, p. 588.
[18] Bonetti 2003, 54.

recognised by the Constitutional Court as a stand-alone constitutional right or 'unitary value', having its basis in the open-ended art. 2 of the Constitution.[19]

2.3. The stages and actors of criminal procedure[20]

In simplified terms, the normal course of criminal procedure looks as follows. Criminal procedure (*procedimento penale*) starts when a notification is registered that a crime has likely been committed. The first stage is that of the preliminary investigation (*indagini preliminari*, regulated in book V of the CPC), under the direction of the Public Prosecutor. The Public Prosecutor or the judicial police (*polizia giudiziaria*)[21] can acquire evidence, in order to decide whether or not to proceed; for some types of evidence-gathering, authorisation from the investigatory judge is required. The evidence gathered here is, as a rule, not directly usable during trial (since it has not yet been contested by the defence), but if contestation of the evidence cannot await trial (for instance, with a seriously ill witness or with a forensic examination of a thing or place that is subject to inevitable modification), the prosecutor or the defence can request an 'evidential proceeding' (*incidente probatorio*, art. 392-404) where the evidence is discussed between parties before a judge.

Although the Public Prosecutor and the judicial police are the main actors in this stage of criminal investigation, both having powers to gather evidence (for the police, see title IV of book V, for the prosecutor, see title V of book V), also the defence has an investigatory capacity during the preliminary investigations (title VI-bis of book V). This includes, for example, the possibility to hear or request written statements from relevant persons (art. 391-bis), access places to observe or to take technical recordings (art. 391-sexies) and, with judicial authorisation, access private places without consent of the rights-holder (art. 391-septies). Moreover, also the victim (literally, person offended by the crime, *persona offesa dal reato*) can play an active role, by presenting memorandums (*memorie*) in any stage of the proceedings and by indicating (except in the cassation stage) elements of evidence (art. 90). She can, through her lawyer or technical consultant, also participate in a non-repeatable technical assessment (art. 360), request an evidentiary proceeding (art. 394) and participate in this (art. 401), and oppose a request for archiving the case (art. 410).

The possible outcome of the stage of preliminary investigations is twofold. If the prosecutor decides not to proceed, he can request the investigatory judge to archive the case. If he decides to proceed, he can request a referral to a trial (*rinvio a giudizio*), and he has to inform the suspect accordingly of the accusation.

If the prosecutor requests referral to a trial, the second stage then consists of a (non-public) preliminary hearing (*udienza preliminare*, also regulated in book V), which involves a contradictoriness-based discussion of the case before a judge.[22] This serves to ensure that the burdensome decision to impose a criminal trial on an accused is taken by a judge, not by a prosecutor. The outcome of the preliminary hearing can be a verdict not to proceed (*sentenza di non luogo a procedere*) or a verdict granting trial.

In the latter case, the third stage starts, that of the trial proper (*giudizio*, regulated in book VII CPC). The ordinary trial is also called the 'debating trial' (*giudizio dibattimentale*), emphasising the crucial role in the trial of oral debate, with cross-examinations. Although the trial is modelled on the Anglo-American trial, the judge has more powers than in the Anglo-American system to intervene in or direct the questioning, and he can also order at his own initiative that more

[19] Corte cost. [Italian Constitutional Court] 12 April 1973, *Foro italiano* 1973, I, 1708. See Mantovani 2013, p. 588.
[20] This section is largely based on Chiavario 2012, p. 59-66, and Tonini 2015, p. 33-38.
[21] The judicial police is a functional part of the (many) Italian police forces, charged with taking note of and solving crime, under the direction of the judiciary authorities (art. 55). It is thus functionally separate from the administrative police, which takes care of the preventive and public-order tasks of policing. The judiciary police consists of a) police officials (*uffiziali*), which include heads, inspectors, superintendents and others of the state police specifically recognised as such, as well as officials of the *carabinieri*, financial, forestal, custodial or other corpses recognised as such, and b) police agents (*agenti*), which include other staff of the state police or certain other corpses (art. 57). The distinction between officials and agents is relevant as some police powers are limited to police officials.
[22] As alternative routes for the second and third stages, various special proceedings are possible (regulated in book VI CPC), which aim at enhancing the efficiency of criminal procedure. These include, for example, a super-direct or an immediate trial (both skipping the preliminary hearing), plea bargaining (*patteggiamento*) or a monetary fine before the investigatory judge (*procedimento per decreto*).

evidence needs to be collected. As the evidence gathered in the first stages can, as a rule, be used in trial only where it has been discussed by the parties, the file 'for the debate' contains only those forms of evidence that have been discussed (for instance, in the evidential proceeding) or non-repeatable official reports from the prosecutor or police; the rest is included in the file 'of the Public Prosecutor', to which the prosecutor and defence, but not the judge, have access. The outcome of the trial can be acquittal (*proscioglimento*, which can take the form of *nolle prosequi* (art. 529) or discharge (*assoluzione*, art. 530)) or, if the judge has gained the conviction that the accused is guilty beyond a reasonable doubt, conviction (*condanna*, art. 533). Against the judgement, appeal is possible on matters both of fact and of law, and subsequently cassation on matters of law (regulated in book IX CPC).

2.4. The types, acquisition, and uses of evidence

2.4.1. Means of evidence and means of searching for evidence

Evidence is regulated in book III CPC. Evidence (*prova*) can relate to the facts concerning the accusation, to the punishability of the suspect and to the determination of the penalty or of security measures (art. 187). The Code lists seven **means of evidence** (*mezzi di prova*) that are specifically regulated:

- witness statements (art. 194-207);
- examination of the accused, the party with a civil claim connected to the trial (*parte civile*), the person civilly liable and the person civilly required to pay the monetary fine, or of an accused in connected proceedings, as far as they cannot be heard as witnesses (art. 208-210);
- confrontations (*confronti*) between persons already questioned or interrogated, where their statements are not in line with one another (so that, for example, memories will be better recalled when confronted with others' memories) (art. 211-212);
- the recognising (*ricognizione*) of persons or things amid a number of similar persons or things, e.g., through a line-up (art. 213-217);
- judicial experiments, to reconstruct how an event may have occurred (art. 218-219);
- expert evidence (*perizia*), in case data or assessments are needed that require specific technical, scientific or artistic expertise, which involves appointment of an expert by the judge (art. 220-232); the public prosecutor and private parties can appoint technical consultants of their own (*consulenti tecnici*, art. 225) to be involved in the task-setting or execution of the expert activities (art. 230); the parties can also appoint technical consultants outside of expert evidence cases, to present memorandums or, with court authorisation, to examine seized objects or to be present at inspections (art. 233);
- documents or, more precisely, documental evidence (*prova documentale*), which can be writings or other documents that represent facts, persons or things through photography, video, phonography or any other means (art. 234-243).

While these so-called means of evidence are suitable for offering the judge evidentiary results that are directly usable to base his decision on (as they usually take place in a contradictoriness-based setting in front of the judge), Italian criminal procedure also regulates specific **means of *searching for* evidence** (*mezzi di ricerca della prova*, title III of book III), which do not yield direct sources for the judge's conviction as such, but rather indirect sources with an evidential function that can serve as evidence in trial after having been subjected to oral debate by the parties.[23] The Code lists four means of searching for evidence:

- inspection of persons, places, or things (art. 244-246);
- search of persons or places (art. 247-252);
- seizure of things (art. 253-263);
- interception of conversations or communications (art. 266-271).

[23] Chiavario 2012, p. 353. The distinction between means of evidence and means of searching for evidence is related to, but not identical with, a distinction between evidence that is constituted in or during the criminal hearing or trial and pre-constituted evidence that already exists outside of the criminal hearing or trial. Means of evidence (with the exception of documents) are generally targeted at evidence being constituted, while means of searching for evidence are generally targeted at pre-constituted evidence. See Chiavario 2012, p. 354.

The enumeration of means of (searching for) evidence is not exhaustive. In contrast to the 1978 legislative project, which only accepted statutorily defined means of evidence,[24] the 1989 Code also allows means of evidence not regulated by law to be admitted. This so-called **'atypical evidence'** (*prove atipiche*) can be admitted by the judge, after having heard the parties on the modalities of allowing this evidence, if they are suitable for proving the facts and do not prejudice the moral liberty (i.e., mental self-determination) of the person (art. 189). The provision on atypical evidence is intended particularly to accommodate technological developments, which may offer means of (searching for) evidence as yet unforeseen by the legislator.[25]

It should also be noted that, as mentioned above, the judicial police, Public Prosecutor, and the defence have certain investigation powers, which are not regulated in book III on evidence but in book V on preliminary investigations and the preliminary hearing. The police (title IV of book V) has the general task to collect all elements useful for reconstructing the fact of the crime and individuating the culpable person (art. 348[1]) and has various specific powers at its command for this task, including identification (349), searches (352), acquisition of mail (*plichi*) or closed correspondence (353), and urgent verifications (*accertamenti*) of places, persons, or things (354). More generally, the police can conduct ordinary investigative activities on the basis of their task description, as indicated in articles 55, 347-348 and 370, if they do not (substantially) interfere with constitutional rights.[26] The Public Prosecutor (title V of book V) similarly shall conduct all activities necessary for determining the criminal proceedings, but also to ascertain facts and circumstances favouring the suspect (art. 358), and has investigation powers including taking biological samples of persons (359-bis), conducting technical verifications that are non-repeatable (360), individuating persons or things (361), and to call upon assistance by the judiciary police or, if necessary, public forces to exercise its functions (378 j^{o} 131). The defence and, to some extent, the victim also have certain investigation powers (*supra*, s. 2.3).

Parties can request admission of evidence. The judge, having heard the parties, decides on the admission of evidence at the request of one of the parties, excluding evidence forbidden by the law and manifestly superfluous or irrelevant evidence (art. 190 j^{o} 495). The judge assesses the evidence by himself, according to the principle of the free conviction of the judge,[27] having to motivate the result and which criteria were applied in the assessment (art. 192[1]).

2.4.2. Sanctions and remedies for unlawfully acquired evidence

Unlawfully acquired evidence is a complex issue in Italian criminal procedure.[28] Doctrine distinguishes between two primary forms of defects leading to non-usability (*inutilizzabilità*) of evidence. First, so-called **'pathological non-usability'** refers to unlawfully acquired evidence. The generic rule for this is established by article 191, entitled 'Unlawfully acquired evidence':

> '1. Evidence acquired in violation of prohibitions established by law cannot be used.
>
> 2. The non-usability can be ascertained also *ex officio* in any state and stage of the proceedings.'

Doctrine is divided as to what the 'prohibitions established by law' refer. Some scholars, pointing out the generic formulation ('by law') hold that it refers to all normative prescriptions in law, including the prohibitions of substantive criminal law and the constitutional limitations to infringements of fundamental rights. Others, however, consider it to be limited to prescriptions in

[24] Chiavario 2012, p. 401.
[25] Chiavario 2012, p. 401.
[26] Article 55, describing the functions of the judicial police, includes the task of the police to take notice of crimes and to 'conduct the activities necessary to secure the sources of evidence'. Articles 347 and 348, in the section on activities at the judicial police's own initiative, require the police to report without delay notices of crime to the public prosecutor, including the elements already collected and indicating the activities conducted so far (art. 347), while subsequently they should continue with the activities mentioned in article 55, collecting in particular every element useful to reconstruct the fact and to identify the perpetrator (art. 348). Article 370 stipulates that the public prosecutor can avail himself of the judicial police to conduct investigative acts and acts specifically delegated. See *infra*, s. 4.3.2 under 'Human tailing' and 'GPS tracking' for an example.
[27] There are some limitations to this principle, where the law establishes conditions for whether or how evidence can be assessed.
[28] Unlawfully acquired evidence is to be distinguished from other defects in criminal procedure, which are regulated through the concept of nullity of acts. Acts are forms of voluntary behaviour by stakeholders in criminal procedure (regulated in book II); where acts deviate from the forms prescribed by law, this can lead to nullity of the act (art. 177-186), which is often reparable. This contrasts with non-usability of evidence, which is non-reparable. See Gaito 2012, p. 1119.

criminal procedure law only (arguing, for example, that the caption refers to unlawfully *acquired* evidence and not to illegal evidence). Moreover, in the latter interpretation, only violations of *prohibitive* norms are sanctioned; deviations from *positive* norms, i.e., prescribing the modalities of evidence-gathering, would not be sanctioned under article 191 (but might lead to nullity if one of the parties invokes the defect).[29] While doctrine is divided and case-law is also equivocal, the Constitutional Court has passed judgements favouring the broad interpretation, of non-usability of unconstitutional or illegal evidence;[30] and a strong argument in favour of the broad interpretation is that the narrow (procedural-law) interpretation would lead to significant gaps in legal protection, particularly for the unregulated forms of evidence that lack procedural requirements.[31] Apart from this controversy, many hold that unlawfully acquired evidence might be used in favour of the accused.[32] Moreover, information declared non-usable as evidence might be used as an informal starting point for further investigations.[33] That leads to the question whether 'fruits of the poisoned tree' are also tainted evidence, but there is no clear line in doctrine or case-law whether or to what extent this doctrine applies in Italy.[34]

Apart from the generic rule, there are also special, explicit rules on non-usability of evidence in specific provisions. For example, interception of communications has a special prohibition to use evidence that has been acquired outside of the situations allowed by law or without observations of the prescribed modalities (art. 271).

The second form of defects leading to non-usability of evidence is called **'physiological non-usability'**; this refers to evidence that, although lawfully acquired, is unusable because it has not been debated by the parties, as required by article 111[4] Constitution. The general rule is provided in article 526, stipulating that the judge cannot use for his decision evidence that has not been legitimately acquired[35] in the debate. Specific provisions also contain special rules of physiological non-usability, for example statements by witnesses who refuse to be subjected to (cross-)examination by one of the parties (art. 500[3]).

3. The protection of places

In the regulation of search, in contrast to several other civil-law systems, Italian law and doctrine do not make a primary distinction in terms of places being investigated, but rather in terms of the type of investigation: inspection and search. Only some special regimes apply to the investigation of certain places, most importantly homes.

3.1. Investigation of places

3.1.1. Inspection

An inspection (*ispezione*) is a means of searching for evidence that aims to 'ascertain the traces and the other material effects of the crime' (art. 244[1]). An inspection can be of persons, places, or things, and has to be based on a motivated order (art. 244[1]). It has primarily a descriptive character, allowing the investigative authorities to perceive directly and to describe material objects that are relevant for evidential purposes. Article 244[2] provides:

> 'If the crime has not left traces or material effects, or if these have disappeared or have been deleted or dispersed, altered, or removed, the judicial authority describes the actual state and, as far as possible, verifies the previous state, taking care also to identify the mode, time, and causes of the possible modifications. The judicial authority can make use of identificatory, descriptive and photographic surveys [*rilievi segnaletici, descrittivi e fotografici*] and any other technical operation, also in relation to informatics or telematic systems, adopting technical measures aimed at safeguarding the conservation of the original data and to prevent their alteration.'

[29] See, e.g., Chiavario 2012, p. 424.
[30] See Gaito 2012, p. 1121, with references.
[31] Dinacci 2015, p. 800-801.
[32] Conti 2008, p. 330.
[33] Conti 2008, p. 330.
[34] Gaito 2012, p. 1119-1120; Conti 2008, p. 330
[35] The term acquired (*acquisito*) in this article refers to evidence being admitted (*ammissione*) and, in the case of statements, also established through debate (*assunzione*). Tonini 2015, p. 244.

During the stage of the preliminary hearing or the debating trial, an inspection is ordered by the judge; during the preliminary investigations, it is ordered by the public prosecutor.[36] It can also be conducted by the police on their own initiative in cases of urgency (if there is a risk of loss of evidence, when the public prosecutor cannot intervene in time or has not yet assumed the leading of the investigations), in the form of verifications (*accertamenti*) or surveys (*rilievi*) of the relevant places and things (art. 354[2]).

For the inspection of places (and things), article 246 stipulates that before the inspection, a copy of the order authorising the inspection has to be given to the accused and to the person actually having the place at their disposal in which the inspection takes place, if they are present (art. 246[1]). Moreover, the judicial authority can provide in the order, with reasons, that these persons shall not leave the place until the operation is concluded, and can have transgressors of this order brought back to the place by force (art. 246[2]). The defence attorney has to be notified at least 24 hours in advance of the inspection (art. 364[3]), and in any case has the right to be present to inspections (art. 364[4]). However, in cases of absolute urgency, if there are grounded reasons to believe that delay will compromise the investigation, the inspection can start earlier; the defence attorney has to be notified of this without delay, except if there are grounds to believe that traces or other material effects of the crime will be altered; nonetheless, the attorney has the right to intervene (art. 364[5]).

3.1.2. Search

A search (*perquisizione*, art. 247) is a means of searching for evidence that consists of searching for evidence or a person to arrest, in the context of a sufficiently concrete and specific case.[37] There are three forms: personal search (*perquisizione personale*, art. 249), local search (*perquisizione locale*, art. 250), and informatics search (*perquisizione informatica*, art. 247[1-*bis*]). All require a motivated decree (art. 247[2]) by a judicial authority, who can conduct the search herself or order police officials to do so (art. 247[3]). However, in situations of *flagrante delicto* or fugitive arrestees or detainees (*evasione*, as criminalised in art. 385 c.p.), police officials[38] can conduct a search themselves; they have to notify the Public Prosecutor of the search within 48 hours, who has to validate the search within the following 48 hours (art. 352). A search includes the power of inspection, and thus to take photographs, as a means of documenting the searched place.[39] If a specific object is sought, the judicial authority can also resort to the less intrusive measure of requesting someone to produce the object; a search is then omitted, except when it is considered useful to complete the investigation (art. 248[1]).

For searches of places (i.e., local searches), a particular place has to be specified, but it does not have to be exactly specified in terms of city, street, and number, as long as the place to be searched is delimited with sufficient precision.[40] Before the search, a copy of the search order has to be given to the accused and to the person actually having the place in which the search takes place at their disposal, if they are present. These persons are informed that they can have themselves assisted or represented by a person of trust (*persona di fiducia*), provided they can be found promptly and are suitable (i.e., at least fourteen years old and capable of mind, art. 120) (art. 250[1]). If these persons are absent, the copy is given to a relative, co-inhabitant, colleague, or, in their absence, the porter or her stand-in (art. 250[2]).[41] If it is given to the porter or her stand-in, in order to safeguard the accused's privacy, the copy needs to be given in a closed envelope (art. 157[3] and art. 80 disp.att. *juncto* 148[3]). If the suspect is present, the Public Prosecutor shall ask him whether he is assisted by an attorney and if not, shall appoint an attorney ex officio (art. 365[1]). The defence attorney has the right to be present when the search is conducted and to present requests, observations, or reservations to the Public Prosecutor, who should note these in the record (art. 365 and 362[7]).

The judiciary authority can also determine for a local search, with a motivated order, that present or newly arriving persons are searched, if there is suspicion that these may hide a *corpus*

[36] Tonino 2015, p. 381.
[37] Tonino 2015, p. 381.
[38] And also police agents in cases of particular necessity and urgency, on the basis of art. 113 disp. att.
[39] Bonetti 2003, p. 237.
[40] Gaito 2012, p. 1458.
[41] If the copy cannot be given to any of these persons, it will be deposited at the records office or the secretariat of the judicial authority conducting the search, and a notice of this deposit shall be affixed to the door of the searched place (art. 80[2] disp. att.).

delicti or things related to the crime – a so-called mixed (i.e., local + personal) search (art. 250[3]). Similarly to inspections, persons may be ordered not to leave and transgressors may be retained or brought back by force (art. 250[3]).

Note that the guarantees offered in the provisions for local searches apply to all closed places (even if uncovered) to which someone has exclusivity rights.[42] Thus, it is limited to places to which a concrete need to protect privacy is set: the guarantees do not apply to places of which no-one has actual disposal (e.g., abandoned houses) or that, through their structural characteristics, cannot be at the disposal of someone in particular (e.g., open places or grottoes).[43] Also prison cells are not considered private places (being open to an undetermined number of people, who have no exclusivity rights) and thus are not covered by the safeguards of place searches.[44]

Relevant things found during a search can be seized (art. 252). It should be noted that, if the search was unlawful, case-law and doctrine vary as to whether seized objects can be used as evidence.[45] Also noteworthy is a judgement by the European Court of Human Rights, finding a violation of articles 8 and 13 ECHR, in a case where Italian police conducted a home search for arms (ex art. 41 TULPS (see note 52)) but (probably since the search did not yield results) the police report was not subsequently validated by the Public Prosecutor; this disregard of the procedural requirement (of art. 352) led not only to a violation of article 8 ECHR, but also of article 13 ECHR, as there was no effective legal remedy to challenge the search in such a case.[46]

3.1.3. Special rules for investigation of the home

There are few specific safeguards applying to investigations of the home. The only safeguard in addition to the general regulation of investigation of places is provided by article 251, which sets temporal limits on searches:

> **251. Search in the home. Temporal limits.**
>
> 1. A search in a dwelling or in the closed places adjacent to this cannot be started before seven a.m. or after 8 p.m.
>
> 2. However, in urgent cases, the judicial authority can provide in writing that the search shall be executed outside said temporal limits.

The temporal limits serve to protect in particular someone's 'sphere of reserve' (*sfera del riserbo*)[47] or domestic peace (*quiete domestica*).[48]

While the search cannot be initiated during night hours,[49] it can extend into night hours if it was started before 8 p.m.[50] Similarly to art. 251[2], there is also an exception for police searches without a warrant (in flagrante or fugitive cases) to be conducted in a dwelling outside the temporal limits if delay would prejudice the outcome (art. 352[3]). Bonetti observes that here, the 'bastion of privacy is nimbly overcome' with 'not irrelevant dangers of abuse'.[51] Also, art. 225 disp. att. stipulates for domiciliary searches that two provisions from special legislation continue to apply.[52] Interestingly, while searches are limited by the legislator to day hours, inspections of

[42] Gaito 2012, p. 1457.
[43] Felicioni 2012, p. 121.
[44] Gaito 2012, p. 1462.
[45] Tonino 2015, p. 384; for an overview, see Feliciani 2012, p. 556-568.
[46] ECtHR 8 February 2005, L.M. c. Italie, Requête no 60033/00. See also Felicioni 2012, p. 68-69.
[47] Bonetti 2003, p. 238.
[48] Felicioni 2012, p. 231.
[49] 'Night hours' are defined in the present code in absolute terms, regardless of the season. The previous Codes connected the temporal limitations to natural darkness, specifying that searches could not take place before sunrise or after sunset (art. 234 CCP-1913) or before one hour before sunrise or after one hour after sunset (Rocco Code). This was based on rural life, although already by 1930 the connection to sunlight appeared incongruous given that urban life had led to gas and electric public lighting. Felicioni 2012, p. 231.
[50] Felicioni 2012, p. 231.
[51] Bonetti 2003, p. 241-241.
[52] These articles provide that police officials shall search homes immediately upon receiving notice or indications that arms are unlawfully held in a dwelling or a private locale or place (art. 41 r.d. 18 June 1931 n 773 (TULPS)), and that the fiscal police can conduct domiciliary searches to investigate financial crimes, in addition to the provisions of the CCP (art. 33 Law 7 Jan 1929 n. 4). Also relevant to note, among other exceptions in special legislation, is the broad exception of art. 25-bis of Law of 7 August 1992, no. 356 (implementing Legislative

homes have no temporal limitations, because inspections are considered less invasive than searches.[53]

What counts as a home in the sense of article 251? Although there is no unitary concept of 'home' in Italian law (the interpretation depending on the legal area), and there is no consensus in doctrine, the majority of authors consider that the reference to 'home' (*domicilio*) in the caption of article 251 is to be interpreted in light of art. 14 Constitution, and that this is best done through the interpretation given to 'home' in substantive criminal law, in particular the provision on trespass (art. 614 c.p.).[54] The substantive criminal law protection of the home covers three types of places:[55] the dwelling (*abitazione*), i.e., 'places suitable for domestic use in which a person freely conducts the activities characteristic of intimate life (repose, alimentation, hygienic practice, and others)';[56] places of private abode (*luoghi di privata dimora*), i.e., places other than dwellings permanently or temporarily destined to carry out private life and work activities;[57] and appurtenances (*appartenenze*), i.e., places that, although not integral part of the environment that constitutes a dwelling, are destined to service or complement this environment.[58] It should be noted, however, that the text of article 251 does not refer to 'homes', but to dwellings and the closed places adjacent to these. Thus, while all homes (as in art. 14 Constitution and art. 614 c.p., including private work places[59]) are protected through the general safeguards applying to local searches (*supra*, 3.1.2), only dwellings and closed places adjacent to these have the additional safeguard of temporal limits. Examples of places recognised in case-law as dwellings are the cabin in a steamship assigned to a particular person, an erected and functioning tent, and a mountain chalet.[60] Also vehicles can fall within the scope of article 251, if they are suitable for habitation and for living domestic life, such as caravans, campers, private yachts (where someone conducts normal acts of domestic life, such as having meals), and motorboats, sailing boats, and private aircraft equipped to conduct essential acts of domestic life.[61] Also vehicles made suitable for doing particular private activities that involve a capacity to include or exclude others, such as mini-vans equipped for direction of television transmissions or medical analysis, count as homes.[62] Moreover, the driver and passenger compartment (*abitacolo*) of a car parked near the home and at the disposal of the person involved counts as a closed place adjacent to the dwelling.[63] Thus, the closed places adjacent to the dwelling do not have to be physically contiguous, as long as they belong to the house,[64] for example, appurtenances such as box rooms (*ripostigli*), lofts, cellars, stairs, entrance halls, and solar pavements.[65]

More in general, the 'home' as constitutionally protected is characterised as a spatial environment in which someone can exercise exclusivity rights, both the right to admit or exclude persons (*ius admittendi*, *ius prohibendi*), and the right to exclusivity of taking knowledge of what pertains to the private, domestic sphere.[66] Thus, also, for example, couchettes on a public train

---

Decree of 8 June 1992, no. 306), which allows police officials to search entire buildings or blocks of buildings if there are motivated grounds to believe arms or fugitives can be found there.

[53] Felicioni 2012, p. 231.

[54] Felicioni 2012, p. 121 ('the notion of home emerging from art. 614 c.p. appears the interpretative key to the procedural regulation of searches; the constitutional regulation, in turn, provides the basis for it').

[55] For a more elaborate overview, see Koops 2016, s. 3.1.2.

[56] Felicioni 2012, p. 117.

[57] Felicioni 2012, p. 117. Places of private abode include non-public places that serve the carrying out of professional, cultural, and political life.

[58] Felicioni 2012, p. 118.

[59] This includes the office of a political party where parliamentarians have their office; this can constitute the parliamentarian's home (*domicilio*), as meant in art. 68[2] Constitution (requiring authorisation of the Chamber of Representatives or Senate for a search at an MP's home).

[60] Felicioni 2012, p. 117.

[61] Felicioni 2012, p. 121-122. Note that, for criminal procedure purposes, domestic activities are distinct from work activities (although the latter are included in the broader concept of 'home' as per art. 14 Constitution), since art. 157[1] (regulating notification of the non-detained accused) explicitly distinguishes between dwellings and places where the accused habitually performs work activities. See Felicioni 2012, p. 117.

[62] Felicioni 2012, p. 122.

[63] Bonetti 2003, p. 238, referring to Cass., Sez. VI, 5 November 1990, *Cass. pen.* 1991, II, 952; Felicioni 2012, p. 112.

[64] Bonetti 2003, p. 238.

[65] Gaito 2012, p. 1462.

[66] Felicioni 2012, p. 120.

can count as home.[67] The constitutional protection of the home thus safeguards the liberty of the home as the 'right of the individual that the closed space that he destines as a base for not only domestic life but for any private activity of his, remain immune from material or immaterial ingressions (*immissioni*) by third parties and in particular by the government.'[68]

Although the temporal limits to domiciliary searches are considered an important form of protection in the literature, it should be emphasised that their practical significance is limited, since violations of the temporal limits do not lead to nullity (not being covered by art. 178[3]) nor to non-usability of evidence (since the legal prohibition of nightly searches do not imply a prohibition of the act, as meant in art. 191, but only see to the mode of execution).[69]

3.1.4. Special rules for other places

Besides homes, there are some regulations for investigations of other specific places as well. **Offices of defence attorneys** can only be inspected or searched a) if the attorney or other persons who sustainably work in the office are accused (*imputato*), and only for the purpose of determining their contribution to the crime, or b) to obtain traces or other material effects of the crime (for instance, to establish how a robbery took place in a lawyer's studio[70]) or to look for specifically pre-determined things or persons (for example, to seek a fugitive or a false bill of exchange known to be hidden in the office[71]) (art. 103[1]). Moreover, at defence attorneys' and relevant private investigators' premises, papers or documents relating to the object of the defence cannot be seized, except if they are *corpus delicti* (art. 103[2]).

To protect the privacy of savings and credit services,[72] art. 248[2] establishes a staged approach that allows a more targeted investigation at **banks**. It stipulates that to find goods to be seized or establish other circumstances useful for the investigation, judiciary authorities or (by delegation) police officials can examine acts, documents, and correspondence, as well as data, information, and software, at banks. Only if the bank refuses to allow this examination, shall the judicial authority proceed with a search.

3.1.5. Investigation by the defence

Not only investigative authorities, but also the defence has powers to investigate places. According to art. 391-*sexies*, the defence attorney (and his substitute and aides) can access places to view the state of the place and the things located there, as well as to describe or document (with technical, graphical, planimetric, photographic, or audio-visual prints) the place or things, and report the findings. If it is necessary to access private places or places not open to the public, and they are not allowed access by the rights-holder, the judge can, upon the attorney's request, order with a motivated decree, and specifying the modalities of execution, authorise the access to these places (art. 391-*septies*[1]). Access to dwellings and appurtenances is not allowed, however, except as far as necessary to secure traces and other material effects of the crime (art. 391-*septies*[3]). The person present at the place shall be informed of the possibility of having assistance by a person of trust (if promptly findable and suitable) (art. 391-*septies*[2]).

3.2. Investigation of computers

3.2.1. Computer investigations during inspection, search, and seizure

In Italian law, computers are considered as a particular type of information carriers that can be investigated during the investigation of places or persons. I use the term 'computer' here as shorthand for the term 'informatic or telematic system' (*sistema informatico o telematico*) that is used in Italian law (a term that is not further defined). Computers are actually part of the concept 'informatic system' (which roughly indicates the hardware and software of a computer), while

[67] Felicioni 2012, p. 122.
[68] Felicioni 2012, p. 52, quoting M. Scaparone (2008), *Procedura penale*, vol. I, Torino, p. 101.
[69] Gaito 2012, p. 1462; Morlacchini 2015, p. 1168.
[70] Tonini 2015, p. 155.
[71] Tonini 2015, p. 155.
[72] Bonetti 2003, p. 238. Felicioni (2012, p. 253) observes, however, that the provision testifies to a gradual reduction of the ambit of bank secrecy, as it allows more in some respects (e.g., to establish circumstances that are 'useful for the investigation' rather than 'to uncover the truth', and to delegate the investigation to police officials) than previous legislation did.

'telematic system' refers to telecommunications- or Internet-related systems; however, since the term 'informatic or telematic system' has been used primarily to implement the Cybercrime Convention, which uses the term 'computer system' in a broad sense (covering both informatic and telematic systems), we can use the term 'computer' as a *pars pro toto* for all informatic or telematic systems as meant in Italian law.

Prior to 2008, when computer investigations were not specifically regulated, part of the doctrine argued that seizure of a computer was an atypical means of searching for evidence, while others compared it to the seizure of documents.[73] Since Act no. 48 of 2008 (implementing the Cybercrime Convention), computer investigations are specifically regulated, and hence now fall under the typical means of searching for evidence. Computer investigations are not regulated as a separate investigation power, however; rather, they are regulated through specific rules that apply within the ordinary powers of inspection, search, and seizure.

Because of the haste with which Act no. 48 of 2008 was approved, rules applying to computer investigations have not been implemented systematically; they are spread across the various provisions on inspection, search, and seizure through inserted sub-sections or clauses, involving different (combinations of) requirements. These are basically computer-forensics-related requirements, defining requirements of result rather than means of execution.[74] However, in Tonini's view, 'Parliament forgot now one, then another of the guarantees that, instead, are all and simultaneously necessary in case of a means of searching for informatic evidence.'[75] Combining the various requirements, Tonini helpfully summarises the rules for computer investigations as follows:

> '1) The duty to preserve the original informatic data unaltered in their authenticity.
>
> 2) The duty to prevent the subsequent alteration of the original data.
>
> 3) The duty to make a copy that ensures conformity of the acquired informatic data with the original data.
>
> 4) The duty to ensure the non-modifiability of the copy of the informatic document.'[76]

Although computer investigations are thus not sui generis powers, but subsumed by the traditional investigation powers, Tonini does consider the 'informatics inspection'—defined as 'observation of the contents of an informatic or telematic system and the conservation of the original data'—to be a new autonomous type of power, to be distinguished from the inspection of goods because of the special characteristics of the inspected good (a data carrier) and of the material looked at (the data).

Although computer investigations have been regulated as part of the traditional investigation powers, the legal goods protected through the safeguards put in place by the legislator are not necessarily the same as those traditionally protected in search and seizure regulation. Felicioni refers to 'informatic privacy' and the 'informatic home' as newly emerged legal goods. Although developed in the context of substantive criminal law (particularly in the context of the criminalisation of hacking), the fact that Felicioni includes these in her treatise on search and seizure suggests that these legal goods also play a role in criminal procedure law. (This is similar to how the legal good of the peace of the domicile in the context of criminal procedure is generally interpreted through the lens of the criminalisation of trespass in substantive criminal law.) Informatic privacy relates to 'the privacy of the individual who develops his own personality also in that virtual place represented by the informatic system, regardless of the strictly personal and confidential nature of the information that might be gathered.'[77] The 'informatic home' has been identified by the Supreme Court (in relation to the criminalisation of hacking), as reported by Felicioni, as the

[73] Tonini 2015, p. 378.
[74] Felicioni 2012, p. 234-235.
[75] Tonini 2015, p. 379.
[76] Tonini 2015, p. 378-379. These four occur (in different arrangements) in several provisions. Tonini mentions a fifth requirement ('The guarantee of installing informatic seals [i.e., a hash code] on the acquired documents'), as an optional measure in art. 260 (on sealing seized goods), which in his view is essential for all informatic data. I do not include this requirement in the list, since it is not mentioned by the legislator, and can moreover be considered a corollary of the second requirement.
[77] Felicioni 2012, p. 69.

> 'ideal space pertaining to the person to which the protection of the privacy [*riservatezza*] of the individual sphere guaranteed by art. 14 Constitution [i.e., protection of the home] can be related. *Cyberspace* as a virtual place is comparable to the physical domestic place provided it is equipped[78] with security measures (for instance, *password*) that express the will of the rights-holder to exercise his *ius excludendi alios*.'[79]

3.2.2. Online (covert) searches

The use of trojans, and similar technical means to remotely access and investigate the contents or use of a computer, is generally discussed under the moniker of 'online search' (*perquisizione online*), or sometimes—inspired by the German Bundestrojaner—as 'state viruses' (*virus di Stato*) or 'informatic sensors' (*captatori informatici*). Although the technique appears to be massively used in practice, there are relatively few court cases on its lawfulness as an investigation power or on the use of resulting evidence.[80]

Court cases and doctrinal critique

Trojans have a variety of functionalities. The two primary functionalities discussed in case-law and doctrine are covertly copying data from the computer and intercepting communications, in particular oral interception through turning on the microphone.

The primary judgement on using a Trojan to **covertly copy data from computers** dates from 2009, in which the Supreme Court held that covertly installing a device on a computer to acquire the files stored on it was an atypical means of searching for evidence, and thus governed by art. 189, for which a motivated order from the Public Prosecutor suffices, which in this case was given on the basis of article 234 to acquire documents (*prova documentale*).[81] According to the Court, the secrecy of communications is not at issue because the program does not intercept a flow of communications (which implies a dialogue with other persons), but merely targets the unidirectional flow of data inside the computer's circuits.[82] Moreover, the Court did not consider the inviolability of the home to be infringed, because the computer was located in a public office, open to a 'community of people that was not particularly extensive, but neither limited or a priori determinable on the basis of a personal decision by the accused', and hence not a constitutionally protected type of place.[83]

The judgement has raised fierce criticism in the literature, for various reasons. The court's reasoning to base the assessment of the inviolability of the home on the place where the computer was located, is criticised as it misunderstands the intrinsic place-independence of computers, in relation to the protected legal good of 'informatic home' or 'informatic privacy' (see *infra* under 'The legal good'). The court's argument leads to 'protecting the data contained in a computer when this is located inside a home, but not when it is located in public places, completely ignoring the factual circumstance that—for instance through accessing the *cloud*—the subject can in both cases conduct in both places activities with the same level of sensitiveness.'[84] Moreover, the use of the Trojan at issue was not really a form of search, which typically only finds existing information; seeing that the Trojan was used to monitor the computer for eight months, it was a measure targeted also at finding future information, which is intrinsically different from securing documental evidence ex article 234 (and moreover, equating the capturing of immaterial data with the capturing of material documents is considered a category mistake).[85] Also, the lack of safeguards in evidence-gathering has been criticised, both for forensic reasons (there is no technology that does not alter the contents of a (personal) computer, violating a basic forensic principle of non-manipulation, and implying that this is a non-repeatable rather than, as the Court

[78] The original uses the term 'munito', which translates here as 'equipped' but may retain a connotation of the primary meaning, 'fortified', thus implicitly strengthening the analogy of the computer with the home as one's castle. [my footnote, BJK]
[79] Felicioni 2012, p. 69-70 (emphasis in original).
[80] Vaciago & Ramalho 2016, p. 91.
[81] Cass., Sez. V, 14 October 2009, no. 16556.
[82] Ibid., as referred to in Trogu 2014, p. 448.
[83] Ibid., as quoted in Trogu 2014, p. 448.
[84] Lasagni 2016, §4. Similarly Trogu 2014, p. 448 (observing that this reasoning would lead to 'the individual who uses his portable personal computer on the public street would lose the right to privacy on its contents, thus legitimating any public or private intrusion').
[85] Iovene 2014, p. 339.

held, a repeatable measure[86]) and for fair-trial reasons, since protections of defence interests applying to traditional searches (e.g., to know it takes place and to have a lawyer present) are absent.[87] Altogether, a considerable part of doctrine considers online covert searches for data retrieval to be unconstitutional, for lack of specific legal rules stipulating the conditions and modes of operation and lack of necessary safeguards to limit the privacy infringement to what is necessary.[88]

Nevertheless, the 2009 judgement was confirmed in the 2012 Bisignani case by the Supreme Court.[89] Interestingly, the prosecutor had requested the investigatory judge to authorise an 'online search', alongside an authorisation for oral interception, both on the basis of article 266 (interception of communications), but the judge had not considered such authorisation necessary for the online search, as, according to the 2009 judgement, a motivated order from the prosecutor would suffice. This was maintained by the Supreme Court.[90]

In contrast, in the 2012 'Ryanair' case, the Supreme Court ruled out the use of a Trojan to monitor data flows from and to a computer. The Trojan had been installed, on the basis of a search and seizure order ex article 247, to capture traveller data in the online booking system to identify, in real-time, drug-trafficking suspects.[91] The court considered this usage to be very different from traditional search and seizure, which takes place on the basis of an existing suspicion, as it was targeted rather at finding new information that might lead to a concrete suspicion; this turns the Trojan into an exploratory surveillance measure, which in that respect is similar to interception of communications, and this is not allowed under current law.[92] While the case was still discussed in terms of capturing data, not communications, the outcome thus differed from the 2009 case, possibly because of the different legal basis on which the measure had been based, or possibly because of a new insight by the Court that there is a difference between using a Trojan to covertly copy existing data (which would be allowed on the basis of acquiring documental evidence, or possibly a search) and using it to monitor future data entered into a system (which would not be allowed in the absence of specific legal rules for this form of surveillance).

The use of Trojans for **intercepting communications**, particularly **oral interception** through turning on the computer's microphone, has triggered more case-law. In the Bisignani case, the investigatory judge authorised this on the basis of article 266[2].[93] However, since article 266[2] stipulates that if communications among people present (*communicazioni tra presenti*) take place in places indicated in article 614 c.p. (homes and places of private abode), this is only allowed if there is motivated reason to believe that the criminal activity is taking place there. In the 2015 Musumeci case, the Supreme Court found that installing spyware (*programma spia*) on a portable device that turned on the microphone was a form of oral interception (generally referred to in Italian as *intercettazione ambientale*, or environmental interception), and that this can only take place 'in clearly circumscribed places, identified at the outset, and not wherever the subject might be.' It continued:

> 'At issue is a technique (…) that presents specific characteristics and that adds something with respect to the ordinary potential of interception, constituted precisely by the possibility to capture conversations between people present not only in a number of places, according to the subject's movements, but—and this constitutes the problematic fulcrum of the issue—without limitation of place. This is prohibited by the constitutional requirements of article 15 Constitution even more so than by the current statutory law.'[94]

[86] Trogu 2014, p. 454-456; Felicioni 2012, p. 71.
[87] Felicioni 2012, p. 71-72.
[88] Marcolini 2010, p. 2866-67; Iovene 2014, p. 341-342; Lasagni 2016, §4.
[89] Cass., Sez. VI, 27 November 2012, no. 254865 (Bisignani case), mentioned in Vaciagio & Ramalho 2016, p. 92.
[90] As reported in Lasagni 2016, §4, referring to Marco Torre (2015), 'Il virus di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali', *Dir. pen. proc.*, p. 1167.
[91] Torre 2015, p. 48.
[92] Cass., Sez. IV, 17 April 2012 no. 19618 ('Ryanair').
[93] Cass., Sez. VI, 27 November 2012, no. 254865.
[94] Cass., Sez. VI, 26 May 2015, no. 27100.

However, this judgement was overturned in 2016 by a decision of the United Sections of the Supreme Court in the Scurato case.[95] They observed that the requirement to specify in advance the places where the interception was to take place, was nowhere required in statutory law nor in ECHR case-law. The Musumeci judgement had confused the term commonly used for oral interception, namely 'environmental interception', which historically assumes that oral interception takes place in a particular environment in which a bug is to be placed, with the term that the law actually uses, which is interception of 'communications between persons present'. The first sentence of article 266[2], saying that communications between persons present can be intercepted in the cases listed in article 266[1], does not contain a requirement to specify the place for such interception. It is only in the second sentence that protected places are mentioned; however, this does not constitute a requirement to *specify* the place of interception beforehand as a condition of authorised interception, but rather a requirement to motivate for the purposes of specifying the mode of execution, namely when it is necessary for the oral interception to install a bug in a protected place. Such necessity is absent in the case of interception through 'informatic viruses', which is irrespective of place and by its nature a form of "itinerant" environmental interception.[96]

The import of this, according to the United Sections, is not that oral interception with Trojans in mobile devices is allowed, as the Musumeci judgment suggested, when the authorisation order *would* describe ex ante the protected places in which the interception was (expected) to take place (and motivating that crime takes place there). Rather, such use of a Trojan is effectively not allowed at all (with the significant exception, however, of organised-crime investigations, see *infra*). This is because the legislative requirement that oral interception can only take place in places of private abode if there is motivated reason to believe criminal activity takes place there, does not allow for exceptions, while the judge cannot foresee and predetermine in which places of private abode the bugged portable device will be used, making it impossible for the judge to effectively supervise that the legal requirement be respected. Allowing Trojan-based oral interception would run the risk of allowing a multiplicity of interceptions between people present in places of private abode (notably also in places of others than the interception target[97]) completely beyond what statutory law currently allows, which is incompatible with Italian law and with the proportionality requirement of article 8 ECHR. Also, it is problematic to find an appropriate sanction mechanism for recordings accidentally made in places of private abode in violation of the requirement of article 266[2], given that the provision does not prescribe a sanction itself, and that the sanction of non-usability is reserved for serious violations of the right to a fair trial (which is not at issue here), while there is also a risk of such conversations being revealed before (non-)usability is discussed. For these reasons, the Court concludes that oral interception with Trojans in mobile devices is in general not allowed.[98]

There is, however, a major exception, which applies in the present case (and which had not been considered in the Musumeci case). Article 13 of Decree-Law no. 152 of 1991 (enacted by law no. 203/91) on combatting organised crime allows for interception under broader conditions in investigations concerning organised crime or threat by telephone; and it stipulates that in organised-crime investigations, oral interception is allowed in places indicated in art. 614 c.p. also if there is no ground to believe that in such places crimes are taking place. Therefore, in organised-crime investigations, an indication of the places in which interception is to take place is irrelevant.[99] This leads the Court to conclude the following principle of law:

> 'Only in investigations of organised crime is it allowed to intercept the conversations or communications between people present—through installing an "informatic sensor" in portable electronic devices (e.g., personal computer, tablet, smartphone, etc.)—also in places of private abode ex art. 614 c.p., even if not individually identified and also if criminal activities are not taking place there.'[100]

The Court goes on to discuss what constitutes organised crime, given that this term has not been defined in the law. Reiterating the United Sections' formulation that organised crime means

[95] Cass., Sez. Un., 28 April 2016, no. 26889 (Scurato case).
[96] Cass., Sez. Un., 28 April 2016, no. 26889, §5.
[97] Cass., Sez. Un., 28 April 2016, no. 26889, §10.1.
[98] Cass., Sez. Un., 28 April 2016, no. 26889, §6.
[99] Cass., Sez. Un., 28 April 2016, no. 26889, §7.
[100] Cass., Sez. Un., 28 April 2016, no. 26889, §11.

'that which has as its object any case characterised by a stable organisation programmatically oriented to commissioning multiple crimes',[101] the Court ultimately formulated the following principle of law:

> 'Offences of organised crime should be understood as comprising not only those listed in art. 51, paras 3-*bis* and 3-*quater* CPC, but also those anyhow depending on an association to commit crime, ex art. 416 c.p.,[102] related to more diverse criminal activities, excluding the mere aiding and abetting (*concorso*) of persons in crime.'[103]

The Scurato judgement is discussed critically by Lasagni, particularly in relation to the last issue: the scope of the definition of organised crime. The list of crimes in article 51[3-*bis*] has been expanded over time and is heterogeneous, and not always based on clearly identifiable criteria.[104] Given that the Public Prosecutor has discretionary power to qualify something as organised crime, it would be desirable to introduce some form of control over this discretionary power, to prevent wrongful collection of potentially extremely sensitive information.[105]

For **video recordings** (using spyware to turn on the computer's or phone's camera), the norms for visual recordings apply (see *infra*, s. 4.3.1), according to the Supreme Court in the Musumeci case.[106] Briefly put, such use of Trojans is allowed, as atypical means of searching for evidence, if visual recordings are made in public places or places exposed to the public, but not in places of private abode or in situations where personal privacy needs to be protected (such as public toilets). Images made in the latter cases have to be excluded from evidence.[107] Although this case has not been overturned by the Scurato judgement (since that discussed only oral interception), one can imagine that the United Sections' reasoning applies here as well—*a fortiori* since visual recordings inside protected places is not allowed at all—so that it can arguably be concluded that, despite the Musumeci case, visual observation through Trojans in mobile devices is not allowed. Only fixed computers in public or publicly accessible places might be infected with malware to turn on a webcam.

Law proposals

The need for regulating the investigative measure of covert online investigations (search and surveillance) has been recognised by the legislature, although so far no proposal has been successful.[108] An amendment to an anti-terrorism Bill of 2015 proposed to add to article 266-*bis* (which regulates interception of informatic or telematic communications, essentially similarly to art. 266) a clause that interception of communication flows relating to informatic or telematics systems would also be possible 'through employing instruments and informatic programs to remotely acquire communications and data present in an information system'; subsequently, an amendment was presented to limit the scope of this to investigations of certain crimes with terrorist purposes.[109] The amendments were rejected, however, as was a subsequent Bill proposing the same clause.[110] In April 2016, a Bill was proposed 'on investigations and seizure

[101] Cass., Sez. Un., 28 April 2016, no. 26889, §14 (referring to Cass., Sez. Un., 15 July 2010, no. 37501).
[102] I.e., when 'three or more persons join for the purpose of committing multiple crimes' (art. 416[1] c.p.).
[103] Cass., Sez. Un., 28 April 2016, no. 26889, §16.
[104] Lasagni 2016, p. 19. The author also observes that the judgement overlooks the fact that Decree-Law no. 152 of 1991 does not only cover organised crime, but has been extended also with crimes against exploitation of prostitution and crimes against individual personality (through art. 9 of Law of 11 August 2003, no. 228), besides already applying also to threat by telephone (ibid.). It is unclear to me, however, whether this extension of the scope of article 13 by Law 228/2003 refers to the possibility of interception under less strict conditions (as meant in the first sentence of art. 13) or also to the possibility of oral interception in protected places (as meant in the third sentence of art. 13); the offence of threat by telephone is in any case mentioned only in the first sentence, not the third, so this offence (except if organised) does not allow Trojan-based oral interception
[105] Lasagni 2016, p. 21.
[106] Cass., Sez. VI, 26 May 2015, no. 27100, §3.
[107] Cass., Sez. VI, 26 May 2015, no. 27100, §3.
[108] See the overviews in Vaciago & Ramalho 2016, p. 92-93 and Cass., Sez. Un., 28 April 2016, no. 26889, §2.
[109] Proposed Decree-Law No. 7 of 18 February 2015, as quoted in Cass., Sez. Un., 28 April 2016, no. 26889, §2.2.
[110] Legislative proposal by Greco, 2 December 2015, XVII Legislature, 3470. Although the motivation for the proposal was to combat terrorist crimes, the actual text of the proposed clause did not include a limitation to terrorist crimes.

relating to data and communications in informatic or telematic systems', which would introduce the possibility to employ 'lawful sensors' (*captatori legali*) for a number of functionalities: remote search, remote seizure of data other than traffic data (both limited to, briefly put, organised crimes), and interception of data flows in informatic systems and geographic localisation of the device, along with several safeguards (such as a subsidiarity requirement, protection measures of acquired data, and technical requirements of the 'sensors').[111] Also, an amendment has been proposed to another Bill to regulate the use of Trojans for oral interception.[112] These proposals are pending as of August 2016.

The legal good to be protected by regulation of online covert searches and surveillance

Legal doctrine, reflecting on the cases involving the use of police Trojans, has made a considerable effort to articulate which legal goods are at issue in this new type of investigation power. They base their criticism of the 2009 judgement, and their overall conclusion that legislative intervention is required before Trojans can be employed, on what they perceive as the main legal goods at stake. Marcolini considers a covert online search to implicate the legal good of the privacy in personal data[113] or (not being clearly consistent) the privacy of private life.[114] Torre observes that the 'inviolability of the mind' (*inviolabilità della psiche*) is infringed, if the Trojan captures whatever the investigated person writes, also if he decides to immediately delete what he has just written.[115] Trogu considers the primary legal good to be the 'informatic home' (which has been conceptualised in doctrine on the hacking offence[116]). This needs to be protected 'as the virtual space (but also physical space in which the informatic data are contained) relating to the individual sphere, which is also constitutionally protected, over which the owner can exercise towards third persons both the *jus prohibendi* and the *jus admittendi*, with a legitimate expectation of privacy.'[117] This protection is aimed 'not only at the very personal contents of the data collected in the protected informatic systems, but offers a wider protection that materialises in the user's *jus excludendi alios*, whatever the contents of the data contained in them, even if pertaining to the sphere of thought or to work activities or not.'[118] And since it is the informatic home that is at stake, covert remote investigations of computers are most similar to making video recordings (of non-communicative behaviour) inside the home, which is not allowed.[119]

Iovene offers perhaps the most profound reflection on the legal good. Observing that the distinction between 'intimate data' and 'social data' (or shared data), between secret information (i.e., unknown) and reserved information (i.e., known but treated with reserve), has lost relevance in today's world, she argues that what is at issue is no longer a matter only of data protection or informational self-determination, but more fundamentally one of the right to personality. It is necessary, she argues, 'to protect the informatic system as a space in which the individual expresses his personality, regardless of the nature of the information entrusted to it.'[120] While it may no longer be possible, in the world of web 2.0, to distinguish between the public and the private sphere, the right to be let alone may have lost some value but continues to capture an essential part of the problem. It is now necessary to 'reaffirm the existence of that sphere of privacy, whose classic boundaries, linked to the physical spaces and to the type of information that one wants to keep others from knowing, are blurring and dissolving.'[121] This can be done by recognising a new legal good, worthy of constitutional protection. While the 'informatic home' seems a good candidate for that, it is not sufficiently precise, since the home serves the interest of the *jus excludendi alios* from a pre-eminently personal or intimate sphere, while computer systems involve a broader range of activities in which people express their personalities, also in

[111] Bill C. 3762, as described in Cass., Sez. Un., 28 April 2016, no. 26889, §2.4.
[112] 'Casson' amendment, mentioned in Vaciago & Ramalho 2016, p. 93.
[113] Marcolini 2010, p. 2861. Also Lasagni 2016, p. 14-15 considers the protection of personal data to be the primary interest involved in online covert searches and surveillance.
[114] Marcolini 2010, p. 2866.
[115] Torre 2015, p. 28.
[116] See Koops 2016, s. 3.2.2 for a brief discussion.
[117] Trogu 2014, p. 434, with reference to Cass., Sez. VI, 4 October4 1999, no. 3067.
[118] Trogu 2014, p. 435, with reference to Cass., Sez. VI, 4 October4 1999, no. 3067.
[119] Trogu 2014, p. 447.
[120] Iovene 2014, p. 334.
[121] Iovene 2014, p. 335.

developing social relations online or in other 'informatic' spaces.[122] In other words, since informatic systems collapse the personal and the social spheres of life, the interest at stake is not so much in protection of an informatic 'home' to enable controlling *access to* information as such, but in protection of informatic privacy (in the sense of reserve, *riservatezza*) to enable controlling what happens with information. Thus, it is 'informatic privacy' (*riservatezza informatica*) that is the legal good to be protected, which can be described as the 'exclusive interest, legally recognised, to enjoy, dispose, and control the digitised information, processes, systems and "spaces", and their uses'.[123] The right to informatic privacy arises as an autonomous right, expanding from the home, given a digital environment 'in which there are no boundaries or *physical* places that are able to reflect the private or reserved character of the activities that take place there or of what is kept there.'[124]

The implication of (informatic) privacy being the primary legal good implicated by covert online searches is that there are no specific constitutional requirements for intrusions, since the right to privacy falls under article 2 Constitution, which, in contrast to articles 13-15, does not require particular statutory guarantees, other than a motivated decree by a judicial authority (which can be a judge but also a prosecutor). However, as Iovene and Torre, among others, point out, European law prevails over statutory law, and since covert online searches infringe article 8 ECHR and article 7 EU Charter, a specific regulation (describing the cases and modes of infringement) by law is nevertheless required.[125] Interesting to note is Iovene's reasoning that it is article 7 of the EU Charter of Fundamental Rights (the right to privacy) rather than article 8 (the right to data protection) that is at stake:

> 'It is not so much to guarantee to the affected person the control of the ways in which his personal data are processed; rather, more fundamentally, to protect the person in a context in which the most varied aspects of his private life are translated into data, which are susceptible to informatic processing. In an environment in which it is no longer possible to distinguish between intimate, reserved, and social data, article 8 Charter turns out inapplicable and one should turn to the wide protection offered by article 7 to protect private life.'[126]

3.3. Investigation of vehicles

Apart from those specifically meant for living domestic life or other private activities in closed spaces (*supra*, 3.1.3), vehicles as such are not consistently considered a home. Part of legal doctrine considers cars to be closed places where people develop their personality, and thus to count as homes,[127] while another part of doctrine, as well as most case-law, seems to consider cars to be unsuited for developing acts of domestic life or relations, and thus not to count as homes in the context of searches. In the latter interpretation, searches of cars belong to the domain of personal searches (*infra*, 4.1.1), the car being considered to fall within the person's sphere of custody.[128]

4. The protection of persons

4.1. Protection from interference with the body

4.1.1. Inspection and search of the body

Inspection of a person (*ispezione personale*) consists in observing and describing the body of a living human being, or part thereof. This concerns not only the normally visible exterior parts of the body, but also those parts normally concealed from view. Thus, it includes for instance a radiographic examination of the inside of someone's body to check whether balls with drugs are

[122] Iovene 2014, p. 335, also referring to R. Flor, 'Brevi riflessioni a margine della sentenza del *Bundesverfassungsgericht* sulla c.d. *Online Durchsuchung*', *Riv. trim. dir. pen. ec.*, 2009, p. 697 et seq.
[123] Iovene 2014, p. 335, quoting R. Flor, '*Phishing, identity theft*, e *identity abuse*. Le prospettive applicative del diritto penale vigente', *Riv. it. dir. proc. pen.*, 2007, p. 899 et seq.
[124] Iovene 2014, p. 336 (emphasis in original).
[125] Iovene 2014, p. 336-337; Torre 2015, p. 29.
[126] Iovene 2014, p. 338.
[127] Felicioni 2012, p. 111, with references.
[128] Felicioni 2012, p. 111, with references.

hidden there; such an examination, to be conducted by a doctor, can be ordered by a judicial authority.[129]

Article 245 contains some specific rules for personal searches. First, inspected persons need to be informed beforehand that they can have themselves be assisted by a person of trust (provided they can be found promptly and are suitable). Second, the inspection is to be conducted with respect to dignity and, as far as possible, of the decency (*pudore*) of the person subjected to the inspection. The inspection can be carried out by a doctor, in which case the judiciary authority may abstain from being present at the operation. Moreover, art. 79 disp. att. stipulates that personal inspections (as well as searches) have to be conducted by a person of the same sex, unless this is impossible or in absolutely urgent cases; this requirement does not apply, however, if the inspection or search is conducted by a medical professional.

During the preliminary investigations, the police can conduct certain activities at their own accord, which includes (if there is risk of modification or loss of evidence) verifications and surveys on persons (*accertamenti e rilievi sulle persone*) that do not constitute a personal inspection (art. 354[3]); this can include inspection of body parts that are not covered by clothes,[130] but not further-reaching forms of inspection.

A search of a person (*perquisizione personale*) can take place if there are grounds to believe that someone conceals on his body a *corpus delicti* or things pertaining to the crime (art. 247[1]). Similar safeguards as for personal inspections apply (being informed of person-of-trust assistance possibility, respect for dignity and, as far as possible, decency) (art. 249). Also in the context of a personal search, the forced radiographic examination of the inside of someone's body (such as the stomach to check for swallowed drug balls) can be ordered.[131] For other forced medical examinations, however, a special regime applies, similarly to taking bodily material for DNA profiling without a person's consent, which requires a motivated order by the judge if it is absolutely indispensable for proving the facts (art. 224-*bis*; see also art. 359-*bis*). However, DNA material left on the crime scene, corpses, or objects can be acquired without particular statutory safeguards (on the basis of art. 354: urgent verifications on places, things, and persons), as this is not considered to interfere with individual freedoms, including personal liberty of article 13 Constitution.[132]

4.1.2. Body-related identification measures

The police can use measure to establish the identity of unidentified persons (suspects as well as victims and witnesses), on the basis of article 349. If someone refuses to identify herself (or provides a presumably false identity), the person can be forced to accompany the police to the police station, where they can be detained for at most 12 (or in complex cases 24) hours (art. 349[4]). In the case of suspects, fingerprints, photos and other anthropometric surveys can be taken (art. 349[2]). This includes taking hair or saliva with consent; if the suspect does not consent, this material can be forcibly taken (provided the person's dignity be respected) with written authorisation by the Public Prosecutor (art. 349[2-*bis*]).

4.2. Protection from interference with the mind

Article 188 protects the moral liberty (*libertà morale*, i.e., mental self-determination) of persons: 'Methods or techniques that are suitable for influencing the freedom of self-determination or altering the capacity to remember and to assess the facts cannot be used, not even with consent of the person at issue.' This implies that measures such as hypnosis, narcoanalysis and lie detectors cannot be used in criminal investigation,[133] neither as incriminating nor as disculpatory evidence.[134] Article 188 thus expresses as a general legal principle in criminal procedure the specific rule that forbids similar methods and techniques during interrogation (art. 64[2]).[135] The same principle is visible in article 189, which stipulates that atypical means of searching for

[129] Tonini 2015, p. 380, referring to Cass., Sez. IV, 2 December 2005, *Guida dir.* 2006, 13, 102.
[130] Tonini 2015, p. 381.
[131] Tonini 2015, p. 382.
[132] Tonini 2015, p. 382 and 517-518.
[133] Bonetti 2003, p. 203; Chiavario 2012, p. 351.
[134] Bonetti 2003, p. 204.
[135] Bonetti 2003, p. 202.

evidence are allowed if they are suitable for proving the facts but only if they do not prejudice the moral liberty of the person.

The principle does not preclude, however, acts of force if the will of the suspect is bent on obstructing an act of investigation that does not require his active participation,[136] or being submitted against his will to a confrontation with a view to identifying the suspect.[137] Also allowed are confrontations (*confronti*) between persons that have already been questioned or interrogated, where their statements are not in line with one another, so that, for example, memories will be better recalled when confronted with others' memories (art. 211-212).

4.3. Protections for behavioural privacy

4.3.1. Visual observation

The regulation of the use of visual observation is based on a series of distinctions. Preliminarily, however, it should be noted that the literature only refers to visual *recordings* in criminal procedure; visual observation by law-enforcement agents, without use of technical devices, is presumably allowed as long as no fundamental rights are infringed, but it is not regulated as a means of searching for evidence (except in the form of inspection, *supra*, 3.1.1, which is not the kind of visual observation meant in this section).

A first distinction is whether visual recordings are made within or outside the context of criminal investigation. Recordings made outside the context of criminal procedure, whether by private or by public parties, can be used as evidence in the form of documental evidence (art. 234 et seq.). This also applies to (private or public) CCTV footage.[138] It may be excluded as evidence, however, if the recordings were made illicitly, although there are different views whether illegal recordings are necessarily unusable.[139] In any case, visual recordings that contain illegally recorded communicational content have to be excluded and destroyed (art. 240[2-6]).

For recordings made by law-enforcement agencies in the course of criminal investigation, if they are instrumental to executing another investigation power, such as recording what is found during an inspection or search, this is regulated by those investigation powers.[140] It is the situation in which visual recordings are not instrumental to another power, but a goal in themselves, i.e., when they are used as a means of their own to acquire evidence, that is the main topic of debate in Italy.

Under the previous Code, the situation was relatively clear, as the legislator, when introducing interception legislation, had inserted a provision in the Code in 1974 that prohibited law-enforcement agents from making visual or auditory recordings in the home (art. 226-*quinquies* CCP-1930).[141] This prohibition was connected to the offence criminalised in art. 615-*bis* Criminal Code, which prohibits to use of visual or auditory recording devices to unduly procure information or images pertaining to the private life taking place in the places indicated in article 614 (i.e., the home, other places of private abode, and appurtenances).[142] Since this offence is limited to 'unduly' (*indebitamente*) procuring images, the prohibition of art. 226-*quinquies* (old) was interpreted as only covering visual observation taking place *inside* the home; images recorded from the outside (*ab extra*), e.g., the courtyard of an apartment block (an appurtenance), were considered admissible. Such so-called '*home-watching*' (this English term is used in Italian) might be indiscrete, but not 'undue': 'who wants to stay away from possible looks, turn off the light and close the shutters'.[143]

The new Code of 1988, however, only took over the prohibition of auditory recordings in the home (and allowing an exception there, see *infra*, 4.5.1), but did not say anything about visual recordings in the home. This was probably not a conscious choice but an oversight by the legislator.[144] As a result, visual recordings in criminal investigation are not regulated in the Code,

[136] Bonetti 2003, p. 204.
[137] Gaito 2012, p. 1088.
[138] Tonino 2015, p. 410, 412.
[139] Marinelli 2007, p. 169-170 (arguing that a doctrinal majority considers illicit recordings to be usable as evidence, implying a distinction between substantive and procedural consequences of unlawful acts).
[140] Tabasco 2011, p. 142-143.
[141] Rizzo 2012, p. 2.
[142] See Koops 2016, s. 3.1, for a discussion of art. 615-*bis* CC.
[143] Rizzo 2012, p. 3, quoting Cordero, *Procedura penale*, 2006, p. 851.
[144] Rizzo 2012, p. 5.

leading to extensive discussions in doctrine and various interpretations in case-law. Eventually, case-law converged in a decision by the United Sections of the Supreme Court in 2006,[145] setting out the main parameters for visual observation, which have been followed in case-law since.

The Court first distinguishes between visual recordings of communicative behaviour and visual recordings of non-communicative behaviour. Behaviour is communicative when a message is intentionally transmitted from someone to another,[146] or when there is 'a minimum of dialogical relationship between present subjects'[147]; this includes speech, sign language, body language (*gesti*), and conventional signs.[148] If the recordings show communicative behaviour, then this is regulated by the provisions on oral interception (art. 266[2], see *infra*, 4.5.1). The distinction between communicative and non-communicative behaviour is not clear-cut; it is criticised by some as 'difficult, weak, and fluctuating'.[149] For instance, since messages in the sense of communication are generally expressions of thought, and these can be expressed in various ways, such expressions can also be made without being directed to someone; it is difficult to classify such non-targeted expressions.[150] Nevertheless, the distinction is firmly rooted in case-law and most doctrine, and in many cases, it will be relatively clear whether certain behaviour is communicative or not.

If it is determined beforehand that visual recordings are to be made of non-communicative behaviour, i.e., if the law-enforcement officials expect to record only non-communicative behaviour, then the lawfulness of this depends on the place where the recordings are made. This relates to the rights that can be harmed by recordings. While communicative recordings infringe the secrecy of communications, non-communicative recordings infringe either the privacy of the home or the general right to privacy, or they do not infringe fundamental rights at all. Thus, the Supreme Court distinguishes between three types of places that influence the lawfulness of visual observation.[151]

Recordings made in **domiciliary places** (those protected by art. 14 Constitution[152]) are not allowed, regardless of whether or not the inhabitant is present. In 2002, the Constitutional Court had already determined that the mention of inspections, searches and seizure as exceptions allowed on the basis of article 14[2] Constitution was not-exhaustive: also other forms of intrusions (enabled by technological developments unforeseen by the constitutional legislator), such as audio-visual recordings, are possible.[153] This also implies that the constitutional protection of domiciles serves to protect not only the right to include or exclude others from entering the place; it also protects 'an intangible sphere of privacy (*riservatezza*), which can also be harmed—through technical devices—without the necessity of physical intrusion.'[154] In contrast to oral interception, however, there is no legal basis, nor a stipulation of legal guarantees, for visual recordings in domiciliary places, so that the Supreme Court concludes that this is not allowed.[155] As a result, not only are such recordings inadmissible as evidence; also, law-enforcement agents making visual recordings in domiciliary places will commit the offence of article 615-bis para. 3 Criminal Code, which criminalises with one to five years' imprisonment the undue making of images with (audio)visual recording devices in domiciles by public officials with abuse of power or with violation of the obligations inherent to the function.

There are two general exceptions to this. First, visual observation within the home is allowed as an incidental by-product of an authorised oral interception activity (where it was determined *ex ante* that (audio)visual recordings of communicational gestures were needed for investigative

[145] Cass., Sez. un., 28 July 2006, *Dir. pen. proc.*, 2006, p. 1349 et seq.
[146] Cass., Sez. IV, 19 January 2005, *Riv. pen.* 2006, p. 363, quoted in Marinelli 2007, p. 173n.
[147] Tabasco 2011, p. 158 (referring to Cisterna).
[148] Marinelli 2007, p. 176.
[149] Tabasco 2011, p. 158 (referring to Camon).
[150] Tabasco 2011, p. 159.
[151] Cass., Sez. un., 28 July 2006, *Dir. pen. proc.*, 2006, p. 1349 et seq.
[152] Art. 14 Constitution speaks simply of domicile (*domicilio*). The domicile is usually divided into three types of places, following the shaping of its protection in the Criminal Code, primarily through art. 614 ('violation of domicile'), which mentions the home (*abitazione*), other places of private abode (*luoghi di privata dimora*), and appurtenances (*appartenenze*).
[153] Corte cost. 24 April 2002, n. 135, *Giur. cost.* 2002, p. 2176 et seq., referred to in Tabasco 2011, p. 147-149.
[154] Tabasco 2011, p. 155.
[155] Cass., Sez. un., 28 July 2006, *Dir. pen. proc.*, 2006, p. 1349 et seq. The method cannot be based on the power of domiciliary inspection: although visual recordings are a form of *inspicere*, they are meant for covert observation, in contrast to the overt method of inspection; Felicioni 2012, p. 114-115.

purposes).[156] Second, if behaviour in domiciliary places is itself not reserved so that it can be observed by outsiders without resorting to particular devices, the protection of domiciles does not apply. For example, someone leaning out of a window,[157] or on a balcony overlooking a public street who can be observed by passers-by without having to use a zoom camera, can simply be recorded by the police, similarly to observation in public places.[158] Visual recordings of people in domiciles are thus not allowed if the investigatory agency has to overcome, through appropriate manoeuvres or applying special instruments, a barrier between the public and the filmed person.[159]

Since domiciles are strongly protected against visual recordings, it is important to determine what counts as a domicile. In the case in point, the Court had to determine whether so-called '*privès*', cubicles on the upper floor of the public locale 'Bora Bora' (where prostitution was suspected to occur), constituted a domicile. Clients could, after payment, withdraw for ten minutes with a girl of their choice in these cubicles, which were separated from the corridor by heavy curtains.[160]

Two streams of interpretation had previously been used in case-law to determine whether the toilet in a public locale (somewhat similar to the *privè* at issue) constitute a domicile in the sense of article 14 Constitution. One stream emphasised that the constitution protects 'places in which an area of intimacy and privacy (*riservatezza*) is temporarily guaranteed', and that this applies also to a publicly accessible toilet since someone entering such a place does not renounce their intimacy or privacy, while they can also temporarily exclude other people from entering the place.[161] Thus, this interpretation focuses on the exclusive character of a place (the *ius excludendi*) and the protection of privacy in the interpretation of domiciliary places.[162]

Another stream, in contrast, emphasised that a place of private abode 'is constituted by a certain "stability" of the relationship between the place and the person that makes use of it', which is absent in the case of a publicly available toilet.[163] In this interpretation, domiciliary places are characterised by the use of a place for executing manifestations of private life (such as repose, nourishment, study, professional activity, leisure) by the people who occupy the place, with a certain duration.[164]

In the 2006 judgement, the Supreme Court followed the latter stream, finding that a public toilet cannot be considered a domicile when it is occupied by a person, and that the same applied to the cubicles in Bora Bora, an environment in which clients withdrew 'for a few minutes' with a girl, under vigilance of the staff, so that no domiciliary character could be attributed to the temporary usage of the cubicles.[165] It is interesting to note that the Court observes on the side here that case-law tends to have an expansive interpretation of the concept of domicile in substantive criminal law (in relation to art. 614-615bis Criminal Code), but a restrictive interpretation of domiciles in the context of criminal procedure.[166]

However, the Court did not want to conclude that the cubicles were public or publicly accessible places without privacy protection. It thus invented[167] an in-between category of private places or '**reserved places**': 'if a public toilet or a cubicle such as those at issue are not a domicile, they are nevertheless a place which should protect the intimacy and the privacy of the

[156] Cass. Sez. IV, 20 March 2008, *Guida dir.* 2008, p. 18, 97, quoted in Tonini 2015, p. 411.
[157] Tabasco 2011, p. 156.
[158] Tonino 2015, p. 412. Cf. also Cass., Sez. II, 24 October – 12 November 2014, n. 46786, quoted in Tonino 2015, p. 412 (considering legitimate and freely usable without any judicial authorization video recordings made by private parties through external cameras installed on their property directed at the entrance, courtyard, and balconies of the domiciles of others, since actions in these circumstances cannot have any claim to privacy, being places, although of private abode, that are freely visible from the outside without taking recourse to particular devices).
[159] Tabasco 2011, p. 156.
[160] Rizzo 2012, p. 37.
[161] Cass., Sez. IV, 16 March 2000, quoted in Rizzo 2012, p. 48.
[162] Cass., Sez. un., 28 July 2006, *Dir. pen. proc.*, 2006, quoted in Rizzo 2012, p. 47.
[163] Cass., Sez. VI, 10 January 2003, n. 3443 and 6962, and Sez. VI, 19 November 2005, n. 11654, quoted in Rizzo 2012, p. 48.
[164] Rizzo 2012, p. 47.
[165] Cass., Sez. un., 28 July 2006, *Dir. pen. proc.*, 2006, quoted in Rizzo 2012, p. 48.
[166] Rizzo 2012, p. 47.
[167] A step criticised by Rizzo 2012, p. 50, as the Court assuming the position of the legislator here, since there was no basis in the law for this distinction.

persons, and that therefore for the purposes of visual recordings they cannot be treated as a public place or a place exposed to the public.'[168] The ground for protecting reserved places that are not domiciles is article 2 Constitution, which includes the general right to privacy. Visual recordings in such reserved places can be made, but only with a motivated decree by a judicial authority, which can be a judge but also a public prosecutor. The results can be used as atypical evidence.[169] This also applies to recordings made by a victim (*in casu*, in an apartment used as a professional studio as the habitual working place) in accordance with the police.[170]

For the third category, **public places**, the Supreme Court judged that there is not any expectation of privacy in public places in relation to pictures. Therefore, the police can make visual recordings on their own initiative, which is also usable as atypical evidence.[171] Examples of such public places from case-law are a construction site (even if private property), the foreground (*piazzale*) of an enterprise, or the locale of a public official.[172] (Note that the same applies to visual recordings in empty reserved places: since the protection of reserved places is connected to the privacy rights of the people temporarily visiting the place, the requirement of a motived order by the Public Prosecutor only applies when the place is occupied.)

The Supreme Court's decision has been criticised,[173] particularly because the combination of the communication/non-communication and the domicile/private place distinctions lead to some seeming inconsistencies. In private (non-domiciliary) places, people are less protected against visual observation than against auditory observation, because visual recording only requires an order by the prosecutor, while oral interception requires an order from the investigatory judge, and the other legal guarantees applying to oral interception do not apply to visual observation. In contrast, in domiciles, people are better protected against visual observation (which is not allowed at all) than against auditory observation.[174] Moreover, law enforcement can easily circumvent the apparent intention to prohibit visual observation in domiciles by using the communication/non-communication distinction, through arguing that they intend, *ex ante*, to visually record communicative behaviour, and then they can use images of non-communicative behaviour as by-catch.[175] More generally, Rizzo argues that there is no reason to consider visual observation (in reserved places) as less intrusive than auditory observation, and that visual and auditory observation should simply be treated alike under the regime of oral interception, regardless or the fact whether the observed behaviour is communicative or non-communicative.[176]

4.3.2. Location tracking

Human tailing

Tracking the movements of a suspect by covertly following him—i.e., tailing or shadowing (*pedinamento*, etymologically suggesting 'following on foot'[177])—falls under the ordinary activities that the police can do on the basis of their task description, as indicated in articles 55, 347-348 and 370.[178] These articles allow the police to conduct activities that do not substantially infringe fundamental rights or liberties, without further specific statutory rules or safeguards. Tailing is

[168] Cass., Sez. un., 28 July 2006, *Dir. pen. proc.*, 2006, quoted in Rizzo 2012, p. 48-49.
[169] Rizzo 2012, p. 49; Tonino 2015, p. 411.
[170] Cass., Sez. III, 19 October 2010, Dir. pen. proc. 2010, p. 1419-30, referred to in Tabasco 2011, p. 153. Tabasco (2011, p. 163) argues that covert visual recordings by the defence can only be used if there is prior judicial authorisation, except when they are made in public places or places exposed to the public.
[171] Tonino 2015, p. 411.
[172] Rizzo 2012, p. 54 (with references).
[173] See extensively Rizzo 2012.
[174] Tabasco 2011, p. 159-160; Rizzo 2012, p. 51.
[175] Rizzo 2012, p. 42.
[176] Rizzo 2012, p. 51-52. Rizzo (p. 2-3) argues that visual observation 'presents an analogous intrusiveness as that of communications interception: covert surveillance which stretches over time and effected through devices that permit going beyond normal sensory perception'. Cf. also Camon 1999, p. 1193 (quoted in Rizzo 2012, p. 2), who argued that 'visual interception' may be very relevant for criminal investigation, but that this comes at a high price 'because of the "shifting" of the technology typical for interception, here applied to intrude upon rights that traditionally are interfered with by inspections or searches: this results in a hybrid of extraordinary harmful capacities.'
[177] Marinelli 2007, p. 227.
[178] See *supra* n. 26 and surrounding text.

considered an activity that constitutes at most a minor privacy interference, so that no specific legal safeguards apply.

GPS tracking

GPS tracking (i.e., attaching a GPS tracking device to a person or object that records the location or transmits this in real-time to a receiver) is usually referred to as 'electronic tailing' (*pedinamento elettronico*) or 'distant tailing' (*pedinamenti a distanza*)[179] (both of which may also cover other forms of technology-facilitated location tracking) or 'satellite tracking' (*tracking satellitare*)[180]. It is also discussed, along with other forms of location tracking, as 'geolocalisation' (*geolocalizzazione*). GPS tracking cannot be qualified under any specifically regulated investigation power. For instance, it is not a form of inspection (although that power might also be used applying technical means), because it is not directed at finding traces or other material effects of the crime.[181] Neither does it fall under the power of communications interception, because that power is targeted at intercepting the contents of communications between two or more persons; this does not cover 'the investigative activity conducted to follow the movements on the territory of a person, to locate him and therefore to examine—at a distance—not the flow of communications that he himself sends or receives, but his presence at a specific place at a certain moment, as well as the followed itinerary, the encounters that occurred etc.'[182]

In a consistent stream of case-law, spearheaded by a judgement of 2002, the Supreme Court has found that GPS tracking is 'a modality, technologically typified, of tailing. As such, it falls under the so-called atypical or non-nominated means of searching for evidence.' Given that it does not infringe upon the constitutional right to secrecy of communications (art. 15 Constitution), it can, just as human tailing (albeit technologically facilitated at a distance), be considered an ordinary activity of examination and ascertainment required from the police on the basis of articles 55, 347 and 370 CPC. Thus, no judicial authorisation is required, not even—in contrast to a production order of traffic data—a motivated order from the Public Prosecutor.[183] The Court observes that the legislator can always intervene with specific norms if he thinks it relevant in light of technological developments.[184]

Thus, the police—both police agents and officials—can conduct GPS tracking at their own initiative. The object of tracking will usually be the suspect, but also others can be traced, such as victims or defendants in connected cases.[185]

As an atypical means of searching for evidence, GPS tracking is governed by article 189, implying that results can be admitted by the judge if they are suitable for proving the facts and do not prejudice the moral liberty of the person. The first requirement is obviously met, and the second as well, because moral liberty is prejudiced only when the person is affected in his mental freedom to choose; since GPS tracking is a covert measure, not noticed by the subject, and the resulting data are not statements (expressions of the mind), the followed person's mental self-determination is not at stake.[186] Although article 189 also includes the clause that results are admitted 'after the parties have been heard on the modalities of allowing the evidence', this is considered not to apply *ex ante* to covert investigation measures, as that would unavoidably thwart the purpose of the measure. Therefore, the parties will only be heard on admitting the resulting evidence, not the evidence collection as such, which is largely a matter of discussing the reliability of the evidence.

While *using* GPS tracking devices is thus not considered in case-law to constitute a substantial privacy infringement, doctrine points out that *placing* GPS devices may be problematic if done in the passenger compartment (*abitacolo*) of a car. A part of doctrine and case-law considers the inside of a car to be a place of private abode, which are considered protected spaces alongside dwellings and appurtenances,[187] implying that entering into a car to place a GPS tracker would

[179] E.g., Aprile & Spiezia 2004, p. 156.
[180] Gentile 2010.
[181] Bene 2014, p. 349.
[182] Cass., Sez. V, 27 February 2002, no. 16130.
[183] Cass., Sez. V, 27 February 2002, no. 16130. See also, e.g., Cass., Sez, I, 10 February 2012, no. 14529, quoted in Bene 2014, p. 348.
[184] Cass., Sez. V, 27 February 2002, no. 16130.
[185] Marinelli 2007, p. 230-231.
[186] Aprile & Spiezia 2004, p. 158-159; Marinelli 2007, p. 240-241; Tabasco 2011, p. 166.
[187] See *supra*, n. 57 and surrounding text.

not be allowed, in the absence of specific legislation indicating the modality and safeguards that should apply to this measure. A majority of doctrine accepts this interpretation of cars, while a majority of case-law rejects it.[188] In doctrine, a car destined for personal use has been considered to be a place of private abode because 'it does not matter whether the place is entirely closed or partially open, in order (…) to be isolated from the external environment in a manner that makes obvious and normally effective the will of the inhabitants to withdraw into domestic life, and thus to exclude outsiders.'[189] Although the issue frequently recurs in literature on GPS tracking, Bene dryly observes that the discussion is highly academic because technological evolution has enabled the placing of GPS trackers also on the *outside* of vehicles, thus foregoing the problem of having to enter a protected space.[190]

The current state of the (case-)law is heavily criticised in the literature. Several authors question the equation of GPS tracking or 'distant tailing' with mere human tailing. They provide arguments why GPS tracking is more pervasive than traditional tailing: it can be very precise and continuous, it can track people also in places that are not visible or readily accessible (where human tailing would be impracticable or not allowed),[191] it has fewer practical obstacles in time and space,[192] and it constitutes a greater privacy infringement than classic tailing because of the thoroughness of the investigation and the possibility to protract it for long periods.[193] On the other hand, authors also observe that a person's movements are tracked only when the tagged car or object is being used, which is less frequent than continuous human tailing,[194] and physical tailing moreover enables police to see the location of others during meetings, which is not possible with electronic tailing unless the other persons are also being electronically monitored.[195] Overall, however, authors tend to consider GPS tracking to constitute a more serious privacy infringement than human tailing, although still less serious than intercepting communications.

More importantly, authors criticise the Supreme Court's limiting its testing of the human-rights infringement to article 15 Constitution, arguing that also other fundamental rights are at stake. Tabasco, for instance, observes that the legislator has passed a law regulating the production order of traffic data (which includes location data generated by cell-phone use), to safeguard the protection of personal data; given the similarity, similar safeguards should apply to GPS tracking, in particular a motivated order by the Public Prosecutor.[196] Such a requirement is fairly broadly advocated in the literature.[197] Bene also concludes, on the basis of data protection (particularly of so-called 'sensitive data') and a comparison with foreign case-law (*Uzun v. Germany*, *United States v. Jones*), that legislative action is required to introduce safeguards, particularly for GPS tracking 'for longer periods, in which the risk is more concrete that the subject will park also in places of private abode.'[198] Costanzo refers to the French Supreme Court, which considered authorisation from a judge to be necessary: 'la technique dite de 'géolocalisation' constitue une ingérence dans la vie privée dont la gravité nécessite qu'elle soit exécutée sous le contrôle d'un juge'.[199] (He notes, however, that the French legislator has circumvented this by only requiring authorisation from a judge if the geo-location tracking continues after two weeks, considering that the first two weeks can be considered an extended *flagrante delicto* situation—a position contested by the Data Protection Authority (CNIL) that argues for judicial authorisation after one week instead.[200]) Also on the basis of the *Uzun* and *Jones* cases, Costanzo concludes that Italian legislation is not compatible with article 8 ECHR and that legislative intervention is needed.

[188] Marinelli 2007, p. 248. See, however, one oral-interception case in which the car was considered a place of private abode, *infra*, note 226.
[189] Bene 2014, p. 360, quoting V. Manzini, *Trattato di diritto penale italiano*, vol. VIII, 5th ed., Torino: Utet 1985, p. 851.
[190] Bene 2014, p. 360.
[191] Bene 2014, p. 352, Marinelli 2007, p. 237, Marcolini 2010, p. 2867.
[192] Marinelli 2007, p. 237; also, Marcolini 2010, p. 2867.
[193] Gentile 2010, p. 1472.
[194] Bene 2014, p. 352.
[195] Marinelli 2007, p. 236-237.
[196] Tabasco 2011, p. 166-167.
[197] E.g., Bene 2014, p. 366-367; Marinelli 2007, p. 257.
[198] Bene 2014, p. 361. Similarly Marinelli 2007, p. 256-257.
[199] Costanzo 2014, referring to French Supreme Court 22 October 2013, nos 13-81945 and 13-81949.
[200] Costanzo 2014.

Particularly interesting is the argument of several authors that location tracking affects the liberty of movement, which is safeguarded by article 16 Constitution ('Every citizen can circulate and stay freely in any part of the national territory, subject to limitations established by law in general for reasons of health or security. No restriction can be determined by political reasons'). Tabasco observes that, 'if the liberty to circulate be understood as liberty to move freely without being spied on by mechanical instruments that do not allow the person to be aware of being "followed", it is evident that the activity of satellite surveying [i.e., GPS tracking, BJK], inherent to the localisation of an individual, infringes such an inviolable right.'[201] He refers to Camon, who considers it defensible that a 'right not to be localised' should exist, as a new component of the liberty of movement.[202]

Bene also raises the question whether GPS tracking infringes article 16 Constitution, understood also as a 'right not to be localised',[203] but she does not get back to this question in her analysis of GPS tracking in relation to fundamental rights. Instead, she argues that the right to anonymity should play a role here, an argument made earlier by Gentile.[204]

Gentile, in her comment on a 2010 judgement on GPS tracking, makes the following observation:

> 'The current loosening up of social relations leads people in fact to develop parts of their private (*proprie*) activities in contact with the public, or at least outside of places of private abode. That premise implies that the persons renounce in that way their own reservedness, when the private (*propri*) thoughts or actions enter in contact with other subjects or are in any case expressed in places freely accessible to outsiders. This undeniable observation can, however, not legitimate any form of intrusion into the private sphere that could engender in the individuals the sensation of being continuously the object of control, generating doubtless prejudicial effects that evoke the so-called *panopticon* effect, inhibiting the human mind at the moment where it develops the obsession of constantly being under control.'[205]

In this context, the so-called 'right to anonymity' (*diritto all'anonimato*) has arisen, which protects people from undue and prolonged intrusions into the private individual sphere, also when they by their own choice act in public places.[206] The right to anonymity is recognised in Italy as part of the inviolable rights of the person, protected by article 2 Constitution, and protects 'situations and personal and family events from public curiosity and knowledge'.[207] It is 'ascribable to the discipline of privacy, understood in a new and more advanced form', and serves as an auxiliary for other fundamental liberties (and ultimately individual self-determination), and this can point the way to a legislative intervention with detailed norms for GPS tracking.[208]

Cell-phone location data

Traffic data can be acquired through a production order to electronic communications providers, on the basis of article 132[3] Data Protection Act, which requires a motivated order from the Public Prosecutor.[209] Traffic data will include location data associated with use of cell-phones. Such data can also be acquired through seizure of data stored with informatics, telematics, and telecommunications providers, for which article 254-bis CPC provides that the judicial authority can order that the seizure take place through a copy on an adequate data carrier, with a procedure that ensures the conformity of the acquired data to the original ones and their non-

[201] Tabasco 2011, p. 166.
[202] A. Camon (2005), 'L'acquisizione dei dati sul traffico delle communicazioni', *Rivista italiana di diritto e procedura penale* (2), p. 594-650 at p. 633, referred to in Tabasco 2011, p. 166.
[203] Bene 2015, p. 348.
[204] Bene 2015, p. 361-362 (paraphrasing the argument by Gentile 2010, p. 1472-73, without, however, mentioning the source).
[205] Gentile 2010, p. 1472.
[206] Gentile 2010, p. 1473.
[207] Italian Constitutional Court 12 April 1973, n. 38, quoted in Bene 2015, p. 362. Both Gentile and Bene refer to G. Di Paolo, 'Acquisizione dinamica dei dati relative all'ubicazione del cellulare ed altre forme di localizzazione tecnologicamente assistita. Riflessioni a margine dell'esperienza statunitense', *Cass. Pen.* 2008, p. 1219 et seq., who suggested to apply the right to anonymity to develop regulation of location tracking.
[208] Gentile 2010, p. 1473.
[209] Article 132 Data Protection Act regulates data retention, the production order, and preservation order for electronic communications service providers.

modifiability. The provider will in that case be ordered to retain and adequately protect the original data. This explicitly includes traffic data and location data (*dati di ubicazione*) (art. 254-bis).

Although acquiring traffic data requires authorization from the prosecutor, the Supreme Court has judged that absence of an authorisation does not render the results unusable, given the limited intrusion into the private sphere and given that it does not fall under the strict norms for interception.[210]

According to Marinelli, cell-phone location data (including those generated in standby mode, i.e., without the cell-phone being used for specific communications) can also be used to locate a fugitive, which constitutes an atypical means of searching for evidence since it does not fall under art. 295[3] that regulates interception of telecommunications to facilitate the investigation of a fugitive.[211]

In a fierce critique, partly based on the *Digital Rights Ireland* case that requires strong safeguards to be in place for obtaining traffic data, Dinacci argues that the regulation of location tracking through a production order of cell-phone data under current law is flawed and effectively unconstitutional, given that a mere authorization from the Public Prosecutor suffices and in light of the lack of any other safeguards in article 256 (which regulates the acquisition of documentation—the provision indicated by the Supreme Court to suffice for producing traffic data).[212] Although that critique may not be shared throughout doctrine, Dinacci offers an interesting argument for considering the constitutionality of cell-phone-based location tracking besides the secrecy and liberty to communicate. He argues that such tracking also triggers the protective sphere of the home: 'one need only think of the case in which the localisation of the position of a person through cells can help establish that that person participated in a meeting, in a specific place or dwelling, with other subjects, who are also being localised through individuating the "radio link".'[213]

The home is used to 'guard that space of freedom that the individual manifests by preserving in certain places the intimacy of his own private life, which is realised through the right to exclude third parties from view and from taking knowledge of the things that are done and said in that special setting.'[214] Under this conception, 'it appears indisputable that the possibility to "trace" the presence of persons in the home of a subject through acquiring traffic data is equivalent to rendering "visible" that which the rights-holder intended to remain confidential.'[215] Therefore, according to Dinacci, acquiring location data through a cell-phone traffic data production order infringes not only the liberty and secrecy of communication, but also the inviolability of the home, and the current regulation, which requires only a motivated decree from the prosecutor and does not otherwise provide any limitation as to when and how the power can be exercised, is not in line with the constitutional requirements.[216]

4.4. Protection from interference with identity, reputation, or honour

Several safeguards exist in criminal procedure to protect people's privacy in relation to their reputation or honour. For example, contrary to the general principle that the trial be public (art. 471), the trial, or parts thereof, can be held behind closed doors if evidence is discussed that may prejudice the privacy of a witness or civil party if it does not concern facts included in the charge (art. 472[2]). Also, for various sexual offences, part of the trial can be held behind closed doors, and this is always the case if the victim is underage; moreover, in such proceedings, questions are not allowed concerning the private life or sexuality of the victim unless these are necessary for reconstructing the facts (art. 472[3-*bis*]). Similarly, the judge can order doors to be closed when underage persons are examined (art. 472[4]).

[210] Cass., Sez. V, 10 March 2010, n. 9667, with comment by Daniela Gentile (Gentile 2010).
[211] Marinelli 2007, p. 229. He does not say in which manner the cell-phone location data are acquired by law-enforcement authorities in this context.
[212] Dinacci 2014.
[213] Dinacci 2014, p. 371.
[214] Dinacci 2014, p. 371, referring to G. Amato's commentary on art. 14 Constitution in G. Branca (ed.), *Commentario allo Costituzione*, Bologna: Zanichelli 1977, p. 66.
[215] Dinacci 2014, p. 371.
[216] Dinacci 2014, p. 392.

Other safeguards are included in article 114, which contains various prohibitions of publication. This includes publication of acts (*atti*) covered by mandatory secrecy (as per art. 329) or, if the proceedings do not reach the stage of debate, acts that may cause prejudice to witnesses or civil parties (art. 114[1],[5]); as well as publication of personal details or photographs of underage witnesses or victims until they become adults, or other information that, also indirectly, may lead to their identification (art. 114[6]). (Art. 13 Criminal Procedure Code for Minors (D.P.R. 448/1998) contains a similar prohibition for all minors involved in the proceedings, including accused minors.) Moreover, no images can be published of persons being deprived of their liberty when they are manacled or otherwise physically coerced, without their consent (art. 114[6-*bis*], introduced in 1999).

4.5. Protection for personal communications

Investigation of communications, in particular interception of telecommunications, is a highly important means of evidence gathering, with a complex set of rules and case-law, very widely discussed in the literature. It would require a report in itself to do justice to this complexity, which is not possible within the scope of the present paper. Instead, I limit the discussion here to oral interception, which contains some basic information on the regulation of telecommunications interception as well.

4.5.1. Oral interception (face to face communications)

Interception of communications is not defined in the law, but has been defined in case-law as the 'capturing, through technical registration devices, of the contents of a secret conversation or communication conducted between two or more people, when the same apprehending occurs by a subject who conceals his presence to the interlocutors'.[217] It is regulated in three forms: interception of telephone or other telecommunications (art. 266), interception of communication flows in relation to informatic or telematics systems (art. 266-*bis*), and oral interception (art. 266[2]), with specific requirements and limitations (art. 267-271).

Oral interception is usually referred to as 'interception between people present' (*intercettazione tra presenti*) or 'environmental interception' (*intercettazione ambientale*) (see also *supra*, 3.2.2 under oral interception). It can be used for investigation of the same list of crimes for which telecommunications interception is allowed—roughly, crimes with a maximum penalty of over five years' imprisonment; drugs, arms, or contraband crimes; and a number of specifically listed crimes (including, for example, threat, market manipulation, stalking, and harassing people by telephone) (art. 266[1]). Like telecommunications interception, oral interception requires authorisation, with motivated decree, from the investigatory judge, and is only allowed if there are serious indicators of the crime (*gravi indizi*) and if it is absolutely indispensable (art. 267[1]). The order can be given for at most two weeks, which can be prolonged with successive two-week periods (art. 267[3]). Results of interception that do not meet these requirements are inadmissible (art. 271[1]).

As is visible from the definition, communications interception concerns only the capturing of communications with technical devices; hence, eavesdropping behind a door is not interception.[218] The device does not have to be (purely) auditory, however: also video recordings constitute interception if they capture conversations (see *supra*, 4.3.1, note 146 and surrounding text). Also, the conversation has to be secret, that is, the interlocutors have to demonstrate the intention of keeping the conversation private; loud conversations in public can be recorded outside of the regime of art. 266 et seq.[219]

More importantly, interception occurs only if it is done by someone outside the conversation setting; hence, covert recording of communications by one of the communication partners, or by someone allowed to be present at the conversation, is not a form of interception (as regulated by art. 266 et seq.); instead, the recording is simply usable as documental evidence.[220] However, if one of the communication partners carries a bug on behalf of the police—the situation referred to as a 'secret agent equipped for sound' (*agente segreto attrezzato per il suono*)—the situation is different. Case-law distinguishes between two situations. If the agent transmits the sound directly

[217] Cass., Sez. Un. 28 May-24 September 2003, *Guida dir.* 2003, 42 at 49, quoted in Tonini 2015, p. 390.
[218] Tonini 2015, p. 390.
[219] Tonini 2015, p. 390.
[220] Tonini 2015, p. 391.

to the police (real-time or 'contextual hearing', *ascolto contestuale*), this is considered equivalent to oral interception by the police and has to conform to the same requirements (such as authorisation by the judge).[221] However, if the sound is not transmitted but 'merely' recorded, leading to a 'delayed hearing' (*ascolto differito*), this is considered by the Supreme Court to be an atypical means of gathering evidence rather than oral interception; even though the registration occurs with equipment provided by the police, the conversation is being recorded with consent of a participant to the conversation, which is considered a smaller privacy interference[222] than direct covert listening by the police themselves. Therefore, fewer legal safeguards apply and a motivated order by the Public Prosecutor suffices for 'mere registration' by a secret sound-equipped agent.[223]

For oral interception in the home, an exceptional regime applies. As observed above (4.3.1), the Code of 1988 took over the existing prohibition of auditory recordings in the home, but allowed one exception, namely when there are grounds to believe that crime takes place there (art. 266[2]). (And it should be borne in mind that this exception also has exceptions: in cases of organised crime or threat by telephone, oral interception is possible within the home without suspicion of criminal activity taking place there; see *supra*, note 99 and surrounding text.) The legal good protected by this clause—the heightened standard for allowing oral interception within the home—is not so much, or primarily, the secrecy of communications, but rather to safeguard domiciliary intimacy.[224]

Vehicles are frequently not considered to be places of private abode (one of the types of place protected by the constitutional protection of the home), at least not in case-law.[225] There is one case, however, in which the Supreme Court, in the context of placing a bug for oral interception, has considered the inside of a car to fall within the concept of a 'place of private abode', which comprises 'all those places that, besides dwelling, accomplish the function of protecting private life and that are thus destined for repose, feeding, professional occupations and leisure activities, among which will be included the driver and passenger compartment of a car used as a rule for transfers from and to a place of work and leisure.'[226]

5. The protection of things

5.1. Seizure of things, documents, and smartphones

There are three forms of seizure (*sequestro*): evidential (art. 253), preventive (art. 321) and conservative (art. 316). Given this paper's focus on evidence-gathering, I limit myself to evidential seizure (*sequestro probatorio*). This consists in securing a mobile or immobile object for evidential purposes, through forced dispossession of the object and creating a bond of non-availability on it (to prevent its modification).[227] The judiciary authority (prosecutor or judge) can, with motivated decree, order the seizure of objects of the crime (*corpora delicti*) or things relating to the crime necessary for ascertaining the facts (art. 253[1]). In cases of urgency (and if there is danger of loss or modification), the police can seize objects themselves (art. 354[2]); this has to be reported to the Public Prosecutor within 48 hours, who then has to validate, with motivated decree, the seizure within the following 48 hours (art. 355[2]).

[221] Tonini 2015, p. 407, referring to Cass., Sez. VI, 6 November 2008, *CED* 241610.
[222] Presumably because it is not a direct interference with the secrecy of the communication, but rather with the privacy expectation that the interlocutor does not (unduly) divulge the contents of the communication to others. The latter is an issue of privacy (*riservatezza*) but not of the secrecy of communications, according to Vele 2011, p. 53.
[223] Tonini 2015, p. 407, referring to Cass. Sez. II, 14 October 2010-4 January 2011 and Cass., Sez. VI, 7 April-2 June 2010, *CED* 247384.
[224] Rizzo 2012, p. 23.
[225] See, for instance, Cass. Sez. VI, 5 October 2000, *Dir. pen. proc.* 2001, p. 93, referred to in Felicioni 2012, p. 111.
[226] Cass., Sez. II, 12 March 1998, in *Riv.pen.* 1998, p. 1177, quoted in Marinelli 2007, p. 249 (who also refers to some judgements from the Constitutional Court finding, in other contexts than criminal procedure, both the driver and passenger compartment and the baggage compartment of a car to be places of private abode).
[227] Tonini 2015, p. 385.

For documents, some special provisions apply. Documents are a special means of evidence (*prova documentale*, regulated in articles 234 et seq.), consisting of writings or other documents that represent facts, persons or things through photography, video, phonography, or any other means (art. 234). Documents that constitute the object of the crime (*corpus delicti*) shall be acquired regardless of who created or keeps them (art. 235); documents originating from the accused can be acquired, including through seizure with or production by other people (art. 237). Documents containing anonymous statements cannot be acquired nor used, except if they constitute a *corpus delicti* or originate from the accused (art. 240[1]). The judiciary authority can have copies made of seized documents and the originals returned, or (if the seizure needs to be maintained) authorise to have an authentic copy made for the legitimate holders (art. 258). Note that while documents will normally be investigated for their contents, they can also be subjected to forensic material investigations (for example, to investigate whether it is counterfeit), which is a form of inspection of things (*supra*, 3.1.1) rather than investigation of seized objects.[228]

People with a right to professional or official secrecy (as stipulated in articles 200 and 201) shall hand over to the judicial authority, when so requested, all acts and documents, as well as informatic data (on adequate data carriers), except if they declare in writing that these are covered by professional, official, or state secrecy (art. 256[1]). The judicial authority can investigate the documents or data if there are reasons to doubt the classification as professional or official secret, and the document or data [carrier] can be seized if the classification proves unfounded (art. 256[2]); similarly, for state secrets as well as for acquisition of documents or acts with secret services, special procedures are foreseen (art. 256[3-4] and art. 256-*bis*, respectively). However, writings by the accused 'with the function of notes to respond to the interrogation' cannot be searched or seized, as this violates the rights of the defence.[229]

For seizure of informatic documents, the general requirements for digital forensic investigations apply (*supra*, 3.2.1). From a systematic point of view, however, it is important to realise that, as Tonini argues, in the system of law no. 48/2008, it is not the information carrier (the computer or hard disk) that is the true object of seizure, but the informatic document itself (i.e., the immaterial object). By implication, if informatic documents are secured through a forensic copy (*copia clone*) while the originally seized data carrier is returned to its owner, it is the forensic copy that is the true object of the seizure (which has, for instance, implications for requests to re-examine seized objects).[230]

For seizure and search of a smartphone incident to arrest, I am not aware of specific literature[231] or case-law. Presumably, therefore, the normal rules for search and seizure apply, in particular the norms for a personal search (*supra*, 3.1.2) in combination with those for investigating or seizing informatic documents (see previous paragraph). Particularly relevant for this type of investigation may be the proportionality principle, given that the Supreme Court has found that entire informatic devices should only be seized in exceptional circumstances, implying that indiscriminate seizure of the entire smartphone, or forensically copying all its contents, may—except in extreme cases—be readily found disproportional.[232]

6. The protection of data

There are no specific rules in the Code of Criminal Procedure for data production orders, except indirectly for certain types of data holders such as electronic communications providers (*supra*, 4.3.2 under 'Cell-phone location data') or banks (*supra*, 3.1.4). A general rule is given in article 362, which provides that the Public Prosecutor shall acquire information from persons who can report circumstances useful for investigation purposes. If the persons have already been heard by the defence attorney (on the basis of art. 391-*bis*), the same questions cannot be posed again. (art. 362). No specific safeguards apply here, except for the rules in the Data Protection Act. If personal data are collected unlawfully, leading to 'unlawful file-making' (*dossieraggio abusivo*), this falls under the prohibition of art. 167 et seq. Data Protection Act and leads to non-usability of

[228] Felicioni 2012, p. 113.
[229] Tonini 2015, p. 381-382.
[230] Tonini 2015, p. 388. See also Cass., Sez. III, no. 38148 of 21 September 2015.
[231] With the exception of a comment discussing the US *Riley* case, Carotti 2014.
[232] See Cass., no. 252223 of 12 December 2011, no. 261509 of 16 January 2013, and, in particular, no. 24176 of 10 June 2015 (information provided by my student Stefano Fantin, 10 November 2015).

the data.[233] If unlawfully collected data do not contain personal data, however, they can be used except if another statutory requirement prevents their use.[234]

For data stored with people with a right to professional or official secrecy, the regime of article 256 applies (*supra*, 5.1).

7.Conclusion

Privacy has been recognised as a full, stand-alone constitutional right under article 2 of the Italian Constitution, which guarantees the inviolable rights of the person. This general right to privacy complements the three major constitutional privacy-related rights of liberty of the person (art. 13), inviolability of the home (art. 14) and liberty and secrecy of communications (art. 15). For assessing whether and to what extent criminal investigation interferes with privacy, it is important to determine which constitutional rights are potentially affected, since the requirements for the legitimacy of interferences differ. A notable difference is that infringements of articles 13-15 require statutory limitations (and thus a specific statutory regulation), while infringements of the general right to privacy (including data protection) under article 2 do not (although they do require authorisation from a prosecutor or judge). Activities that do not substantially infringe fundamental rights or liberties can be based on the task description of the police, without further specific statutory rules or safeguards. The difference might be mitigated by article 8 ECHR, however, since its requirement of foreseeability may also necessitate investigation activities to have a sufficiently specific statutory basis.

The overview of criminal investigation powers shows, however, that Italian criminal investigation does not, in general, have very specific statutory rules to regulate privacy interferences in criminal investigation. The system of Italian criminal procedure puts more emphasis on means of evidence (and how these are admissible through debate) than on means of searching for evidence, which only includes four classic types of investigation (inspection, search, seizure, and communications interception). The general provision on atypical evidence (art. 189) therefore serves as an important stop-gap for investigation methods not specifically foreseen by the legislator, which includes a wide range of technically-facilitated investigation methods that have emerged over the past decades. The result is an under-regulation of criminal investigation powers in statutory law, which has to be compensated for by case-law, in particular of the Constitutional Court and the Supreme Court, and which leads to extensive debates in doctrine on the assessment of investigation powers in relation to privacy concerns.

On many topics, discrepancies can be observed between case-law and doctrine, although neither show particular consensus in their lines of argumentation. Courts come up with sometimes surprising, presumably pragmatic, solutions, such as the invention of 'reserved' places in the context of visual surveillance, or the distinction between real-time and delayed listening by police through sound-equipped secret agents. While doctrine sometimes shares such distinctions and solutions, authors are frequently critical of the way in which courts assess under-regulated investigation powers (for instance, in the case of GPS tracking or online covert searches), arguing that other constitutional rights are (also) at issue than the one(s) taken into account by the courts, and often calling for the legislator to intervene with specific and more detailed regulation (a call that is not easily answered in the Italian law-making context).

The notion of legal goods plays an important role in these debates. By looking at the underlying values that are to be protected under privacy-related constitutional rights, argumentations can be constructed why and to what extent certain privacy rights are triggered by an investigation method, and legal goods often provide a useful lens for making analogies with existing and more clearly regulated investigation powers—or for arguing, by contrast, why an investigation power differs from existing ones. Italian doctrine offers rich discussions of legal goods in relation to new technology-facilitated investigation powers, which is useful not only for understanding Italian law but also for comparative legal analysis.

What emerges from the doctrinal debates on the legal goods at issue in the broad domain of criminal investigation is a strong emphasis on the capacity of individuals to shield parts of their private life from others' access or cognition. The cornerstone of this capacity is the protection of

[233] Conti 2008, p. 329.
[234] Tonini 2010, p. 242.

the home, as the 'spatial projection of the person' that serves as necessary spiritual breathing space. It is characterised by exclusivity rights, both the right to admit or exclude persons and to control who can take knowledge of what pertains to the private, domestic sphere. The emphasis on access control is broader, however, than the physical space of the home; it is also visible, for instance, in the regulation of oral interception, which is based on the premise that people can reasonably expect their conversations to be secret within the circle of those allowed to access the conversation space. For situations where access or cognition by others cannot be fully controlled (which is often the case when people engage in wider social relations), the legal good of privacy as reserve, as protected by article 2 Constitution, becomes more prominent.[235]

What I find particularly interesting in Italian doctrinal debates is the emergence of new legal goods that serve to address gaps in legal protection arising from new technological affordances in criminal investigation in the context of an under-regulating Code of Criminal Procedure. The blurring of boundaries between private and public space, in the sense that behaviour and information that traditionally typically manifested themselves in private now increasingly can be noticed and acquired without physically intruding into the home, leads some authors to emphasise that new legal goods are needed. In particular, the notion of 'informatic privacy' (which is more encompassing than the notion of 'informatic home', as it not only sees to access control but also to reserve with respect to shared data) is a promising concept to address normative challenges such as the regulation of covert online searches. Such a concept demonstrates a shift in importance from secrecy or seclusion (which are privacy-related values safeguarded through access control) to reserve (as a privacy-related value safeguarded by broader mechanisms of regulating information flows), in a world where traditional public/private boundaries are increasingly difficult to draw.

At the same time, values of secrecy and seclusion remain important, and the preservation of people's capacity for access control is also advocated through doctrinal proposals for new legal goods, such as a 'right not to be localised' and an emphasis on the right to anonymity (as part of art. 2 Constitution), which protects people from undue and prolonged intrusions into the private individual sphere, also when they by their own choice act in public places. And the home remains an enduring cornerstone of privacy protection, not only through its potential to be expanded with a more encompassing, metaphorical digital space in which human personality should be able to develop and manifest itself, but also through its on-going relevance in debates on investigation methods such as location tracking.

Altogether, doctrinal debates on topical investigation methods such as covert online searches, visual observation, and location tracking demonstrate a continuous search for a solid and sustainable normative framework that allows assessing the intrusiveness of criminal investigation in a world of increasing mobility and datafication. Through proposals for new normative concepts such as informatic privacy and the right not to be localised, in combination with strengthened attention for the right to anonymity, Italian doctrine seeks to help protect the overall, underlying value that people should be able to develop and manifest their personality without undue constraints, which is ultimately what privacy protection seeks to achieve.

Literature

Aprile, Ercole & Filippo Spiezia (2004), *Le intercettazioni telefoniche ed ambientali. Innovazioni tecnologiche e nuove questioni giuridiche*, Milano: Giuffrè.

Bene, Teresa (2014), 'Il pedinamento elettronico: truismi e problemi spinosi', in: Adolfo Scalfati (ed.), *Le indagini atipiche*, Torino: Giappichelli Editore, p. 347-367.

Bonetti, Michele (2003), *Riservatezza e processo penale*, Milano: Giuffrè editore.

Camon, Alberto (1999), 'Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove "incostituzionali"', *Cass. pen.* (4), p. 1188 et seq.

Carotti, Bruno (2014), 'Una pronuncia della Corte Suprema su *privacy* e nuove tecnologie', *Rivista trimestrale di diritto pubblico* (3), p. 869-873.

Chiavario, Mario (2012), *Diritto processuale penale. Profilo istituzionale*, 5th ed., Milanofiori Assago: Wolters Kluwer Italia.

[235] Cf. the two-prong approach to privacy as access control plus protection against further spreading of lawfully acquired information that is visible in Italian substantive criminal law, see Koops 2016, section 6.

Conso, Giovanni, Vittorio Grevi & Marta Bargis (2014), *Compendio di procedura penale*, 7th ed., s.l.: Wolters Kluwer Italia/CEDAM.
Conti, Carlotta (2008), 'Inutilizzabilità', in: G. Spangher (ed.), *Procedura penale* (Dizionari sistematici), Milano: Il Sole 24 Ore, p. 325-330.
Costanzo, Pasquale (2014), 'Note preliminari sullo statuto giuridico della geolocalizzazione (a margine di recenti sviluppi giurisprudenziali e legislativi), *Diritto dell'Informazione e dell'Informatica* (3), p. 331-344.
Dinacci, Filippo Raffaele (2014), 'Localizzazione attraverso celle telefoniche', in: Adolfo Scalfati (ed.), *Le indagini atipiche*, Torino: Giappichelli Editore, p. 369-393.
Dinacci, Filippo Raffaele (2015), 'Le regole generali delle prove', in: G. Spangher (ed.), *Procedura penale. Teoria e pratica del processo, Vol. I. Soggetti, Atti, Prove*, Milanofiori Assago: Wolters Kluwer Italia, p. 757-824.
Felicioni, Paola (2012), *Le ispezioni e le perquisizioni*, 2nd ed., Milano: Giuffrè editore.
Gaeta, Piero (2015), 'Il pubblico ministero e la polizia giudiziaria', in: G. Spangher (ed.), *Procedura penale. Teoria e pratica del processo, Vol. I. Soggetti, Atti, Prove*, Milanofiori Assago: Wolters Kluwer Italia, p. 141-261.
Gaito, Alfredo (ed.) (2012), *Codice di procedura penale commentato. Artt. 1-369bis*, 4th ed., Milanofiori Assago: Wolters Kluwer Italia.
Gentile, Daniela (2010), '*Tracking* satellitare mediante gps: attività atipica di indagine o intercettazione di dati?', *Diritto penale e processo* (12), p. 1464-73.
Iovene, Federica (2014), 'Le c.d. perquisizioni *online* tra nuovi diritti fondamentali ed esigenze di accertamento penale', *Diritto penale contemporaneo* (3-4), p. 329-342.
Koops, Bert-Jaap (2016), *Privacy-related crimes in Italian law*, Working paper, version 1.0 (December 2016), https://ssrn.com/abstract=2877668.
Lasagni, Giulia (2016), 'L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti"', *Diritto penale contemporaneo*, 7 October 2016, http://www.penalecontemporaneo.it/d/4995-luso-di-captatori-informatici-trojans-nelle-intercettazioni-fra-presenti (accessed 14 November 2016).
Mantovani, Ferrando (2013), *Diritto penale. Parte speciale I. Delitti contro la persona*, s.l.: CEDAM.
Marcolini, Stefano (2010), 'Le cosiddette perquisizioni *on line* (o perquisizioni elettroniche)', Cassazione penale (7/8), p. 2855-2868.
Marinelli, Claudio (2007), *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Torino: Giappichelli Editore.
Morlacchini, F. (2015), 'Ispezione, perquisizione e sequestro', in: G. Spangher (ed.), *Procedura penale. Teoria e pratica del processo, Vol. I. Soggetti, Atti, Prove*, Milanofiori Assago: Wolters Kluwer Italia, p. 1140-1202.
Rizzo, Corrado (2012), *Lo strumento investigativo delle riprese visive*, Torino: Giappichelli Editore.
Tabasco, Giuseppe (2011), *Prove non disciplinate dalla legge nel processo penale. Le 'prove atipiche' tra teoria e prassi*, Napoli/Roma: Edizioni Scientifiche Italiane.
Tonini, Paolo (2010), *Diritto processuale penale. Manuale breve*, Milano: Giuffrè Editore.
Tonini, Paolo (2015), *Manuale di procedura penale*, 16th ed., Milano: Giuffrè Editore.
Torre, Marco (2015), 'Mezzi di ricerca della prova informatica e garanzie difensive: dagli accertamenti investigativi al virus di Stato. Le indagini atipiche – Perquisizioni *on line* e captatore informatico nel diritto vivente', presentation 15 July 2015, available at http://www.fondazioneforensefirenze.it/uploads/fff/files/2015/2015.II/2015.07.15%20Mezzi%20ricerca%20prova%20informatica/Slides%20Dott_%20Marco%20Torre.pdf (accessed 14 November 2016).
Trogu, Mauro (2014), 'Sorveglianza e "perquisizioni" *on-line* su materiale informatico', in: Adolfo Scalfati (ed.), *Le indagini atipiche*, Torino: Giappichelli Editore, p. 431-456.
Vaciago, Giuseppe & David Silva Ramalho (2016), 'Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings', 13 *Digital Evidence and Electronic Signature Law Review*, p. 88-96.