Review Article
Open Access
CrossMark

Remote control systems in Italian and European legislation

Abstract

The essay examines the Italian and European legislative innovations (in particular, Germany, France, England) regarding investigations carried out using the Trojan virus.

Keywords: trojan horses, spyware, computer sensors, investigative tools, interception, cooperation

Volume 11 Issue 1 - 2023

Wanda Nocerino
Lecturer in Criminal Procedure, University of Foggia, Italy

Correspondence: Wanda Nocerino, Lecturer in Criminal Procedure University of Foggia (Italy), Street: Largo Papa Giovanni Paolo II, Foggia, Italy, Email wanda.nocerin@unifg.it

Received: December 21, 2022 | **Published:** April 19, 2023

The computer sensor as a remote "special investigation" technique

The issue of investigations using computerized detectors continues to make noise in the national and international legal area: despite the more or less recent legislative regulation in both Italy and Europe, doubts and perplexities still remain about the compatibility with the fundamental principles. All the "insiders" - legislator, doctrine and jurisprudence, each for their own sphere of competence - have questioned themselves for a long time on the scope and limits of use of the computer *virus* in investigative activities, helping to outline the physiognomy and the role that the *Trojan* takes on the internal and supranational procedural circuit.[1–3] Despite the richness of the contributions offered, the subject still seems to have blurry outlines, requiring careful study due to the impact on the constitutional principles and the evidentiary categories of the criminal trial.

Each legal analysis, however, requires some preliminary considerations, useful for framing the tool of the computer detector in the vast panorama of investigative techniques, so as to measure its scope (linked to the "technical" performance, the rate of investigative use and the alignment with the new research paradigms at European level) and its next possible evolutions. From the very definition of electronic sensor, one can discern both its typical characteristics and the technical and legal pitfalls it carries.

It can be said that the sensor - which, it is specified, does not constitute a procedural "institution" but a tool with which to implement the (more or less) traditional means of searching for evidence - is a disguised system, remotely inoculated, which, eliminating the effects that prevent knowledge of the communication or data, it allows unencrypted interception of the audio video content and data exchanged or allows interception between those present, and remotely collects the positions assumed by the apparatus on the territory. In the notion we can see the first prerogative of the *virus*, i.e., belonging to remote control systems. It is a "remote" investigation tool, made available by technological innovation through machinery, equipment and devices capable of carrying out activities, once conducted in the presence and on the site of the investigation, from a remote location.

It is not the only investigative tool of its kind. Think of the more dated bugs, commonly used for intercepting conversations and communications between those present, of directional microphones, of tracking using geolocation devices (GPS tracking), of the increasingly used video recordings made by investigative bodies for investigative purposes. Remote access offers great advantages to investigations, in terms of high intrusiveness and information potential, as well as low risk of " discovery ". But there is no doubt that these advantages have been amplified, and will be more and more, by the historical moment in which we live; moment in which the criminal process, like any other sector of life, requires that activities, communications, relationships take place remotely as a tool to contain the epidemic from Covid-19. Which easily leads to the preliminary thinking that, never before, can an unprecedented cultural opening make its way, a sort of favor by the internal and European legislator, by doctrine and jurisprudence, towards the more generalized use of remote investigations and towards a stabilization of those emergency measures born "in time", with the aim of giving an acceleration to the judicial machine.[4–6] It could be assumed that the attention paid in recent years to all forms of remote investigation (in an attempt to provide adequate answers in terms of the compatibility of the investigative results with the established system, very often resorting to the magmatic category of atypical evidence) reaches to take on new directions, inclined to recognize a conceptual autonomy and a more solid hold with respect to the traditional values of the criminal process.

But there's more. Extrapolating it from the wide range of remote investigation tools, the further characteristic of the IT sensor should be emphasized; that is which makes it the prototype of special investigative techniques (TSI), i.e. unconventional investigative methodologies which – for some time now – have been regulated (particularly at an international level) to counter offenses with respect to which the needs of repression are fueled by a growing social alarm (organized crime, drugs, corruption, child pornography , terrorism) but above all to penetrate modern criminal organizations which, in certain sectors, have shown themselves to be impermeable to ordinary investigative means. More concretely, the computer sensor falls within the category of electronic surveillance which allows remote control of the movements of subjects not already identified or identified with a minimum use of police personnel and potentially over boundless territorial areas.

In this case - unlike traditional remote investigation tools - the intention is not to control an "area" of investigative interest or a single "individual" involved (for various reasons) in an investigation, but anyone and anywhere who moves within the tool's range of action, so as to operate a penetrating and ubiquitous monitoring that does not encounter limits and boundaries of any kind, significantly affecting the complex of inviolable guarantees of the individual. In addition to the Trojan, there are other electronic surveillance tools. Think of

the sophisticated SAPR (remotely piloted aircraft systems, commonly referred to as drones), equipped with cameras for environmental monitoring and infrastructure control or even the most modern analytical video surveillance techniques based on artificial intelligence. However, compared to these, the electronic *virus* goes even further than the already pervasive forms of digital control, rummaging in the most intimate sphere of the individual, in the deepest "I", attacking the very psyche of whoever is being monitored. In fact, if it is true that the freedom of the person includes even the material things that represent fundamental parts of his existence, then this approach must extend in relation to the mobile phone and more generally to any electronic device, taking into account the use that is commonly done and of the distinctly personal and delicate contents entrusted to it.[8]

It goes without saying that malware, not only a "special surveillance technique" but also a "remote investigation technique", has peculiarities that inexorably distance it from the more well-known special investigation methodologies and make it unique among existing investigation tools. The interest of the scholar is grafted into this conceptual framework, whose investigation must inexorably start from the most daring aspects (at least for the jurist) relating to the functionality of the Trojan virus, without which it is not possible to fully grasp its potential.

Without delving deeply into the meanderings of the most refined computer technicality, it can be said that the *virus* allows the inoculant to take full possession of the target machine and, consequently, to learn an in(de)finite amount of data and information that is unlikely they could be known (and knowable) by investigators using traditional investigative techniques, exploiting the portability and inscrutability of the tool.[7–9]

However, the chameleonic nature of malware, combined with the ontological intolerance of spacetime predeterminations, generate many doubts in the scholar about the compatibility of the resulting investigative results with the procedural fabric and the supranational regulatory network. In this case, the risk to be avoided is that remote investigations via viruses Trojan, in their multiple functional and systematic facets, go beyond the contents and legislative dimensions of the individual legal systems that host one – albeit embryonic – discipline and the related internal and supranational "equipment". This contribution will address these aspects, focusing in particular on the differences between national legislation (only apparently more "guaranteed") and the European disciplines that have given voice to the multiple remote special investigation techniques also as a response to the threats of international terrorism.[10–13]

From a structural point of view, the research initially focuses on the analysis of internal legislation, highlighting the rules, limits and criticalities of the discipline outlined by the legislator. Once the boundaries of use of the *virus* in internal investigations have been defined, the investigation intends to continue along two directions: in a comparative key, proceed to analyze the regulation of surveillance techniques in European systems, highlighting similarities and differences with respect to the internal legal system; secondly, to dwell on the "new" cross-border investigations conducted using remote forensics techniques. In this sense, the research sets itself the ambitious goal of tracing the most suitable cooperation tool for the transnational collection of information, in order to verify the existence of a regulatory coverage of the research activities and acquisition of evidence that transits from and to the 'abroad.

Surveillance tools in Europe: comparative approaches

In Europe there is a tangible legislative dissonance in this matter, brutally contrary to that harmonization process hoped for by the European Community since its origins. In fact, if a more or less complete regulation of *surveillance* systems is introduced in some legal systems, in others, apparently more guaranteed (such as Italy), remote control techniques are not the subject of legislation. It is not believed that this approach can be the result of a causal factor: the choice to standardize remote control techniques, even with a preventive function, is typical of those legal systems that are (more or less) directly affected by terrorist attacks of international origin for which, as a consequence of the proclamation of a state of emergency, the level of protection of individual guarantees is weakened in the name of national security.

Before analyzing the regulatory status in force in some European countries, symbol of the regulatory framework on surveillance, it is appropriate to point out right now that the same regulatory shortcomings are found in all legislative interventions. First of all, the openness to large-scale interception activities is based on opaque and unclear foundations, lacking the specification of the elements or conditions that justify recourse to the measure in question (lack of mandatory nature). Furthermore, none of the regulations provides for the introduction of adequate control and supervision elements regarding the execution of the operations necessary to prevent possible abuses (lack of jurisdiction).

It is already anticipated that - on several occasions - both the internal Courts and the ECtHR have intervened to "quench" the internal pressures of those countries that are increasingly inclined to adopt electronic surveillance systems. Therefore, it can be affirmed, without fear of contradiction, that above all the jurisprudential trend of the ECtHR, in combination with the internal decisions of unconstitutionality, represent the symptomatic indicators of the change of a system which, while not neglecting the needs of national security, requires offering adequate protection to the right to privacy and IT confidentiality.

The use of *Trojan virus* in Italian legislation

The subject of interceptions using computer data collectors is the result of an unprecedented jurisprudential and legislative stratification. Despite the efforts made, the new provisions are implemented only four years after the first reform intervention. This affair, it has been said, " has grotesque features". More precisely, after a disorganized jurisprudential production aimed at limiting the use of the Trojan in criminal investigations referring only to the most serious crimes of organized crime (Court of Cassation, Section Un., 28 April 2016, no. 26889), the definitive entry of the IT sensor into the criminal process was already consecrated in 2017 (Legislative Decree 29 December 2017, no. 216) . Although promulgated in January 2018, the decree has not been fully implemented. After a series of legislative rebounds that have postponed its implementation and supplementary laws aimed at "correcting the shot" of the hasty legislator of 2017 (Law of January 9, 2019, no. 3), precisely on December 31, 2019 – on the day of its hypothetical entry into force – the Council of Ministers amends the regulations contained therein (Legislative Decree 30 December 2019, n. 161), arranging a further deferment of the effectiveness of the provisions introduced, before 29 February 2020 , then as of

Citation: Nocerino W. Remote control systems in Italian and European legislation. *Forensic Res Criminol Int J.* 2023;11(1):19–24.
DOI: 10.15406/frcij.2023.11.00363

April 30, 2020 (Law of February 28, 2020, no. 7), and, finally, as at 31 August 2020 (Legislative Decree April 30, 2020, no. 28), with the aim of "allowing the completion of the complex organizational measures in place, also relating to the preparation of electronic and digital devices" .

Beyond the temporal profiles, it can be highlighted that the legislative insert - through a modification of paragraph 2 of art. 266 criminal code - aims to formalize the establishment of a new technique of wiretapping between those present to be conducted by placing IT captors in portable electronic devices, attributing a specific face to the activity in question: not a new form of wiretapping, to be placed alongside telephone, environmental and telematic ones, but only a new tool through which to carry out an "old" means of researching evidence, i.e. to conduct environmental interceptions. Furthermore, that law addition of an unprecedented paragraph 2 *bis* to art. 266 of the criminal code, it is envisaged that such forms of interception are always permitted in places of private residence (art. 614 of the criminal code), regardless of the existence of the well-founded reason to believe that a criminal activity is taking place in that place, only in the case of crimes pursuant to art. 51, paragraphs 3 - *bis* and 3- *quater,* criminal code and for "serious" crimes against the public administration, subject to indication of the reasons justifying the intrusion.

Further changes are recorded in relation to the content of the authorization decree. Through an interpolation of paragraph 1 of the art. 267 criminal code, the proceeding judge is required to make a further documentary effort for which the decree would assume the guise of a provision accompanied by a "strengthened" motivation. In fact, the judge is always required to indicate the reasons (specific, *pursuant to* Article 2, conversion laws of Legislative Decree No. 132 of 30 September 2021) which make the particular operating method necessary. But it should be noted that the "necessity" indicated in the decree is not equivalent to the requirement of the "indispensability" of recourse to the particular investigative tool which, conversely, is not required by the normative datum. From the literal wording of the provision in question, it is clear that proof of the fact that recourse to this particular form of interception is the only practicable operational tool is not necessary, since the judgment of necessity does not coincide with that of a certain fruitlessness of the other forms of environmental interception but rather with proof [...] of a less easy practicability of traditional operations.

However, in the event that proceedings are carried out for crimes other than those indicated in art. 51, paragraphs 3 - *bis* and 3- *quater*, criminal code, as well as for "serious" ones against the public administration, the motivational obligations are further "aggravated", the judge also having to indicate the places and the time, even if indirectly determined, in relation to which activation of the microphone is permitted. Then, through the introduction of a new paragraph 2- *bis* to art. 267 criminal code, the role of undisputed protagonist of the prosecutor in the context of the emergency procedure is attenuated: the same, in fact, can proceed to authorize the execution of the operations by means of a computer *virus* with a motivated decree - which must mention the specific reasons for the urgency, such as not to allow waiting for the natural jurisdictional provision - only in the case in which proceedings are carried out for organized and economic crimes referred to in art. 266, paragraph 2 -*bis,* criminal code. Lastly, the reforms also affect the regulation of the prohibitions on the transmigration of results acquired via *Trojan* in other proceedings (art. 270 criminal code) and the probative use of illegitimately acquired data (art. 271 criminal code).

With reference to the first aspect, the legislator introduces an unprecedented paragraph 1- *bis* to art. 270 of the Code of Criminal Procedure, ruling that, without prejudice to the prohibition of use of the catchment product in proceedings other than those in which the same were ordered, "the results of the interceptions between those present carried out with an IT sensor on a portable electronic device can also be used to prove crimes other than those for which the authorization decree has been issued, if included among those indicated by article 266, paragraph 2- *bis* criminal code , conditioning their use to the canon of "indispensability". As regards, however, the ban on the ultra-vis use of the data acquired, through the interpolation of an unedited paragraph 1 *bis* of art. 271 criminal code, it is established that "Noever the data acquired during the preliminary operations for inserting the computer sensor on the portable electronic device and the data acquired outside the time and place limits indicated in the decree can be used authorisation". This is a rule intended to affect not the mere non-compliance with executive procedures but aimed at overseeing some fundamental application boundaries of the instrument, albeit regulated through operational precautions of a technical nature.

Beyond the innumerable criticality profiles that can be highlighted in the legislation highlighted, what I would like to highlight here is the questionable legislative choice - entirely internal - to regulate only one of the many activities that *malware* is, at least potentially, capable of carrying out once inoculated on the target machine, on the observation that, through the mere activation of the microphone of the portable electronic device on which the *virus* acts, the resistances of those who had seen a "bulimic" creature in the sensor could be overcome capable of conducting multiple activities at the same time. On this point, in fact, the doctrine advances reservations, believing that the "hidden" side, on which the novella has remained silent, creates even greater interpretative difficulties than those directly linked to reading the text.

The German experience...

Among the European countries that adopt a legislation to regulate the use of remote control systems - especially in the preventive phase - Germany and France stand out, as "pioneer" states in the legalization of Trojan software even before the terrorist threat. In order to better understand the "content" of the reforms, it is necessary to start from a quick overview of the previous legislative system. As far as the German legal system is concerned (based on the principle of seeking material truth in its broad dimension as a rule common to investigative and evidentiary activity, pursuant to § 155, 244 paragraph 2 StPO), the inviolability of the secrecy of correspondence and telecommunications is protected by art. 10 of the Basic Law (*Grundgesetz*); the interference to the enjoyment of the right in *question* is, however, expressly permitted by the articles 100 a) and 100 b) of the *Strafprozeßordnung* (StPO), in relation to procedural interceptions. With regard to preventive wiretapping, the law on the limitation of epistolary, postal and telecommunications secrecy of 2001 (*Gesetz zur Beschränkung des Brief–, Post– und Fernmeldegeheimnisses*, of 26 June 2001) legitimizes the interceptions carried out even in the absence of a criminal proceeding.

With reference to the use of the computer sensor, in 2006, the art. 5, paragraph 2, no. 11 of the Constitutional Protection Act of North Rhine- Westphalia allows a government delegation intelligence body to monitor and access computer systems connected to the Internet in order to covertly intercept data and communications using technical capture tools. Then, in 2008 (*Bundeskriminalalamtgesetz* (BKAG) of 25 December 2008), the German federal legislator introduced new provisions aimed at allowing investigations through the use of IT means that allow the acquisition of data remotely. In a context such

Citation: Nocerino W. Remote control systems in Italian and European legislation. *Forensic Res Criminol Int J.* 2023;11(1):19–24.
DOI: 10.15406/frcij.2023.11.00363

as the one described - which seems to legalize tout court the captive activity before and after the crime by means of technical surveillance and monitoring tools - the constitutional jurisprudence assumes a central role which, starting from 2008, questions about the possibility of admitting remote surveillance technical tools. In that circumstance, the Court, while declaring the aforesaid legislation unconstitutional, not respectful of the principles of proportionality and specificity, does not absolutely exclude the admissibility of technical investigative tools, however deeming it appropriate to provide additional and subsidiary protection with respect to that already in force.

Consequently, the investigative operations likely to compress this new right of personality (direct projection of the new digital reality) can be justified, not only for purposes of repression of crimes, but also for preventive purposes, provided that the principle of proportionality is respected and the reservation of jurisdiction (*Bundesverfassungsgericht* , 2 March 2010 (1 BvR 256/08, 1 BvR 263/08; 1 BvR 586/08), available at *http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html*). More recently, when faced with the question, the Court takes on more severe tones, declaring the unconstitutionality of some provisions of the federal law called " *Bundeskriminalamtgesetz* ", which governs the duties and activity of the federal police force (*Bundeskriminalamt*) and cooperation in criminal matters between state and federal governments and with third countries. In the same vein as the 2008 ruling, the *Bundesverfassungsgericht* recognizes the legislator's duty to balance the protection that the State must grant to citizens and the fundamental rights claimed by them, stating that this balance must be carried out in compliance with the principle of proportionality, according to which «the investigative powers which profoundly affect privacy must be limited by law to the protection of sufficiently important interests in cases in which a sufficiently specific danger to these interests can be foreseen" (*Bundersverfassungsgericht* , 20 April 2016, 1 BVR 966/09, 1 BVR 1140/09).

Despite the attempt to curb the indiscriminate use of technical monitoring tools both in the preventive and procedural phases, the *Bundestag*, just over two months after the Munich attack, intervenes to redraw the symmetry between some of the essential elements of German democracy, that is, the relationships between freedom and security, *privacy* and intelligence, justice, prevention and repression. In particular, in October 2016 the Communication Intelligence Gathering comes into force Act, whereby the external security agency (the Federal Intelligence Service, BND) becomes the holder of the power to collect and process all communications from foreign citizens or entities that pass through the major Internet exchange node in Frankfurt for needs of contrasting not only terrorism and organized crime but also for prodromal acts and, therefore, in the presence of the risk that an abstract danger crime could be committed, determining an exponential anticipation of the state intervention threshold.

In this renewed context, the immeasurable recourse to remote control techniques finds fertile ground. In 2017, in fact, the German government approved legislative amendments concerning the "*Bundestrojaner*" to allow the authorities to install software and decrypt private use of the Internet without consent. Not only. A few months ago (June 2021) the Government coalition reached an agreement on the use of state Trojans by both the federal police and the constitutional protection service, so as to extend the - already lax - rules in force in the preventive system also in that procedural.

....and the French one

With reference to the French legal system, the matter of interceptions is articulated on a double track: on the one hand, the art. 100 of the *Code of procedure pénal* relating to ordinary proceedings provides that it is the *juge d' instruction to order* wiretapping operations in proceedings for *délits or crimes* punished with more than two years' imprisonment and for a renewable term of four months, on the other hand, following the law of 9 March 2004, it is possible to order preventive interceptions on the basis of a derogatory discipline envisaged by art. 706-95 criminal code in the matter of organized crime - regulated in book IV of the *Code de procédure* - which already allows during the *enquête préliminaire or de flagrance* to resort to interception operations. *ad hoc* discipline can be found in the French legal system – even before the terrorist emergencies that devastated the country – in relation to the use of technical collection instruments. In fact, the art. 706-102-1 criminal code regulates the so-called "*captation des données informatiques*" which allows, again via a device inoculated on a computer medium, access to all the user's information present *therein* and the performance of a series of saving, storage and transmission activities for such data. Furthermore, the law n. 731 of 3 June 2016 introduces, in the articles 706-95-4 and following of the *Code de procédure pénale*, a specific discipline of the *IMSI Catcher*, another technological tool, similar to an antenna, which allows the telephone number to be picked up and located and which, in the most updated versions, can also allow data to be intercepted.

Despite the preparation of a rather detailed regulatory apparatus (and, at least in form, guaranteed) on the subject, just two weeks after the Paris attacks, Parliament issues the International Electronic Communication Law (Law 24 July 2015, no 2015–912, *www.legifrance.gouv.fr*) which authorizes an external intelligence agency (so -called French Directorate General for External Security) to intercept, collect and monitor communications sent or received abroad without the need to receive any judicial authorization and, consequently, without specifying the "motives" of the interference, i.e. the reasons why the measure is deemed suitable for safeguarding collective security.

The English experience and the censures of the ECtHR

The main regulatory source on wiretapping is the Regulation of Investigatory powers Act 2000 (RIPA), with which the legislator, innovating the previous regulation of 1985, carries out an organic review of the investigative powers of the investigative authorities and the police forces, which became necessary due to technological evolution and, above all, the diffusion of communications electronics and encryption devices. The law of 2000 regulates, in particular, the investigation activities whose exercise contemplates the interception of communications, the acquisition of data relating to telephone traffic, the decryption of data, the use of agents and informants. It outlines a framework of guarantees through the delimitation of the purposes for the legitimate use of these investigative tools, the identification of the subjects authorized to use them, the provision of specific authorization procedures, the assignment to the judiciary of independent supervision tasks and, finally, the recognition to the persons concerned of a right of opposition, depending on the case, to the carrying out or continuation of the aforementioned activities.

Investigatory was issued on 29 November 2016 powers Act (so-called Snooper Card) with which the country, also due to the terrorist alarm felt in neighboring states, legitimizes the use of massive surveillance with technical tools as an expedient for neutralizing the phenomenon. The legislative intervention in question unfolds along two guidelines: on the one hand, the right of the British intelligence agencies (British Intelligence Community) to carry out non-targeted interceptions of data and communications is consecrated; on the other

Citation: Nocerino W. Remote control systems in Italian and European legislation. *Forensic Res Criminol Int J.* 2023;11(1):19–24.
DOI: 10.15406/frcij.2023.11.00363

hand, it allows public authorities to view the records relating to user communications, regardless of the authorization (mandate) of the judicial authority.

However, a few years later, the EctHR (ECtHR, 13 September 2018, *Big Brother and others v. United Kingdom, applications* no. 58170/13, 62322/14 and 24960/15) intervenes to censure the legislation in force in the United Kingdom, as it violates the right to privacy (art. 8 ECHR) and freedom of expression (art. 10 ECHR). According to the Strasbourg Court, "the data collection methods and the amount of people tracked are not sufficiently specified and [...] there are no rules on filtering, searching and selecting the communications subject to control. [….] Collecting not only traffic data but also the content of communications that can be monitored is a serious invasion of privacy. [...] The mass surveillance system is not, in itself, a violation, but such a system must meet strict criteria [...]. What is implemented in the United Kingdom, however, exceeds the degree of interference that can be considered "necessary in a democratic society".

The pronouncement essentially represents the milestone of a European policy aimed at the progressive undermining of European standardization which legitimizes the use of *surveillance techniques* in the absence of a precise standardization that outlines the times, cases and methods of interference, with a view to a proportion between investigative and prevention needs and the protection of fundamental rights.

The impact on fundamental rights

A time analyzed the discipline of the Trojan virus, it is necessary reflect on impact of usage of the rights remote control systems on fundamental rights. The interceptions constitute an intrusion in private life and in specific of the correspondence (ECtHR, Grand Chamber, 6 September 1978, *Klass v. Germany* , No. 5029/71 , § 41; ECtHR , section IV, May 18, 2010, *Kennedy v. Kingdom United* , No. 26839/05, § 118-129 and 151; ECtHR , section II, 10

April 2007, *Panarisi v. Italy* , No. 46794/99; ECtHR , section II, 31 May 2005, *Vetter v. France* , 59842/00; ECtHR, Grand Chamber, 16 December 1992, *Niemietz v. Germany* , No. 13710/88, § 32), to be considered , in principle, undesirable and difficult compatible in one society democratic (ECtHR, Grand Chamber, 2 August 1984, *Malone v. Kingdom United* , No. 8691/79, § 67) . More in the detail, interceptions they determine evident collisions with rights constitutionally guaranteed, such as the art. 13 of the Constitution, bulwark of the freedom of each individual , the art. 14 of the Constitution, placed to protect the home, the art. 15 of the Constitution, which protect freedom and privacy of the correspondence and of each another form of communication , as well as, shifting the gaze beyond the borders national law , the principle of proportionality that imposes the need for a perfect correspondence between the results prosecuted and i means used and , more particularly , between the potential force invasiveness of the medium under consideration and the inevitable wound of the rights fundamentals.

Just as many threats yes warn in relation to the rights of "second generation", such as confidentiality and privacy, to be understood as a prerequisite of the freedom, foundation of the capacity for self-determination individual (CJEU, 8 April 2014, *Digital Rights Ireland Ltd v Ireland*, in *eurlex.europa.eu*; CJEU, 13 May 2014, *Google Spain v AEPD*, in *eur-lex.europa.eu*). If this is what is strenuously maintained in relation to traditional procedural captures, more specific reflections seem necessary when the intrusion is carried out through technical data acquisition tools. In the face of the indiscriminate performance that the computer sensor, at least potentially, can achieve, it is inevitable that the intrusion into the intimate sphere of the controlled person manifests itself in a hitherto unknown extent, as profound as it is pervasive, to such an extent as to the psychic breakdown. In fact, the ability to monitor remotely, secretly and without limits, each activities that the subject leads, determines the proliferation of threats to " third party" rights generation ", typical of a " society.

2.0", designed to protect the new ones needs of an individual computerized and impose a leap qualitative in the identification of rules aimed at guaranteeing it. Think of the refurbished right at the confidentiality of the systems computer science (BVerfG, February 27, 2008, no. 370/2007-595/2007, in *BverfGE* 120, 27), to home protection information technology, as well as the law to intangibility of digital life, which unlike of the already known guarantee of the secrecy and integrity of the systems computer , does not focus their own sphere of protection on instrument IT itself considered , but yes concentrate on the individual , presiding over his subjectivity in relation to anyone data or activity breakthrough within a system computer and network .

Since the Trojan virus is capable of violating fundamental rights, it is necessary for the legislator to redefine the matter in order to make it compliant with European principles, which impose clarity, sufficiency, specificity of the case as well as, in particular, respect for the principle of proportionality (ECtHR, Grand Chamber, 26 April 1979, *Sunday Times, c. Kingdom United*, No. 6538/74, § 47). A regulation in a clear and complete form both of the individual activities that can be carried out and of the cases in which the intrusion could be legitimate, would be functional to the protection of the principle of legality as well as to confer certainty to the right of defense, so as to allow the controlled to have effective knowledge of the methods of interference by the investigators in the sphere of individual confidentiality, assessing the compliance of the activity performed with respect to the limits identified by the content of the provision and by the content of the authorization decree.

But above all, the standardization of the other forms of surveillance and control that can be carried out in the procedural phase is foreseen as inevitable, both in terms of foreseeing specific requirements for the treatment and use of the acquired data, and of control regarding the lawfulness and legitimacy of the activity conducted. Although the state of the art is very critical, the legislator knowingly decides not to respond to international requests that require the introduction of a more precise discipline of the technical instruments of collection, in order to definitively dispel the numerous suspicions of illegitimacy that have always been generated but exacerbated by the "immoderate" use of technology.

Acknowledgments

None.

Conflicts of interest

The author declares there is no conflict of interest.

References

1. Aimonetto. *Processo penale francese*, in *Enciclopedia del diritto*, II, 2008. p. 723.
2. Bassoli. *Uk: approvato l'Investigatory Powers Act*, 2016. p. 10.
3. Bronzo P. *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, in Giostra-Orlandi, *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*. Turin. 2018;2:235–262.

Citation: Nocerino W. Remote control systems in Italian and European legislation. *Forensic Res Criminol Int J.* 2023;11(1):19–24.
DOI: 10.15406/frcij.2023.11.00363

4. Filippi L. L'ispe-perqui-intercettazione "itinerante": le Sezioni Unite azzeccano la diagnosi ma sbagliano la terapia. *Archivio penale*. 2016;348–353.

5. Gialuz M, L'emergenza nell'emergenza: il decreto-legge n. 28 del 2020, tra ennesima proroga delle intercettazioni, norme manifesto e "terzo tempo" parlamentare. *Sistema penale*. 2020.

6. Kostoris –Orlandi. *Contrasto al terrorismo interno ed internazionale*, Turin, 2006; Kostoris –Viganò, *Il nuovo "pacchetto" antiterrorismo*, Turin, 2015.

7. Ligustro A, Sessant'anni dell'Italia all'ONU: per una celebrazione senza retorica. *Diritto pubblico Comparato ed Europeo*. 2016;3–12.

8. Nocerino W. *Il captatore infromatico nelle investigazioni interne e transfrontaliere*. Cedam. 2022. Nocerino W, *Il tramonto dei mezzi di ricerca della prova nell'era 2.0*. *Diritto penale e processo*. 2021. p. 1017.

9. Patanè, *Processo penale inglese*. Enciclopedia del diritto, II, 2008.

10. Peloso C. *La scelta della Francia di autorizzarsi a derogare la convenzione europea dei diritti dell'uomo: la portata dell'articolo 15 Cedu nel quadro dello stato di necessità*. 2016.

11. Peloso C. *La tutela della riservatezza nell'era delle nuove tecnologie: la vicenda dei captatori informatici per le intercettazioni tra presenti nei reati di terrorismo*. 2017.

12. Picone. L'insostenibile leggerezza dell'art. 51 della Carta dell'ONU. *Rivista diritto internazionale*. 2016;99(1):7–31.

13. Rafaraci. *Processo penale tedesco*, in *Enciclopedia del diritto*, II, 2008, 831 ss.

14. Renucci, *État d'urgence: la France s'autorise* à *déroger* à la Convention ed*h*. 2015a.

15. Spangher. *Critiche. Certezze. Perplessità. Osservazioni a prima lettura sul recente decreto legislativo in materia di intercettazioni*. 2018.

Citation: Nocerino W. Remote control systems in Italian and European legislation. *Forensic Res Criminol Int J*. 2023;11(1):19–24.
DOI: 10.15406/frcij.2023.11.00363