Diego Zannoni[*]

GPS Surveillance from the Perspective of the European Convention on Human Rights

Abstract

GPS surveillance as an investigation technique and the use of the data collected by this means as evidence in criminal proceedings raises a number of issues relating to the potential violation of the European Convention on Human Rights. One could argue that States are entitled to protect themselves against the exacerbation of criminality and terrorism. However, there should be clear limitations to the investigation techniques States use for such purposes and to the way in which the evidence collected are used in criminal proceedings. With reference to GPS surveillance, this article attempts to strike the delicate balance between a need for proactive and effective investigations on the one hand and the right of individuals to respect for their own private life and their defensive rights in criminal trials on the other.

1. Introduction

GPS surveillance is increasingly used as an investigation technique. Since geolocation data contains both spatial and temporal information, it permits the identification of the exact position of objects on earth. The advantages it offers in comparison to traditional visual surveillance are obvious: greater precision in monitoring and an effective concealment of the operators[1]. On the other hand, the use of GPS surveillance as a technique of investigation and of the data collected by this means as evidence in criminal proceedings raises several issues relating to the potential violation of the European Convention on Human Rights[2].

* Phd Doctor in international law and European Union law (University of Padova); Postdoctoral Fellow (McGill University, Montreal).The author currently is a researcher at the University of Padova.

1 For a comparison between GPS and visual surveillance see *infra* par. 5.

2 "Special investigation techniques", including GPS surveillance, are defined by the Recommendation of the Committee of Ministers of the Council of Europe as "techniques applied by the competent authorities in the context of criminal investigations for the purpose of detecting and investigating serious crimes and suspects, aiming at gathering information in such a way as not to alert the target person". Recommendation Rec (2005)10 of the Committee of Ministers to Member States on "special investigation techniques" in relation to serious crimes including

DOI: 10.5771/2193-5505-2018-2-294

While a prudent legislator should be concerned with constantly updating the applicable legislation as technology develops, the growing role of special investigation techniques has so far rarely been followed by timely updates of domestic legislation[3]. As a result, domestic and international courts have been called upon to play a 'role of substitution'[4] on several occasions and to strike the delicate balance between a need for proactive and effective investigations on the one hand, and the right of individuals to respect for their own private life and their defensive rights in criminal trials on the other.

One could argue that States are entitled to protect themselves against the exacerbation of criminality and terrorism. However, there should be clear limitations to the investigation techniques States can use for such purposes and to the way in which the evidence collected is used in criminal proceedings. Claiming otherwise would mean subscribing to the classic inquisitorial view that the end justifies the means.

As far as GPS surveillance is concerned, there are two distinct phases to be analysed: 1) the investigation taking place before the trial and 2) the trial itself and, in particular, the legal regime which applies to evidence. There are also differences in the law applying to these two phases. In Italy, for example, satellite tracking as an investigative activity is not expressly provided for by the law, which has triggered discussions in the literature as to whether Article 189 of the Code of Criminal Procedure regulating atypical evidence may be applicable to it[5]. Such a distinction is relevant because the findings collected during pre-trial investigations cannot always be used by judges as evidence for the purposes of reaching a final verdict. The procedural law of each State establishes whether this is possible and under what modalities[6]. The Council of Europe recom-

acts of terrorism, 20 April 2005. The covert or secret nature of the technique is however not generally considered as sufficient for it to qualify as a "special investigation technique", since there must be an additional element of deception, disguise, cunning and subterfuge. Concurring opinion of judge Pinto de Albuquerque in Lagutin and others v. Russia, Applications nos. 6228/09, 19123/09, 19678/07, 52340/08 and 7451/09, 24 April 2014, footnote n. 1.

3 The development of the Internet, for example, posed a number of legal challenges and prompted the verification of whether and to what extent "the same rights that people have off line must also be protected online" according to the expression used by the Human Rights Council. See Human Rights Council, resolution L.13 The Promotion, Protection and Enjoyment of Human Rights on the Internet, 29 June 2012. For an overview on the right to respect for one's private life on the Internet see M. Carta, *Diritto alla vita privata ed internet nell'esperienza giuridica europea ed internazionale*, in Diritto dell'informazione e dell'informatica, 1/2014, pp. 1-19.

4 A. Serrani, *Sorveglianza satellitare GPS: un'attività investigativa ancora in cerca di garanzie*, in Archivio penale, 2013, p. 2.

5 This is part of the broader issue of the possible application of the norms regulating atypical evidence to atypical investigation techniques. S. Signorato, *La localizzazione satellitare nel sistema degli atti investigativi*, Rivista italiana di diritto e procedura penale, 2012, pp. 589-594; M. Stramaglia, *Il pedinamento satellitare: ricerca ed uso di una prova "atipica"*, Diritto penale e processo, 2/2011, pp. 215-216. See *infra* par. 4.

6 For an overview of the Italian legal framework see D. Gentile, *Tracking satellitare mediante GPS: attività atipica di indagine o intercettazione di dati?*, Diritto penale e processo, 12/2010, p. 1470-1471.

mends Member States to "take appropriate legislative measures to permit the production of evidence gained from the use of special investigation techniques before courts". However, it adds that "procedural rules governing the production and admissibility of such evidence shall safeguard the rights of the accused to a fair trial"[7].

Given that geolocation information is obtained from radio navigation satellites[8] and the fact that international treaties and resolutions applying to outer space do not contain any specific reference to the use of GPS data for investigative purposes, the legal literature which so far has dealt with the issue has suggested an amendment to the current space law framework[9]. However, these proposals do not appear to be very persuasive. Firstly – but this is a merely factual consideration – because of the low likelihood of them being endorsed. The United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS) established in 1958 to develop and codify international norms governing the exploration and use of outer space[10], has gradually lost its initial impetus. This already became evident in the controversial adoption of the 1979 Moon Agreement, which attempted to establish an international regime for the exploitation of mineral resources of the moon and other celestial bodies and was opposed by the major space powers[11]. Since the adoption of the Moon Agreement, the law-making process for outer space activities has slowed down and UNCOPUOS has only adopted non-binding guidelines.

Apart from that, the upstream applicability of these proposals is doubtful given the technicality of radio navigation. The GPS signal is broadcast by satellites, but this is only the first stage of the process. A receiver on earth picks up and decodes the signal in order to provide the position information required. The activity is, therefore, only at the beginning a space activity and continues on earth. The admissibility and use of data obtained in this way in court proceedings is a 'terrestrial' issue and does as such not pertain to the law applicable to space activities.

7 Recommendation Rec 2005(10), *op.cit*., par. 7.

8 The satellite systems currently in operation are the American Global Positioning System (GPS), the Russian Global Orbiting Navigation Satellite System (GLONASS) and now also the European Galileo. As for the terminology, regardless of the constellation to which the satellites sending signals belong, the commonly used term is GPS, derived from the name of the first constellation in operation.

9 R. Purdy, *Pulling the Threads Together and Moving Forward*, in R. Purdy, D. Leung (Eds.), Evidence from Earth Observation Satellites: Emerging Legal Issues, Leiden, 2012, pp. 417-418; A. Vettorel, *Global Positioning System Evidence in Court Proceedings and Privacy: The Case of Italy*, Air and Space Law, 2017, pp. 311-312; C. Candelmo, V. Nardone, *Satellite Evidence in Human Rights Cases: Merits and Shortcomings*, Peace Human Rights Governance, vol. 1, issue 1, 2017, p. 92; 109.

10 UNCOPUOS was established as an *ad hoc* committee by means of UNGA Resolution 1348 (XIII), Question of the Peaceful Use of Outer Space, adopted on 13 December 1958, and became then permanent with UNGA Resolution 1472 (XIV), International Co-operation in the Peaceful Uses of Outer Space, adopted on 12 December 1959.

11 Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, opened for signature in New York, 18 December 1979; 18 ILM 1434, 1363 UNTS 3, entered into force 11 July 1984.

The objective of this article is to assess the legitimacy of GPS surveillance as an investigation technique from the perspective of the European Convention on Human Rights and to clarify the limits within which GPS data may be used as evidence in court proceedings. Taking the principle of proportionality as a guiding principle, a comparison of GPS surveillance with other investigation techniques, namely interception of telecommunications and visual surveillance, is developed. The right to respect for private life is used in order to outline which limits regarding the fundamental rights of the individual are currently being exceeded during trials – but also before trials and outside the courtroom – due to the challenges posed by an increasing demand for security[12].

2. *GPS surveillance and respect for private life*

GPS trackers are devices which determine the precise location of vehicles or objects on which they are installed. Their basic function is, therefore, to monitor movements of objects. However, this satellite tracking technique is often combined with further investigation activities (such as visual surveillance), permitting the identification of the passengers on the vehicle or who use the monitored object, thus linking the movements of vehicles or objects to the movements of persons[13].

GPS surveillance is an investigation technique which presupposes that the monitored person is unaware of its use, because its effectiveness depends on the secrecy of the operations and on the surprise effect. This raises the first issue to be dealt with in this article, i.e. whether the use of satellite localization in investigations interferes with the right to respect for private life of the monitored person and, if so, what conditions must be met for such an interference to be considered as lawful.

According to the well-established case law of the European Court of Human Rights (ECtHR), "private life" is a broad term which cannot be comprehensively defined. Departing from the original notion of the right to respect for private life as a right to no third-party interference with the intimacy of one's private and family life and a right to identity and development of the individual, the ECtHR ended up defining it as a right to establish and develop relationships with other human beings and with the outside world and as a right to self-determination in relation to all the areas in which one's personality is expressed. The definition, therefore, includes an element of inter-

12 A. Gaito, S. Furfaro, *Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in E.M. Amborsetti (Ed.) Studi in onore di Mauro Ronco, Torino, 2017, p. 555.

13 The ECtHR specified that "Il existe deux méthodes pour y procéder: d'une part, le suivi dynamique d'un terminal de télécommunication, avec l'exploitation de la technologie propre d'un téléphone, d'une tablette ou d'un véhicule équipé d'un système GPS; d'autre part, un dispositif matériel directement installé sur un moyen de transport ou un autre objet, à l'instar d'une balise". Requête no 31446/12 Mohamed Ben Faiza c. la France, introduite le 22 mai 2012, arrêt du 8 février 2018, par. 53.

action between individuals and others, even in a public context, which may fall within the concept of "private life"[14].

The notion was subsequently further extended to include the right to control the terms and conditions based on which personal information is collected, stored and processed – in other words: the right to self-determination in the sphere of information (*Recht auf informationelle Selbstbestimmung*)[15]. The ECtHR has defined a limit beyond which an interference with a person's private life occurs: the systematic collection and storing of data relating to the private life of an individual, even without the use of covert surveillance methods[16], and even if the monitored activity to which the data refer has no intimate nature and is carried out in a public place[17].

Indeed, from the point of view of the right to respect for private life, there is no difference between the interception of telephone communications, which by its nature is not public, and the covert surveillance of any other human behaviour, which, wherever it may take place, the concerned person does not want to become public. As obvious as it may seem, this observation is crucial, because it involves the need to shift the focus from places, which are normally considered as the element qualifying for protection, to persons, who, as a centre of subjective imputation in different life situations, wish for their activities not to become public. In other words, being a person in a public place does not *tout court* imply that an individual renounces their privacy[18]. The subsequent use of the information stored has no bearing on that finding[19].

Since GPS surveillance is an investigation technique consisting in the systematic collection and storing of data determining individual movements[20], it can be considered

14 Peck v. The United Kingdom, Application no. 44647/98, 28 January 2003, par. 57.

15 Differently from the ECHR, the Charter of Fundamental Rights of the European Union provides for the protection of personal data as an independent and distinct right from the right to respect for one's private life (Articles 7 and 8). Since the protection of personal data has its roots in fundamental values, which are positivized in both conventional instruments, it seems possible to exclude for both that the consent of the person the data refer to may enable any use thereof, particularly when this is in contrast with the respect for the human dignity of the person concerned. See also M. Carta, *op.cit*., pp. 18-19.

16 Uzun v. Germany, Application no. 35623/05, 2 September 2010, par. 46 and case law cited therein.

17 Rotaru v. Romania, Application no. 28341/95, 4 May 2000, par. 43; P.G. and J.H. v. The United Kingdom, Application n. 44787/98, 25 September 2001, paras. 56-57; Peck v. The United Kingdom, *op.cit*., paras. 57; 59; 62-63; Perry v. The United Kingdom, Application no. 63737/00, 17 July 2003, paras. 36-38; Uzun v. Germany, *op.cit*., par. 43.

18 The American doctrine uses the expression "right to public anonymity" which "provides assurance that, when in public, one will remain nameless-unremarked, part of the undifferentiated crowd – as far as the government is concerned". C. Slobogin, *Public Privacy: Camera Surveillance of Public Spaces and the Right to Anonymity*, Mississippi Law Journal, vol. 72, 2002, p. 213.

19 Kopp v. Switzerland, 13/1997/797/1000, 25 March 1998, par. 53; Amann v. Switzerland, Application no. 27798/95, 16 February 2000, par. 69.

20 Uzun v. Germany, *op.cit*., par. 51.

an interference with one's right to private life in the context of the above[21]. The same applies to the collection and storing of data on a person's movements using the information provided by nearby cell towers indicating a cellphone's approximate location (cell site location information)[22].

The protection of the right to private life in the context of GPS surveillance was at the very core of two ECtHR judgments: *Uzun v. Germany* and the more recent *Ben Faiza v. France*. The first leading case originated with the application filed against Germany by a German national who was suspected of participation in offenses committed by an extremist terrorist movement. The applicant alleged that the observation via GPS he had been subjected to – both as a standalone measure and, in any case, because of its aggregation with further measures of surveillance ordered – and the use of the data obtained by this means in the criminal proceedings against him, had violated the right to respect for his private life under Article 8 and his right to a fair trial enshrined in Article 6 of the ECHR[23]. The ECtHR was once again called upon in the case of *Ben Faiza v. France* to rule on the potential infringement of the right to respect for private life by a surveillance measure via GPS. However, the factual background of this case was considerably different from that of *Uzun v. Germany*. Indeed, in *Ben Faiza v. France*, the applicant was prosecuted by national authorities not for a terrorist crime, but for drug trafficking.

3. GPS surveillance and interception of telecommunications: a double-standard regime

Article 8 (2) ECHR permits an interference with the right to respect for one's private life by a public authority on the condition that such interference is "in accordance with the law and is necessary in a democratic society". From the perspective of the Strasbourg Court, the impugned measure shall have some basis in domestic law in order to be "in accordance with the law" within the meaning of Article 8 (2). More substantially, this means that the law must be accessible to the person concerned, who must be able to foresee its consequences for them[24]. From the object and purpose of Article 8, it follows that "in accordance with the law" also relates to the quality of the law, i.e. its compatibility with the "rule of law", which is expressly mentioned in the preamble to

21 Uzun v. Germany, *op.cit*., par. 52; Ben Faiza v. France, *op.cit*., par. 54-55. In this regard A. Serrani uses the expression "diritto a non essere localizzati" [right not to be geolocalised], as included in the right to respect for private life. A. Serrani, *op.cit*., p. 10.

22 Ben Faiza v. France, *op.cit*., paras. 66-68.

23 Uzun v. Germany, *op.cit*., par. 3.

24 "A norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail". Sunday Times v. The United Kingdom, Application no. 6538/74, 26 April 1979, par. 49.

the Convention. This implies that domestic law must provide for adequate protection against arbitrary interference with the safeguarded rights by public authorities [25].

It must be noted that GPS monitoring as an investigation technique is not expressly regulated in all Member States. However, the Court of Strasbourg, which deals with different legal traditions, has developed a rather elastic concept of "law", according to which prevalence is given to substance over form. In fact, the ECtHR has always understood the term as including both enactments of a lower rank than statutes and unwritten law[26]. Moreover, even where the relevant norm exists in writing, the notion of "law" includes not only the normative text in force, but also the interpretation given by the jurisprudence[27]. This is also true for the rules of criminal liability, provided that the jurisprudential interpretation clarifying the text of the rule is consistent with the essence of the offense and reasonably foreseeable[28].

As far as the requirement of foreseeability is concerned, this cannot mean that an individual should be enabled to foresee *in concreto* when the authorities are likely to intercept their communications or track their movements, so that they can adapt their conduct accordingly. As mentioned above, special investigation techniques require the monitored person to be unaware of them in order to be effective. Instead, this requirement means that the law must be sufficiently clear in its wording to give citizens an adequate indication as to the circumstances and conditions public authorities are empowered to resort to these secret and potentially dangerous interferences with their rights to private life and correspondence[29].

The ECtHR appears to interpret the "in accordance with the law" requirement flexibly, depending on the level of interference with the right to respect for one's private life, by the specific investigation technique used, thus effectively applying a double standard. In essence, the "in accordance with the law" requirement is given a "stronger" significance when methods of visual or acoustic surveillance such as tele-

25 The Court highlighted that the protection afforded by Article 8 would be "unacceptably weakened" if the use of modern surveillance techniques in the criminal justice system were allowed "at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private life interests". S. and Marper v. The United Kingdom, Applications nos. 30562/04 and 30566/04, 4 December 2008, par. 112; Kruslin v. France, Application no. 11801/85, 24 April 1990, par. 27; Lambert v. France, Application n. 88/1997/872/1084, 24 August 1998, par. 23; and Perry v. The United Kingdom, Application no. 63737/00, 17 July 2003, par. 45; Roman Zakharov v. Russia, Application no. 47143/06, 4 December 2015, paras. 302-303.

26 Kruslin v. France, *op.cit*., par. 29; Huvig v. France, Application no. 11105/84, 24 April 1990, par. 35.

27 Ben Faiza v. France, *op.cit*., par. 56 and case law cited therein.

28 Such principles, developed by the ECtHR under Art. 7 ECHR (cf. S.W. v. The United Kingdom, 22 November 1995, par. 36, Streletz, Kessler and Krenz v. Germany, 22 March 2011, par. 50), were explicitly expanded upon by the ECtHR in the Uzun v. Germany case related to Art. 8 ECHR.

29 Malone v. The United Kingdom, Application no. 8691/79, 2 August 1984, par. 67; Kruslin v. France, *op.cit*., par. 30; Huvig v. France, *op.cit*., par. 29; Weber and Saravia v. Germany, Application no. 54934/00, 29 June 2006, par. 93. Cf. R. Bobbio, *Democrazia e segreto*, Torino, 2011, p. 44.

phone tapping are used, which have a more direct impact on a person's right to private life. By contrast, it is attributed a "weaker" significance when referring to investigation techniques which, in the words of the ECtHR, "interfere less" with a person's private life[30]. According to the ECtHR, satellite monitoring should fall within this second category, since it can only detect a person's position [31].

The difference between the two categories seems nonetheless one of nature or substance rather than degree or intensity of interference, as the reasoning of the ECtHR might suggest[32]. As mentioned above, GPS tracking monitors the location of the object the GPS tracker is installed in and, as a consequence, of a person, without any interception and record of conversations or images of opinions or feelings[33]. This rules out that geolocation falls within the *genus* of the interception of telecommunications and that the strict standards set up and applied in that specific context by the ECtHR are applicable to GPS surveillance of movements in public places.

In the case of interception of telecommunications, the law must be particularly precise in its terms to give citizens an adequate indication of the conditions and circumstances in which authorities are empowered to resort to this secret and potentially dangerous interference with the right to private life and correspondence[34]. The ECtHR indeed requires that the law specifies the nature of the offences leading to an interception order; a definition of the categories of people liable to have their communications monitored; a limit on the duration of such monitoring; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which the data obtained may or must be erased or the records destroyed, in particular where the accused has been discharged by an investigating judge or acquitted by a court[35].

30 Uzun v. Germany, *op.cit*., par. 66; Ben Faiza c. France, *op.cit*., par. 53.

31 Uzun v. Germany, *op.cit*., par. 66.

32 It has been argued that there is also a purely technical difference between the two investigation techniques. They both intercept what is technically defined as a signal, but while the interception of telecommunications acquires a reserved signal intended for the exclusive use of the intercepted person, GPS tracking captures a signal anybody in the world is free to use: in fact, any satellite tracker uses the same signal in order to obtain its own coordinates. S. Signorato, *op.cit*., p. 584; M. Stramaglia, *op.cit*., p. 214; T. Bene, *Il pedinamento elettronico: truismi e problemi spinosi*, in A. Scalfati (Ed.), Le indagini atipiche, Torino, 2014, p. 350. This assumption as such cannot be shared. While it is true that the signal sent by the satellite is available to all, this is not necessarily the case for the signal sent by the GPS tracker.

33 Ben Faiza c. France, *op.cit*., par. 53.

34 The ECtHR has ruled that information relating to the date and length of telephone conversations, and in particular the numbers dialled, constitutes an "integral element of the communications made by telephone". Malone v. The United Kingdom, Application no. 8691/79, 2 August 1984, par. 84; Copland v. The United Kingdom, Application no. 62617/00, 3 April 2007, par. 43. Simultaneously, such information is by its very nature to be distinguished from the interception of communications. P.G. and J.H. v. The United Kingdom, Application no. 44787/98, 5 September 2001, par. 42; Ben Faiza v. France, *op.cit.*, par. 66.

35 Malone v. The United Kingdom, *op.cit*., par. 68; Valenzuela Contreras v. Spain, 58/1997/842/1048, 30 July 1998, par. 46; Weber and Saravia v. Germany, *op.cit*., par. 95 and further references; The Association For European Integration and Human Rights and

Even if the interception of telecommunications is legitimate because it is taking place in accordance with the law and deemed necessary for the protection of a democratic society, the storing of personal data can only be accepted for a limited and appropriate period of time provided for by the law. This clearly implies an assessment in terms of necessity and proportionality of the duration of data retention, taking into account the purposes for which the data is stored and preserved and the gravity of the underlying offenses[36]. These principles led the ECtHR to believe that there is no violation of Article 8 when the seriousness of the crime justifies the long-term storage of personal data in a database for 30 years, for example in the case of rape and sexual assault of a minor under 15 years of age committed by a person in a position of authority[37]. In another case, it considered that the retention in the national fingerprint database of the fingerprints of a French citizen who was suspected but not convicted of having stolen some books was a disproportionate interference with the applicant's private life[38].

On the other hand, according to the ECtHR, a lower level of guarantees is sufficient for GPS monitoring, i.e. a legal basis, even a generic one, which is accompanied by the provision of adequate and effective protection against arbitrariness, depending on the circumstances of the case[39]. Thus, in the case of GPS surveillance, a "simplified lawfulness test" applies[40], and the scope of the margin of appreciation of Member States consistently increases[41]. This is, of course, without prejudice to the discretion of national legislators to extend the strict standards required by the ECtHR for the surveillance of telecommunications to GPS monitoring and thereby strengthen the guarantees provided for the latter[42].

4. The significance of "in accordance with the law" for GPS surveillance

The provisions of the German Code of Criminal Procedure challenged in the *Uzun v. Germany* case permitted that, without the knowledge of the person concerned, "a) photographs may be taken and visual recordings be made, b) *other special technical*

Ekimdzhiev v. Bulgaria, Application no. 62540/00, 28 June 2007, paras. 75-77; Bykov v. Russia, Application no. 4378/02, 10 March 2009, par. 76; Kennedy v. The United Kingdom, Application no. 26839/05,18 May 2010, par. 152 (where the relevant part of the Weber and Saravia judgement is quoted in full).

36 M.K v. France, Application no. 19522/09, 18 April 2013, par. 32.

37 Gardel v. France, Application no. 16428/05, 17 December 2009, par. 69.

38 M.K v. France, *op.cit*., par. 43.

39 Uzun v. Germania, *op.cit*., paras. 63-66. In the case of GPS surveillance, for instance, it is not mandatory for national legislation to indicate the circumstances in which GPS data shall be erased or destroyed. Cf. A. Galetta, P. De Hert, *Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance*, Utrecht Law Review, 2014, p. 61.

40 A. Galetta, P. De Hert, *op.cit*., p. 61.

41 Leander v. Sweden, Application no. 9248/81, 26 March 1987, par. 59; Peck v. The United Kingdom, *op.cit*., par. 77.

42 A. Serrani argues that the preferable legislative option is to extend the guarantees provided for the interception of telecommunications to GPS tracking. A. Serrani, *op.cit*., p. 12.

means intended for the purpose of surveillance may be used to investigate the facts of the case or to detect the perpetrator's whereabouts if the investigation concerns a criminal offence of considerable gravity and if other means of investigating the facts of the case or of detecting the perpetrator's whereabouts had less prospect of success or were more difficult"[43]. According to the ECtHR, the open clause "other special technical means" made the use of GPS foreseeable, although this was not expressly mentioned[44]. The reasoning which led to and supported this conclusion was that "in any system of law, including criminal law, however clearly drafted a legal provision may be, there is an inevitable element of judicial interpretation. There will always be a need for elucidation of doubtful points and for adaptation to changing circumstances". It is proved by the fact that "in the Convention States, the progressive development of the criminal law through judicial law-making is a well entrenched and necessary part of legal tradition"[45]. Thus, according to the ECtHR, the finding of the domestic court was a reasonably foreseeable development and clarification of the relevant provision[46]. Under these terms, however, the ECtHR ends up stating the obvious and does not seem to focus on the real issue at stake. The wording of the German norm was apparently drafted in such a way that it easily and certainly covered GPS surveillance. The real point to clarify, however, was to determine whether each technique of investigation should or should not be *explicitly* contemplated by the law in order for the foreseeability requirement to be satisfied. This is implicitly excluded by the ECtHR. Given the steady evolution of social reality and the constant technical-scientific progress, specific provisions for all investigation techniques in the law would frustrate investigative needs. Thus, if an investigation technique cannot be brought into accordance with an investigation technique provided for by the law through interpretation, this does not necessarily mean that it is *contra legem.* Moreover, although general, the German provision was not generic in the sense that, in order to use those "other special technical means", it intended for specific requirements to be met – "strict standards" in the ECtHR's view[47]. The use of these techniques is only permitted 1) for offences of considerable gravity and 2) if other means of investigating the facts of the case or of detecting the perpetrator's whereabouts had less prospect of success or were more difficult.

In the *Ben Faiza v. France* case, the French provision challenged as a possible legal basis for GPS surveillance was Article 81 of the Code of Criminal Procedure which states that "le juge d'instruction procède, conformément à la loi, à tous les actes d'information qu'il juge utiles à la manifestation de la vérité. Il instruit à charge et à décharge". In contrast to the German norm, the French provision merely refers to "actes d'information qu'il juge utiles à la manifestation de la vérité" in general and generic terms. Consequently, according to the ECtHR, it neither satisfied the "foreseeability" required by Article 8 ECHR, nor included adequate and sufficient guarantees

43 The norm was Article 100 (c) par. 1 n. 1 of the Code of Criminal Procedure.
44 Uzun v. Germany, *op.cit*, par. 68.
45 *Ibidem*, par. 62.
46 *Ibidem*, par. 68.
47 *Ibidem*, par. 70.

against abuse[48]. Moreover, the ECtHR pointed out that, before the adoption of the *loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation*, the French Council of Ministers had admitted that "Le projet de loi vise à donner un fondement législatif strict à des pratiques qui, jusqu'alors, en étaient *dépourvu*, et reposaient sur des dispositions très générales du code de procédure pénale"[49].

In fact, as far as the requirement of the existence of adequate and effective guarantees against abuse is concerned[50], the laws so far adopted by ECHR States Parties are very different in content. The French Supreme Court affirmed in two judgements issued when there was no specific legislation on GPS in France that "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", while a mere authorization from a public prosecutor was deemed insufficient in the light of Article 8 ECHR[51]. The French legislator then took action through the adoption of the *loi relative à la géolocalisation*, permitting public prosecutors to issue authorizations for GPS surveillance for up to fifteen days[52]. In Italy, the Court of Cassation has instead remarked that, for the use of GPS in investigations, not even an order by the public prosecutor is required[53].

From among the alternatives of the order being issued by an impartial judge or by a public prosecutor, as it was in the *Uzun v. Germany* case, Judge Pinto de Albuquerque opted for the former, arguing that it can be assumed that there is an international consensus as to the minimum content of human rights-compatible legislation on special investigation techniques. Indeed, he included the "use of Global Positioning System (GPS) satellite-guided positioning systems" among the special investigation techniques for which a judicial authorization and regular reviews are needed[54]. He also added that, only in cases of urgency, an authorization may be issued by a public prosecutor on the

48 Ben Faiza v. France, *op.cit*., par. 59.

49 Emphasis added, Ben Faiza v. France, *op.cit*., par. 61.

50 "The Contracting States [do not] enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not […] adopt whatever measures they deem appropriate". Klass and others v. Germany, Application no. 5029/71, 6 September 1978, par. 49. The Court underlines that, whatever system of surveillance is adopted, there shall exist adequate and effective guarantees against abuse. *Ibidem*, par. 50; Malone v. The United Kingdom, *op.cit*., par. 81.

51 Cour de cassation, 22 October 2013, 13-81.949; 13-81945.

52 Loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation.

53 See Cass. Pen. Sez. V, 27 February 2002, n. 16.130; Cass. Pen. Sez. V, 7 May 2004, n. 24.715; Cass. Pen. Sez III, 2 December 2008, n. 47.460; Cass. Pen. Sez. V, 15 December 2009, n. 9.667; Cass. Pen., Sez. II, 21 May 2013, n. 21.644; Cass. Pen., Sez. V, 21 March 2017, n. 13.822. For an overview of the Italian legislation and case law, see P. Costanzo, *Note preliminari sullo statuto giuridico della geolocalizzazione (a margine di recenti sviluppi giurisprudenziali e legislativi)*, Il Diritto dell'informazione e dell'informatica, 2014, pp. 341-344.

54 Concurring opinion of judge Pinto de Albuquerque in Lagutin and others v. Russia, *op.cit.*, par. 2; paras. 8.1; 8.1.8.

condition that it is subsequently confirmed by a judge in a prompt manner[55]. If such reasoning was to be adopted, Italian law would be incompatible with the ECHR.

By contrast, in the *Uzun v. Germany* case, the Strasbourg Court took the view that an order by a public prosecutor was sufficient for GPS surveillance to satisfy the level of guarantees required by Article 8 ECHR. The ECtHR issued no further statement as to whether such an order was necessary as a minimum guarantee. This issue was not relevant – and was not dealt with – in the subsequent judgment *Ben Faiza v. France* where GPS surveillance was ordered by a judge (*le juge d'instruction*)[56].

The position of the European Court may seem a step back in respect to the position adopted by the French Supreme Court in the two judgements outlined above. It is, however, consistent with its case law, according to which every investigative measure must at least be subject to *ex post* judicial control in order to have adequate guarantees and, if such a measure is found to be unlawful, the person affected must be given the option of having the evidence obtained from its use excluded from the trial[57].

Therefore, where GPS data has been obtained unlawfully or incorrectly, there must be a domestic remedy in order to exclude it from being used during the trial. For this minimum guarantee to be effective, the methods by means of which the surveillance measure is carried out must be documented, including the circumstances and the modalities under which the GPS tracker is introduced in the private sphere of an individual. This is to enable a proper review by the judge and the parties of the legality and reliability of the evidence collected.

In the light of the above, an analysis of the Italian law on GPS surveillance appears appropriate: first of all, in order to assess whether there is a risk for Italy of being found in violation of Article 8 ECHR, and secondly because, according to the well-known decisions of the Italian Constitutional Court n. 348 and n. 349 of 2007, the ECHR provisions as interpreted by the Court of Strasbourg constitute interposed parameters of constitutionality of Italian domestic norms pursuant to Article 117 of the Italian Constitution[58].

As was the case in France before the adoption of the *loi relative à la géolocalisation*, GPS surveillance lacks an explicit legal basis in Italy. Both the legal doctrine and the jurisprudence generally find such legal basis in a combination of norms, namely Articles 55, 348, 370 of the Code of Criminal Procedure[59]. The respective norms describe the powers of the judicial police (funzioni della polizia giudiziaria), including in the

55 *Ibidem*, par. 8.2.

56 Ben Faiza v. France, *op.cit*., par. 51.

57 Uzun v. Germany, *op.cit*., paras. 71-72. Even in case of a search warrant, the ECtHR argued that "the absence of a prior judicial warrant was, to a certain extent, counterbalanced by the availability of an *ex post factum* judicial review. The applicant could, and did, make a complaint to a court which was called upon to review both the lawfulness of, and justification for, the search warrant". Smirnov v. Russia, Application no. 71362/01, 7 June 2007, par. 45.

58 This position was confirmed by the Constitutional Court in judgements n. 39 of 2008; n. 311 and 317 of 2009, n. 138, 187, 196 of 2010 and then, n. 80, 113, 303 of 2011.

59 According to the Court such combination of articles offers the legal basis for GPS surveillance, as in general for those investigative means which are not explicitly contemplated by

collection of evidence (assicurazione dei mezzi di prova), as well as the powers of the public prosecutor (atti diretti e delegati). In short, GPS surveillance falls within the general functions of the judicial police, who traditionally have the task of carrying out – on their own initiative or on behalf of the public prosecutor – "gli atti necessari per assicurare le fonti di prova e (…) quant'altro possa servire per l'applicazione della legge penale [the necessary acts to collect sources of evidence and (...) anything else which could be necessary for the application of criminal law]"[60]. There is also a second interpretation, according to which GPS surveillance would fall within the scope of Article 189 of the Italian Code of Criminal Procedure, which regulates those 'atypical' evidences which are not explicitly provided for by the law[61].

In our view, neither the first nor the second interpretation offers a satisfactory solution in compliance with the ECHR. When following the first interpretation, the powers of the judicial police and the public prosecutor become so general and broad that the related norms would hardly pass a 'test of compatibility' with Article 8 ECHR. Article 370 ccp, for example, is emblematic in stating that "il pubblico ministero compie personalmente ogni attività di indagine" [the public prosecutor personally performs all investigative activities] without any further specification. When following the second interpretation, the conclusion is similar. In addition to the capacity of the evidence to ascertain facts, Article 189 ccp only provides for the general requirement that atypical evidence does not affect the moral freedom of the person concerned in order for it to be admitted as evidence by the judge. The conditions required by the Court of Strasbourg for having a legal basis appear to be lacking in Italian law, also with regard to guarantees, for which Italian law includes no provisions at all. In fact, neither Articles 55, 348, 370, nor Article 189 of the Code of Criminal Procedure provide any guarantee. Moreover, as pointed out above, the Italian Court of Cassation has consistently taken the view that not even an order from the public prosecutor is necessary for the use of GPS for investigative purposes.

5. Justification of GPS surveillance as an interference with private life

Provided that GPS surveillance is "in accordance with the law", the assessment of the potential justification of such interference with the right to respect for private life requires the ascertainment that it is "necessary in a democratic society" in order to

the law. Cass. Pen. Sez V., 27 February 2002, n. 16.130: Cass. Pen., Sez. II, 27 March 2008, n. 16.818; Cass. Pen. Sez. II, 25 March 2011, n. 1.727; Cass. Pen. Sez. I, 17 April 2012, n. 14.529; Cass. Pen., Sez. II, 21 May 2013, n. 21.644; Cass. Pen. Sez. V, 21 March 2017, n. 13.822 (which merely refers to Art. 55 ccp).

60 Art. 55 Italian Code of Criminal Procedure.

61 A. Laronga, *Il pedinamento satellitare: un atto atipico lesivo di diritti inviolabili?*, in Questione Giustizia n. 5, 2002, p. 1154-1155. *Contra* M. Stramaglia emphasizes the aside, contained in Art. 189 ccp, "sentite le parti sulle modalità di assunzione" [once having heard the parties on the modalities of acquisition]. From here he deduces that Art. 189 ccp only applies to evidences, and not to investigation means, which cannot be properly acquired. See further M. Stramaglia, *op.cit*., p. 215; A. Serrani, *op.cit*., p. 7.

achieve further specific objectives listed in Article 8 ECHR: national security, public safety or the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals and, finally, the protection of the rights and freedoms of others[62]. Thus, the interference must correspond to a pressing social need. Although not explicitly provided for, a further requirement, namely the proportionality of the interference to the legitimate objective pursued, has consistently been assumed to be part of the necessity requirement[63].

There do not seem to be any problems as far as the first aspect is concerned: GPS surveillance is aimed at the prevention of crimes, which certainly represents a pressing social need as far as explicitly mentioned in Article 8 ECHR[64]. In addition, States cannot renounce their "right to self-preservation". As long as terroristic and criminal organizations avail themselves of new technologies for communication and organization, States need to have the same means at their disposal.

In order to assess the second requirement – the proportionality of GPS monitoring – a comparison with more traditional visual surveillance methods may prove fruitful, given that the latter appears to be the closest investigation technique. In fact, since visual surveillance is the activity of monitoring the movements of a person, satellite geolocation could be classified as a technological *species* of that *genus*[65].

According to some authors, GPS surveillance is characterized by greater intrusiveness compared to visual surveillance, since it enables an extremely precise and continuous monitoring, even in places which would otherwise be invisible and where visual surveillance would therefore not be practicable[66]. However, precision and continuity of monitoring are not necessarily synonymous with greater intrusiveness. In fact, while GPS technology is also able to detect very detailed movements in places which are otherwise invisible, it does not permit the all-encompassing monitoring of all things visible through visual surveillance (e.g. gestures and encounters of persons, etc.). It only intercepts the movements of a person and only while the person uses the vehicle or object on which the GPS tracker is installed.

In conclusion, while it is true that visual surveillance, unlike satellite tracking, is unlikely to be used continuously over longer periods of time, e.g. due to the cost of the investigative activity, it should be noted that, at least in principle, visual surveillance

62 "Il reste à examiner si l'ingérence était «nécessaire dans une société démocratique» pour atteindre ces objectifs". Matheron v. France, Application no. 57752/00, 29 March 2005, par. 34. According to A. Gaito and S. Furfaro the very aim of the interference shall be the maintenance of the democratic society. A. Gaito, S. Furfaro, *op.cit*., p. 561.

63 Leander v. Sweden, *op.cit.*, par. 58; Ben Faiza v. France, *op.cit*., par. 78.

64 "The Court has therefore to accept that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime". Klass and others v. Germany, Application no. 5029/71, 6 September 1978, par. 48.

65 A. Laronga, *op.cit.*, p. 1154.

66 D. Gentile, *op.cit.*, p. 1472; F. Iovene, *Pedinamento satellitare e diritti fondamentali della persona*, Cassazione penale, 2012, p. 3557.

would be more intrusive than satellite geolocation if it was carried out over the same period of time[67].

When considering that the aim pursued by GPS surveillance as an investigation technique is the prevention and suppression of crimes and that it qualitatively "interferes less" with the private life of the person concerned, also in comparison to traditional visual surveillance, it can be assumed that the requirement of proportionality will, as a rule, be satisfied, except if GPS monitoring is carried out over substantially long periods of time and/or when the investigation concerns minor offences. This can be deduced *a contrario* from the reasoning of the ECtHR in the *Uzun v. Germany* case. Indeed, although there was no statutory time constraint in German law, the ECtHR was "satisfied that the duration of such a surveillance measure was subject to its proportionality in the circumstances and that the domestic courts reviewed the respect of the proportionality principle in this respect"[68]. Furthermore, the ECtHR noted that, under Article 100c par. 1 n. 1 (b) par. 2 of the Code of Criminal Procedure, such surveillance via GPS could only be ordered against a person suspected of a criminal offence of considerable gravity or, in very limited circumstances, against a third person suspected of being in contact with the accused, and if other means of detecting the whereabouts of the accused had less prospect of success or were more difficult[69].

6. GPS data and the right to a fair trial

Experience shows that the application of GPS is characterized by a small margin of error[70]. But while a reliability test of the GPS technique in itself seems superfluous, it could be necessary to verify the lack of negative influences from external sources – both intentional or not –, in the concrete circumstances of the case, which could jeopardize the functioning of the GPS tracker and thus the reliability of the evidence collected. The reference here is not to the jammer, a device preventing the GPS tracker from identifying its coordinates. In fact, since such a system *tout court* prevents the possibility of capturing the positioning data of the monitored object, its possible use does not affect the reliability of the geolocation. The reference is instead to spoofing, which leads the GPS tracker to process positioning data from incorrect coordinates and, for this reason, could produce irreversible consequences on the reliability and correctness of the evidence collected[71].

67 M. Stramaglia, *op.cit*., p. 224.
68 Uzun v. Germany, *op.cit*., par. 69.
69 *Ibidem*, par. 70.
70 Although GPS tracking on an open site may be clustered within a few metres, multipath propagation elsewhere may cause errors of up to 300 metres in the same tracking record. Indoor positioning then remains both elusive and a very active area of research. For a proposal of a reflectometry system measuring the deformation of the correlation function of various radio navigation signals received indoors, see J. Dampf, T. Pany, *Measuring High Bandwidth GNSS Signals for Indoor Positioning*, InsideGNSS, September-October 2013, pp. 76-80.
71 As long as a radio navigation signal is authenticated, it cannot be spoofed, with the consequent enhancement of the integrity and reliability of the geolocation information derived

The technical characteristics of GPS described so far are not without legal consequences on the level of the guarantees for the accused. It is a fundamental aspect of the right to a fair trial provided for by Article 6 ECHR that criminal proceedings, including the elements of such proceedings which relate to procedure, should be adversarial and that there should be equality of arms between prosecution and defence[72]. This means that both prosecution and defence must be given the opportunity to have knowledge of and comment on the observations filed and the evidence adduced by the other party. From this, it is deducible that the prosecution authorities shall disclose to the defence all material evidence in their possession for or against the accused[73]. This should also be applied to GPS data, which should be preserved and made available to the defence in order to give the latter the opportunity to assess and eventually challenge the authenticity and reliability thereof[74]. This is not always the case in the Member States of the Council of Europe. In Italy, for example, the coordinates acquired through GPS tracking are transposed into support documents by the police. This documentary support is used as evidence of the operations performed[75]. However, such transposition activity of GPS data into documentary support is beyond any control and errors or intentional manipulations thereof may be covered by police testimonies that everything was done correctly[76].

therefrom. For an international law perspective on spoofing, see D. Zannoni, *The Radio-Spectrum: International Regulation and Current Challenges*, Annals of Air and Space Law, vol. XL, 2015, pp. 696-697.

72 "A trial would not be fair if it took place in such conditions as to put the accused unfairly at a disadvantage". Delcourt v. Belgium, Application no. 2689/65, 17 January 1970, par. 34.

73 Georgios Papageorgiou v. Greece, Application no. 59506/00, 9 May 2003, par. 36; Fitt v. The United Kingdom, Application no. 29777/96, 16 February 2000, paras. 44-45.

74 Cf. Cass. Pen. Sez. V, 10 February 2016, n. 5550, par. 4. The defence had censured that the original support where GPS data had been recorded had been lost. However, the Court of Cassation dismissed this complaint because it was not proved and, in any case, because GPS data had been considered in combination with other data collected by other investigative means.

75 "Il sistema di rilevazione satellitare "GPS" costituisce pertanto un'attività investigativa atipica, assimilabile al pedinamento, che può entrare nella valutazione probatoria del giudice anche attraverso l'acquisizione delle annotazioni e delle relazioni di servizio redatte dalla polizia giudiziaria sulle coordinate segnalate dal sistema stesso. […] Le coordinate segnalate dal sistema stesso (c.d. tracciati) trasfuse nelle annotazioni di P.G., sono infatti la prova delle operazioni compiute". Cass. Pen., Sez. II, 21 May 2013, n. 21.644, p. 22.

76 "Si tratta di una ordinaria attività di polizia giudiziaria, posta in essere con l'ausilio di strumenti tecnici […]. Essa non è regolata da norme cogenti in riferimento ai dati raccolti. I suoi risultati, per altro, sono veicolati nella istruttoria dibattimentale attraverso le dichiarazioni di chi ha effettuato e/o coordinato l'operazione di "pedinamento"". Cass. Pen. Sez. V, 10 February 2016, n. 5550, par. 4. See further, on this issue, A Serrani, *op.cit.*, pp. 8-9; M. Stramaglia, *op.cit*., p. 220.

7. Conclusions

People perform a significant part of their activities outside their home or private premises, where their thoughts are expressed, and they interact with other individuals. However, this undeniable fact cannot legitimize any form of intrusion into their private life which could cause them to feel that they are constantly being controlled in a way that would be comparable to Orwell's Big Brother. The very idea of being constantly monitored would cause individuals to change their lifestyle and ultimately affect their freedom of self-determination (the so-called *panopticon* effect)[77].

ECHR States Parties enjoy a margin of appreciation, the scope of which will depend not only on the legitimate aim pursued by the measure of investigation adopted, but also on the particular nature and the gravity of the interference with the right to respect for private life. For the use of GPS as a special investigation technique and subsequently as evidence in court, the ECtHR seems to be satisfied with a rather generic framework of guarantees, at least in comparison to the guarantees required for the interception of telecommunications.

Nevertheless, there are some limits to the margin of appreciation of the States Parties. GPS surveillance must be necessitated by a concrete and effective need for investigations in accordance with an *ex ante* assessment. This does not mean that the request for this special investigation technique must be supported by clear, strong incriminating evidence (*dringender Tatverdacht*). It is nonetheless necessary that the leads at disposal provide at least sufficient cause to suspect (*hinreichender Tatverdacht*) that an offence has been, is being or will be committed. In this case only, the interference with somebody's private life will be "necessary in a democratic society", as required by Article 8 ECHR.

The GPS surveillance measures adopted must be proportional. This requirement may not be satisfied where GPS surveillance is used for investigations pertaining to very minor crimes and/or lasting for extensive periods of time. An assessment must be carried out for the surveillance via GPS, both *per se* and in combination with other measures of surveillance eventually taken, in order to verify whether these measures affect the right to private life of the person concerned. Indeed, an individual surveillance measure may not affect a person's right to private life, while the contrary may be the case when the same measure is ordered in aggregation with further measures of surveillance. It is worth considering, for example, the potential capacity of online

77 The Panopticon is a type of institutional building and a system of control designed by J. Bentham in the late 18th century. The scheme of the design is to allow all (pan-) inmates of an institution to be observed (-opticon) by a single watchman without the inmates being able to tell whether or not they are being watched. Although it is physically impossible for the single watchman to observe all the inmates' cells at once, the fact that the inmates cannot know when they are being watched implies that they are incentivized to act as though they are being watched at all times. As a consequence, the inmates are compelled to constantly control their own behavior. Cf. M. Foucault, *Sorvegliare e punire*, Torino, 2005, p. 67.

surveillance, a technique that enables investigators to detect and record in real time whatever occurs on a specific device (personal computer, tablet, smartphone)[78].

When several surveillance measures are carried out simultaneously and all activities of a person are monitored, what is eventually achieved seems to go beyond the simple "sum" of the intercepted data. However paradoxical this may sound at first, the level of interference with the private life of the person concerned may eventually violate the inviolability of the psyche, with the consequence of a qualitative change of the affected legal good. Total and comprehensive surveillance (*Rundumüberwachung*), i.e. surveillance capable of drawing up a complete profile of an individual's personality, is without question incompatible with the ECHR[79].

Shifting to the guarantees, the Strasbourg Court took the view that an order by a public prosecutor is sufficient for GPS surveillance to satisfy the requirements of Article 8 ECHR. The ECtHR has not provided any further clarification as to whether such an order by a public prosecutor is necessary as a minimum guarantee. An affirmative answer appears to be most appropriate. It is true that conversations, images, opinions or feelings cannot be intercepted through GPS. However, GPS data are not merely a list of positions. A person's movements permit conclusions to be drawn on their lifestyle. Thus, while GPS surveillance admittedly implies a qualitatively different interference with a person's private life compared to the interception of communications, it nonetheless seems that it should be not left to the complete discretion of the police. Then, as far as the *ex post* control of the measure is concerned, there is no doubt that it shall be attributed to a third-party organ which is impartial with respect to the opposing interests at stake, i.e. to a judge rather than to a public prosecutor. The ECtHR case law and the underlying need to avoid the possibility of abuse lead to the conclusion that it is the only way of excluding a halo of prejudice arising from the fact that both the controller and the controlled are bearers of the same interest.

Based on the above, gaps giving rise to concerns of conventional legitimacy, which are not adequately filled by the jurisprudential interpretation, can be identified in the legal framework of some States Parties for the use of GPS surveillance for investigative purposes. Indeed, in the absence of specific norms, the scope of protection for the right to respect for private life remains unclear and this leaves open the door to an 'inquisitorial' attitude of the jurisprudence.

78 When a person updates his or her profile within a specific social network, this activity as well as any other activity carried out via the same device can be monitored and intercepted. In the Weber and Saravia v. Germany case, the ECtHR dealt with the difference between strategic and individual monitoring. The first consists in the screening of conversations using keywords. By contrast, so-called individual monitoring is the interception of telecommunications of specific persons and serves to avert or investigate certain grave offences the persons monitored are suspected of planning or having committed. Weber and Saravia v. Germany, *op.cit*., par. 4.

79 This can be deduced from the reasoning developed in the Uzun v. Germany case, where the ECtHR verified whether the applicant had been subject to total and comprehensive surveillance, which was eventually ruled out. Uzun v. Germany, *op.cit*., par. 80.

Although the ECtHR does not require an explicit legal basis for GPS surveillance, it appears that States Parties should legislate in this field in order to regulate such investigation technique and to precisely define its scope of application[80]. In doing so within the scope of their margin of appreciation, States Parties can provide for a more extensive protection of the right to respect for private life beyond the minimum of guarantees required by the ECtHR. The law should indicate the nature, purpose, maximum duration and grounds for its adoption, the competent authority to authorize, conduct and supervise its entire application and, finally, remedies which can be used in cases of unlawful GPS tracking[81].

80 According to the Istanbul Resolution on "The principle challenges posed by the globalization of criminal justice", special investigation techniques – including electronic search and surveillance powers – should be precisely defined in the law and compatible with the rule of law; they should not be used except in the absence of less restrictive legal means; thus, they should be proportionate to the aim pursued; finally, they should not be carried out without a court warrant. Cf. Resolution "The principle challenges posed by the globalization of criminal justice", XVIIIth International Congress of Penal Law, Istanbul, 20-27 September 2009.

81 Cf. Recommendation Rec (2005)10 of the Committee of Ministers to Member States on "special investigation techniques" in relation to serious crimes including acts of terrorism, 20 April 2005, (a) General principles; Concurring opinion of judge Pinto de Albuquerque in Lagutin and others v. Russia, Applications nos. 6228/09, 19123/09, 19678/07, 52340/08 and 7451/09, 24 April 2014, par. 3.