Araştırma Makalesi/Research Article **Doi: 10.55009/bilisimhukukudergisi.1382980**

INVESTIGATION AUTHORITIES' ABILITY TO SECRETLY OBTAIN EVIDENCE FROM ELECTRONIC DEVICES THROUGH REMOTE ACTIVATION IN THE FRENCH PENAL PROCEDURAL CODE

Fransız Ceza Muhakemesi Kanunu'nda Soruşturma Makamlarının Uzaktan Etkinleştirme Yoluyla Elektronik Cihazlardan Gizlice Delil Elde Edebilmesi

Prof. Dr. Murat BALCI[*]

Assoc. Prof. Kerim ÇAKIR[**]

Abstract

The proposal that adds amends Article 230-34 with Article 230-34-1 and Article 706-96-1 with Article 706-96-2 in the French Penal Procedural Code creates an amendment allowing the collection of evidence through audio and visual recordings, as

[*] Fatih Sultan Mehmet Vakıf University Law Faculty, Professor in Criminal Law and Criminal Procedural Law Department, E-mail: balci53@hotmail.com; ORCID ID: 0000-0002-8506-7911.

[**] Marmara University Law Faculty, Associate Professor in Criminal Law and Criminal Procedural Law Department, E-mail: kerimcakir@marmara.edu.tr; ORCID ID: 0000-0003-1821-9935.

Makale Gönderim Tarihi/Received: 29.10.2023.

Makale Kabul Tarihi/Accepted: 27.12.2023.

Atıf/Citation: Balcı, Murat ve Çakır, Kerim. "Investıgation Authorities' Ability To Secretly Obtain Evidence From Electronic Devices Through Remote Activation In The French Penal Procedural Code." *Bilişim Hukuku Dergisi* 5, no. 2 (2023): 126-150.

well as geolocation data, by accessing technological devices. This is particularly relevant in cases related to terrorism and organized crime. Additionally, new paragraphs have been amended to Articles 230-36 and 706-97 of the French Penal Procedural Code. As a result of these amendments, investigation authorities are for the first time in a penal procedural code, empowered to secretly obtain evidence from electronic devices through remote activation.

In this context, the current article will address how and which authorities can listen to a person during an investigation, the offenses that allow this measure to be applied, the limitations of cataloged offenses, and how eavesdropping for intelligence purposes will be conducted. Considering this information, the article will also explore the effect the regulation will primarily have on the right to defense, right to privacy, freedom of communication, and protection of personal data.

Keywords: remote activation of electronic devices, geolocation data, audio and visual recording, respect for private life, terrorism, organized crime.

Öz

Fransız Ceza Muhakemesi Kanunu'na 230-34 maddesinden sonra 230-34-1 maddesini ve 706-96-1 maddesinden sonra 706-96-2 ekleyerek değişiklik yapan yasa tasarısı ile özellikle terör suçları ve organize suçlar bakımından yürütülen soruşturmalarda uzaktan aktivasyon yöntemiyle ses ve görüntü kaydı yapılarak elektronik cihazlardan delil elde edilmesini ve yer tespiti için teknolojik cihazlara erişilmesini mümkün kılan bir düzenleme yapılmıştır. Aynı şekilde Fransız Ceza Muhakemesi Kanunu madde 230-36 ve 706-97'ye yeni fıkralar eklenmiştir. Değişiklikler ve eklemeler neticesinde, soruşturma makamlarının uzaktan erişim yoluyla elektronik cihazlardan gizlice delil elde etmesi uluslararası alanda ceza muhakemesi kanununa ilk kez getirilmektedir.

Bu bağlamda çalışmada, soruşturma evresinde suç şüphesi altında bulunan kimsenin elektronik cihazlarının ne şekilde kimler tarafından dinlenebileceği, söz konusu tedbirin hangi suçlarda uygulanacağı, katalog suç sınırlaması ve istihbarat amaçlı dinlemelerin ne şekilde yapılacağı ele alınacaktır. Bu bilgiler ışığında söz konusu düzenlemenin savunma hakkı başta olmak üzere, özel hayatın gizliliğine, haberleşme hürriyetine, kişisel verilerin korunmasına etkisi değerlendirilecektir.

Anahtar Kelimeler: Elektronik cihazlara uzaktan aktivasyon, yer belirleme, ses ve görüntü kaydı, özel hayata saygı hakkı, terör suçları ve organize suçluluk.

INTRODUCTION

This article addresses specific amendments to the French Penal Procedural Code that were submitted to the French Senate on May 3, 2023 for Article 3, which permits audio-visual materials to be obtained from technological devices through their remote activation, especially in investigations carried out regarding terrorism and organized crime, as well as geolocation data; these being different from the first draft and Article 3,[1] which permits remote activation for the purposes of obtaining geolocation data and was supplemented by certain limitations such as applying this measure only for prosecuting offenses that carry least 10 years of incarceration,[2] have triggered some debates in the Senate. The article delves into how audio and visual recording evidence may be obtained from electronic devices in investigations conducted for terrorism and organized crime through remote activation, as well as how technological

[1] Assemblée Natıonale-Rapport (June 23, 2023) Tome I, p. 11.

[2] Assemblée Natıonale-Rapport (June 23, 2023) Tome I, p. 15. In the initial version of the proposal, the threshold was for at least a five-year incarceration; upon modifications from the Senate, however, this was raised to 10 years. Nevertheless, the National Assembly opted for the five-year incarceration again in a plenary session, although the Commission had previously rejected the relevant amendment that had reduced 10 years to five.

devices may be accessed for geolocation data through Articles 230-34-1[3] and 706-96-2[4] of the French Penal Procedural Law

[3] An available translation of Article 230-34-1 is as follows: "When research or investigation regarding a crime or misdemeanor which is punished with at least five-year imprisonment so requires, the judge of freedoms and detention, upon request of the prosecutor of the Republic or investigating judge, can authorize, under the same conditions which are mentioned in 1° and 2° of the Article 230-33, remote activation of an electronic device, without knowledge or consent of its owner or possessor, only for the purposes of their geolocation in real time. The decision shall include all the elements that permit identification of the device.

Remote activation that is mentioned in the present article cannot concern the electronic devices utilized by the people mentioned in Article 100-7."

[4] An available translation of Article 706-96-2 is as follows: "The judge of freedoms and detention, upon the request of the prosecutor of the Republic or investigating judge, can authorize remote activation of an electronic device, without knowledge or consent of its owner or possessor, only for purposes of operations mentioned in Article 706-96. Duration of the authorization mentioned in the premier paragraph of the Article 706-95-16 is reduced to 15 days, which can be renewed once. These durations mentioned in Paragraph 2 of the same Article 706-95-16 has been extended to two months, with the total duration of the operation not exceeding six months.

The prosecutor of the Republic or investigating judge can appoint all the physical and legal persons authorized and registered in one of the lists foreseen in Article 157, for performing remote activation of an electronic device mentioned in the present article. The prosecutor of the Republic or investigating judge can also prescribe resorting to state means subjected to secrecy of the national defense according to forms foreseen in Chapter I of Title IV of Book I.

Remote activation of an electronic device mentioned in the present article cannot concern the electronic devices used by those mentioned in Article 100-7. If it appears that data collected by means of this activation came from a device which is found in a place mentioned in Articles 56-1,56-2, 56-3, or 56-5, these cannot be transcribed. Dispositions of the present paragraph is prescribed to sanction of nullity.

An available translation of Article 706-96 is as follows: "Application of technical means can be resorted to for the purposes of, without consent of the concerned person, capturing, fixing, transmitting, and recording private or confidential speeches of one or more people, in private or public places or vehicles, or images of one or several people in a private place."

(FPPL) that have been created and the new paragraphs that are proposed for amending Articles 230-36[5] and 706-97[6] of the FPPL.

One point that deserves particular attention is that, the use of remote activation can provide accessibility without distinction to almost every kind of system, such as all types of technological devices, specifically messaging applications in mobile devices, microphone and sound applications for facilitating the usage of these devices (e.g., Siri), the newest models of cars, location services, smart watches, and data that can be remotely accessed. Hence, different from other protection measures such as using a different device for capturing sounds and images regarding clarifying an investigation about a suspect, remote activation will eliminate time wasted while positioning this device in the best location with regard to a suspect being investigated by the prosecution. This is because access to this type of electronic data will be achieved through the use of certain regulations and infrastructural applications that are intelligence-based in nature.

Article L811-3 of the French Internal Security Code stipulates that intelligence-based operations may be exercised for national independence, for maintaining territorial integrity and national security, and for preventing terrorism and organized crime. The subsection titled "Eavesdropping on Certain Places and Vehicles and Collecting Electronic Data" concretely regulates the intelligence methods that require official

[5] An available translation of Article 230-36 is as follows: "In order to perform remote activation of the electronic device mentioned in Article 230-34-1, the prosecutor of the Republic or the investigating judge can appoint all the physical and legal persons authorized and registered in one of the lists foreseen in Article 157. The prosecutor of the Republic or investigating judge can also prescribe resorting to state means subjected to secrecy of the national defense according to forms foreseen in Chapter I of Title IV of Book I."

[6] An available translation of Article 706-97 is as follows: "When remote activation of an electronic device has been decided by applying Article 706-96-2, the decision shall include all the elements that permit identification of this device."

permission in Section III of this code. Pursuant to Article L853-1, if intel that is needed for illuminating the prosecution cannot be obtained through any other methods permitted by law, technical means that enable eavesdropping on communications which are classified as private or confidential or that enable obtaining, summarizing, conveying, or recording of images of a private place can be authorized. Moreover, this article also covers authorization for trespassing in a private place.

Pursuant to the same section of Article L853-2 regarding electronic data, access to electronic data that is stored in an electronic system may be recorded, stored, and conveyed as long as information cannot be obtained through any other means. Relying on these two provisions, legal arrangements can be seen to have been made that enable audio and visual material to be captured by remote activation, as well as electronic data involving geolocation if the legally required conditions are satisfied, especially for terrorism and organized crime. These provisions should be noted as having been adopted for intelligence services, not for criminal investigations. Given that these provisions cannot be addressed for criminal investigations, the intention has been made to create such an amendment, as will be shown below.

I. DATA OBTAINED THROUGH REMOTE ACTIVATION AND VIOLATING THE RIGHT TO RESPECT FOR ONE'S PRIVATE LIFE

Lawyers have taken the proposal to utilize all sorts of electronic devices as investigation tools to be considerably serious such extent that the Paris Bar Association on May 17, 2023 shared its opinions on this proposal that had been sent to the Senate on May 3, 2023. The Paris Bar Association made a legal assessment regarding the right to a fair trial and violation of privacy. In its opinion, it defined these amendments as "significant modifications in penal procedural code which reinforce competences of investigation agents and prosecution to the detriment of the guarantees of the essence of the right to

respect for privacy of private life and defence rights" in order to point out potential breaches of the most fundamental principles laid and preserved in the FPPL.[7]

Considering that remote activation applies to all electronic devices,[8] this measure constitutes a grievous intervention in the principle of respect for private life, one which cannot be justified by the protection of public order. Furthermore, when no prohibitions exist for collecting these types of data, defense rights may also be hindered due to eavesdropping on the communications between lawyers and their clients.[9]

In particular, the facts that this method is not restricted in time, that night searches have been extended to such a degree that the principle of prohibition of night searches became almost inexistent for *in flagrante delicto*, and that judicial police are entitled through remote activation to locate suspects as well as capture their sounds and images, notably in case of terrorism and organized crimes, demonstrates that these provisions have been drafted in conflict with the "Constitution, the European Convention for the Protection of Human Rights and

[7] Avocats Barreau Paris, Communiqué du Conseil de l'Ordre (May 17, 2023), https://www.avocatparis.org/communique-du-conseil-de-lordre.

[8] We think that the expression "obtaining evidence from electronic devices by recording sound and image and geolocation" should cover all kinds of technical means that allow one to go beyond the boundary of a human's capacity to perceive.

[9] Some of these concerns are subsequently mitigated by the Senate's extended exception list; see: Assemblée Natıonale-Rapport (June 23, 2023) Tome II, pp. 164–165. Despite the rights violations, some argue that remote activation should be included in the code. The parliamentary debates from June 23, 2023 in particular underlined the necessity of remote activation. As for geolocation data, this was suggested as already being present in the code; however, due to the emphasis on placing a GPS tracker making the police force's duty more difficult, trackers being no longer as functional and able to be destroyed quickly, and police officers taking risks while placing a tracker, supporters of the proposal suggested that the possibility of police officers being exposed to harm ought to be taken into consideration. See Assemblée Natıonale-Rapport (June 23, 2023) Tome II, pp. 120–122.

Fundamental Freedoms, and the European Union Charter of Fundamental Rights."[10]

Even in terms of the fight against crime and criminals, accessing electronic devices that have become central to people's lives, their location data, and any level of sounds and images using mobile applications through remote activation cannot comply with the principle of the right to privacy of private life, of which all people are endowed upon birth and is deemed sacred under Article 8 of the ECHR.[11] If one approaches the problem from the angle of private life being restricted, this measure is seen to infringe upon the very essence of this right and the purpose it aims to protect. Moreover, this situation may cause this measure to become a legally rooted violation of other fundamental principles and individual rights.

In this regard, the approach of the ECtHR concerning the application of these provisions, as well as Article 8 of the ECHR concerning data captured through remote activation and violation of privacy of private life, has particular importance.

According to rule of law, individuals are granted a life space where they can develop and shape their physical and spiritual existence as they wish. Article 12 of the Universal Declaration of Human Rights, Article 17 of the International Covenant on Civil and Political Rights,[12] and Article 8 of the ECHR explicitly

---

[10] Avocats Barreau Paris, Communiqué du Conseil de l'Ordre (May 17, 2023), https://www.avocatparis.org/communique-du-conseil-de-lordre.

[11] Goodison, Sean E., Robert C. Davis, Brian A. Jackson. "Digital Evidence and the U.S. Criminal Justice System." A Project of the RAND Corporation (2005): p. 5; Pfeifle, Anne, Alexa, "What Should We Do about Privacy: Protecting Privacy for Users of Voice-Activated Devices", Washington Law Review vol. 93, no. 1 (March 2018): p. 424.

[12] Article 17 of the Convention stipulates "No one shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence, nor to unlawful attacks on one's honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." Namely, privacy of private life is guaranteed.

stipulate that individuals have a free space where they are protected against state interventions.

As noted in the ECHR, party states are not allowed to adopt any measure they consider appropriate for the sake of espionage and the fight against terrorism. Furthermore, if they plan to adopt some measures, they are obliged to foresee sufficient and effective guarantees against possible abuses.[13] Competences for the secret observation of citizens can only be justified to the extent that they are necessary for the protection of democratic institutions.[14] An intervention in a fundamental right must be pertinent and rely on sufficient cause. In addition, it must pursue a legitimate aim and be commensurate with this aim.[15] Therefore, any restrictions of human rights should be accompanied by legitimate purposes in such a climate where technology develops new instruments for espionage and monitoring activities and where states seek to prevent terrorism and organized crime.[16]

The sole existence of a legal ground that permits an internal system to secretly monitor carries the risk of being observed by anyone to whom this provision is applicable.[17] Although national law makers have a certain margin of appreciation in deciding which monitoring system is needed, party states to the ECHR do not have limitless initiative in submitting people under their sovereignty to secret monitoring.

This monitoring similarly constitutes an intrusion into private life when state agents systematically collect and store data about certain individuals, even if they are collected from

[13] (Weber and Saravia v. Germany, § 106).

[14] (Klass and Others v. Germany, § 42; Szabó and Vissy v. Macaristan, §§ 72–73).

[15] (Segerstedt-Wiberg and Others v. Sweden, § 88).

[16] (Klass and Others v. Germany, § 36).

[17] (Weber and Saravia v. Germany, § 78).

public places and concern solely professional or public activities.[18]

Placing a GPS device in someone's car to store data concerning places they have been and data on their activities in public places amounts to an intervention in private life.[19] Cases where national law does not explicitly mark the boundaries of the extent of initiative is granted to authorities nor the form measures take with regard to collecting information about people's private lives and how it is stored in a database, especially when no minimum guarantee is foreseen against possible abuses, violates the right to respect for private life as stated under Article 8§1 of the ECHR.[20]

As shown above, national legislation must stipulate sufficiently precise, effective, and comprehensive guarantees regarding how monitoring measures are ordered and executed using potential indemnity provisions. The condition of "necessary in a democratic society" shall be interpreted to cover two situations: firstly, all measures as a general requirement shall protect democratic institutions; secondly as a special requirement, they must be absolutely necessary for obtaining important intelligence in an operation.[21] A secret monitoring measure that does not satisfy these necessary conditions becomes open to abuse by authorities.

---

[18] (Peck v. United Kingdom, § 59; P.G. and J. H. v. United Kingdom, §§ 57–59, Amann v. Switzerland [BD], §§ 65–67; Rotaru v Romania [BD], §§ 43–44).

[19] (Uzun v. Germany, §§ 51–53).

[20] For a case in which the name of an applicant had been recorded in a Monitoring Database that had collected travel information (by train or plane) in Russia, see Shimovolos v Russia, § 66).

[21] (Szabó and Vissy v. Macaristan, §§ 72–73). The court decided that communications and telephone conversations (including from the workplace and home) were covered by the concept of private life and communication pursuant to Article 8. (Halford v. United Kingdom, § 44; Malone v. United Kingdom § 64; Weber and Saravia v. Germany, §§ 76–79).

Another point that deserves attention is that, because technological devices are becoming more and more sophisticated, the rules regarding these matters need to be more detailed.[22]

One can reach the same conclusion for monitoring, metering, and eavesdropping on telephone communications in the context of an ongoing prosecution, and a breach of Article 8 emerges in such a case as well. A lawmaker who uses the term "complying with law" in the wording of provisions in national law does not imply solely the national law but also the international law with which one must comply.[23] As for secret monitoring activities conducted by public authorities, an individual ought to be protected against an arbitrary intervention in their rights under Article 8.[24] In addition, legal rules must have clear wording to such an extent that individuals can comprehend under which conditions and in which cases public authorities may resort to such secret measures. Interventions amount to a breach when no legal system exists regulating the usage of a bug and when related guidelines are neither binding nor publicly accessible.

Concerning the utilization of modern scientific techniques in criminal justice, their extensive usage at any cost may ruin the equilibrium between their potential advantages and the right to private life. Hence, the protection assured by Article 8 may be unacceptably undermined.

A breach of other's private lives may emerge in penal procedural law system as well due to remote activation. Because all sorts of communication may possibly be pertinent for any criminal case, and sounds and images must be analyzed multiple times in ongoing trials just to determine their relevance to a case,

[22] (Kruslin v. France, § 33).

[23] (Halford v. United Kingdom, § 49).

[24] (Khan v. United Kingdom, §§ 26–28).

remote activation may become problematic for suspect's private life. Furthermore, given that different people's data may be captured by the same data pool, data of those who are not suspects in a case may be processed while implementing the measure.[25]

The fact that no restrictions exist on how data are to be processed aggravates the breach even further. The idea suggesting that individual privacy and tracking geolocation may violate freedom of movement is worth discussing in the face of public interests. Despite the fact that protection of public order is the central principle in the preamble of the proposal, these methods are criticized as they are too intrusive into private life to be justified in any case. A similar criticism was made on June 23, 2023 during parliamentary discussions to underline rights and freedoms breaches: "Do we have to go until the point that technology allow us even if the measures contradict freedoms?"[26]

In 1967, the USA Supreme Court decided that, because electronic secret eavesdropping "involves an extensive intervention to privacy by its nature," it can be allowed only under "precise and distinctive conditions." As a consequence, the New York state administration cancelled the eavesdropping code that did not comply with these parameters, serving as an example of the contradictory nature these measures have with respect to rights and freedoms.[27]

II. AMENDMENT PROPOSALS FOR MITIGATING BREACHES OF PRIVATE LIFE AND DEFENSE RIGHTS

The Senate proposed certain modifications to the text on the proposal to mitigate the effects of potential violations due to

[25] Kardell, Nicole. "Remote Search Warrants and the Continued Threat to Privacy Rights." (December 2014): 1 https://www.ifrahlaw.com/crime-in-the-suites/remote-search-warrants-continued-loss-privacy/

[26] Assemblée Natıonale-Rapport (23 juin 2023) Tome II, p. 120.

[27] Kardell 2014, 2.

remote activation for geolocation and obtaining audio-visual material.[28] In order to understand the proposed restrictions, one can analyze the context of some of the professions that hold prominent roles in public office and look at special regulations for the practices of their professions. For instance, electronic devices belong to those who are obliged to keep professional secrets, and the devices where these people live or work cannot be subjected to remote activation.[29] Similarly, transcribing the communications captured by this method is prohibited to avoid possible violations. These limitations did not exist in the first version of the proposal and were subsequently added after the evaluations in the Senate. We should further note that such restrictions are necessary for lawyers and judges to achieve coherency with other relevant provisions of FPPC. One should also bear in mind that eavesdropping by those who hold judicial professions to such a degree constitutes an obvious violation of the principle of rule of law.

Thanks to technological developments, electronic data produced by devices has been exponentially enlarged in quality and quantity. Therefore, they have become useful instruments for shortening the procedural process for decisions rendered within a reasonable time as a component of the right to a fair trial, for finding suspects in serious crimes such as terrorism and organized crime, and for reestablishing public order that has become derailed due to committed crimes. By relying on these motivations, proposals have expressed the need for new and special investigation instruments in the penal procedural law of civil law jurisdictions, and various points of view have been reflected therein. The Parliamentary Opinion Report prevailingly suggested that resorting to remote activation is

[28] Some criteria shall be satisfied for restrictions on rights and freedoms to be lawful see The Impact of Pegasus on Fundamental Rights and Democratic Processes, European Parliament (January 2023): p. 55.

[29] Assemblée Natıonale-Rapport (23 juin 2023) Tome I, 21.

useful for fighting against ever better large-scale organized crime in terms of research and investigation.[30]

III. HOW THE VARIETY OF DATA OBTAINED THROUGH REMOTE ACTIVATION INFLUENCES PERSONAL DATA PROTECTION

The extent of electronic data that is obtained through remote activation method can cover a wide range of content, such as emails, sounds, images, personal health information, and credit card and account information shared with online shopping sites. In relation to protecting the relevant contents, the possessor implicitly expresses that they have no consent to access to their information by using password security methods. In this context, we shall note how the practice being discussed in this article carries the risk of a breach of personal data as a sub-branch of private life.[31]

Remote activation may possibly cause personal data breaches as a result of certain measures such as identifying suspects' IP addresses. Regarding this matter in comparative law, the Federal Constitutional Court remarked in one of its decisions on inventorying data information that once it has settled the procedure concerning personal data, the legislative organ shall create legal grounds for the collection and conveyance of these data. The court further emphasized that, unless this data is essential for investigation and prosecution, a breach of fundamental rights will absolutely not be justified.[32]

A similar proposal able to exemplify this discussion is in regard to research warrants in Article 41 of FPPL. Because courts can order arrest warrants solely for people and properties within its jurisdiction pursuant to Article 41 of FPPL, the competence of investigative agents is restricted to suspects based only on

[30] Assemblée Natıonale-Rapport (June 23, 2023) Tome I, 167.

[31] Ceffinato, Tobias, Aktuelles-Internetstrafrecht, JuS 2021, 311, BeckOnline, 13.

[32] Ceffinato 2021, 25.

"particular situations," even if they have been subjected to a criminal charge. This can be accepted as a benchmark of the importance of the principles of legal certainty and privacy as requirements of the rule of law.[33]

Regarding "ordering search warrants that allow searching computers and other electronic storage mediums when location is hidden through remote activation" in *Riley v. California*, the dictum of the USA Supreme Court, which stipulates "searching a modern electronic device such as a smart phone or computer means even a higher level of intervention to privacy than a comprehensive search of a house," explains the seriousness of the danger intervention in privacy has to breach the relevant proposal of Article 41 and, by analogy, the FPPC proposal.[34]

One should bear in mind that the proposal of a federal code has an aspect that permits stored data to be confiscated regardless of court jurisdiction. Although saying that the amendment proposal for Article 41 has completely cancelled the application of the former version would be untrue, the amendment does not seem to comply with the spirit of the code in terms of breaches when the purpose of the amendment is acknowledged as not violating other constitutional and legal rules.

IV. COMPARISON BETWEEN PRESENT INVESTIGATION INSTRUMENTS AND SPECIAL INVESTIGATION INSTRUMENTS

The present version of the code stipulates that, when research and investigation are so required and the state needs to be protected, the prosecutor and investigating judge may order the utilization of geolocation technics in the classical sense for crimes with sentences of two or more years of imprisonment and can order the capture of sounds and images using classical

[33] Kardell 2014, 1, Pfeifle 2018, 425.

[34] Kardell 2014, 2; Goodison-Davis-Jackson 2005, 11; Pfeifle 2018, 426.

technics with respect to the special offences set forth in the code. Nevertheless, remote activation methods for the purposes of geolocation and obtaining sounds and images are distinct from traditional methods. By taking these differences into consideration, the Commission has used its competence to offer modifications to the presented proposal by foreseeing new guarantees to these measures.[35]

Guarantees for geolocation activities. To conduct geolocation classically, the offense must involve a sentence of at least three years if a bug is to be placed by trespassing onto a private vehicle garage, private property, or vehicles on public or private roads. If a bug is to be placed by entering any other private place, the offence in question must involve a sentence of at least five-years imprisonment. However, remote activation requires at least a sentence of ten-years imprisonment.[36] Secondly, this measure can only be ordered after judicial scrutiny. A trial judge is the competent authority for ordering a remote activation. Depending on the stage of the trial, either the Prosecutor of the Republic, a freedoms and detention judge (JLD; *juge des libertés et de la détention*), or the investigating judge can order this method to be applied. A judge is obliged to include details concerning "clarification of all of the characters that serve identification of the targeted device," and as a third limitation, this method cannot be applied to lawyers or judges.[37] As for duration, this measure can be renewed for an additional 15 days to 1 month under the authorization of a JLD. Under the authorization of the investigating judge, remote activation can

[35] Assemblée Natıonale-Rapport (June 23, 2023) Tome I, p. 21. For the traditional and new monitoring methods, see The Impact of Pegasus on Fundamental Rights and Democratic Processes, European Parliament (January 2023): 19 et seq.

[36] See footnote 2.

[37] Assemblée Natıonale-Rapport (June 23, 2023) Tome I, 159.

be resorted to for a renewable four months and a maximum of one year, or a maximum of two years for organized crime.[38]

Guarantees for recording sounds and images. The present FPPC allows classical eavesdropping and image obtainment methods as a "state measure subjected to national defence" using technical equipment to be orderable by the prosecutor or investigating judge, whereas remote activation can be ordered only with judicial authorization. With respect to the duration, remote activation can be ordered for a period not exceeding six months.

When comparing geolocation through remote activation, this measure is more intrusive to freedoms; therefore, regarding capturing sounds and images through remote activation, not only are the devices people use excluded, but devices found in certain specific places are excluded from transcription. For instance, the offices of people in charge of judicial duties, press companies, and doctor clinics are excluded. The last paragraph of the new Article 706-96-3 also stipulates that the judge who had authorized the techniques for capturing sounds and images shall order the data that cannot be transcribed to be destroyed as soon as possible under the conditions foreseen in Article 706-95-14.[39]

Based on this background, we should note that the communications and activities of those people unrelated to the conduct or people under investigation that is obtained while recording sounds and images through remote activation is referred to as inadvertent evidence or accidental evidence in penal procedural law. No provision exists concerning accidental evidence that has been obtained from secret monitoring measures while recording sounds and images on electronic devices or accessing electronic devices for geolocation data through remote activation. The lack of regulations regarding

[38] Assemblée Natıonale-Rapport (June 23, 2023) Tome I, 162.

[39] Assemblée Natıonale-Rapport (June 23, 2023) Tome I, 173

evidence that is obtained unrelated to the subject matter of investigation but that raises suspicion of the commission of another offence may result in the emergence of unlawful consequences.

V. TRANSBORDER APPLICATION OF REMOTE ACTIVATION

One should be aware of the fact that obtaining evidence from electronic devices by recording sounds and images and accessing electronic devices for geolocation data regarding terrorism and organized crime also concerns international criminal law. Offenses in this regard may be revealed through significantly crucial electronic data that must be acquired by the police force in the international sphere. Therefore, both the nationalities of suspects and the criteria of the competent courts where the crime has been committed shall be taken into consideration.[40]

As much as these aforementioned modern technologies and opportunities of the globalized world have allowed for the idea of establishing a cloud computing system for use in cross-border criminal trials[41] to satisfy the need of accessible information and the globalization of criminal evidence as a consequence of this situation, investigations have also become more and more comprehensive. Timely access to the electronic data service providers keep has become a basic component of governmental

[40] Abraha, Halefom H. "Regulating Law Enforcement Access to Electronic Evidence Across Borders: The United States Approach." *Information & Communications Technology Law*, vol. 29, no. 3 (2020): 326.

[41] "*Cloud computing is the on-demand availability of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the user. Large clouds often have functions distributed over multiple locations, each of which is a data center. Cloud computing relies on sharing of resources to achieve coherence and typically uses a pay-as-you-go model, which can help in reducing capital expenses but may also lead to unexpected operating expenses for users.*". See https://en.wikipedia.org/wiki/Cloud_computing (date of access: 21.08.2023)

efforts at protecting public security and fighting against serious crimes such as terrorism.

Terrorism and organized crime can be subjected to international cyber investigations. Evidence requests regarding these crimes cannot usually reach the requesting countries in a timely manner; therefore, international mutual cooperation treaties are applied to overcome this problem (i.e., Mutual Legal Assistance Treaty [MLAT]). Without a treaty, the police force should be noted to be unable to access data from another country remotely. Otherwise, this could be interpreted as a violation of the principle of equality of sovereign states and of the sovereignty rights of states in broader terms.[42]

The most problematic issues for prosecutions in the cyber domains are identifying the offenders, their contacts, and the content of their communications. The first method that comes to the mind is IP control.[43] Nonetheless, due to anonymization methods used by suspects and the utilization of systems that designate dynamic IPs, the intended results cannot always be achieved by IP control.[44] Thus, the development of new prosecution methods is required.

The sole treaty that succeeded with respect to unification regarding the collection and obtainment of electronic evidence with particular regard to cybercrimes is the Council of Europe's Convention on Cybercrime, also known as the Budapest Convention. Having been drafted by taking individual rights and freedoms into consideration as well as interventions in privacy, the Convention obliges party states to comply with

---

[42] Osula, Anna-Maria. "Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study." *International Journal of Law and Information Technology* vol. 24, no. 4 (Winter 2016): 345.

[43] As long as IP addresses involve electronic traffic data, these data can be remotely accessed if legal conditions are fulfilled pursuant to the German Penal Procedural Code (StPO) § 100g. See Ceffinato 2021, 13.

[44] Ceffinato 2021, 13.

certain regulations in order to mitigate the unsolicited effects of possible violations. The Convention's provisions that are directly applicable to domestic laws should not hinder states' positive obligations regarding guaranteeing fundamental rights and freedoms and preventing breaches.[45]

Article 19 of the Convention allows access, storage, and search of data in computer systems at the national level. Article 32(b) permits transnational access to another person's computer system using remote activation with the consent of the domestic authority. Seeking data on location is exclusive to party states and geolocation.

Fundamental rights and freedoms shall not be violated, even in cases where cross-border remote activation tools are used for sound and image recording or for geolocation data.

Some regulations exist in comparative law with regard to obtaining digital evidence through the use of technical equipment. In order to prevent violations, the Estonian Penal Procedural Code (EPPC) with its strict application measures stipulates that, if "technical equipment is used for collecting evidence," involved parties shall be notified of this technique and its purpose beforehand. Given that monitoring via remote activation – eavesdropping, access to data, capturing images – carries the urgent risk of intervention to fundamental rights, this method can only be resorted to as a last remedy.[46]

In the Netherlands Penal Procedural Code, searching and storing a system from somewhere else can only be authorized if it is mandatory for unveiling the truth.

In Article 110 titled "Examination of Electronic Storage Mediums" of the German Penal Procedural Code, Paragraph 3 prescribes the presence of a mutual legal assistance treaty to be required for using remote activation to access data not located in

[45] Osula 2016, 346.

[46] Osula 2016, 354.

Germany.[47] The German Federal Head Prosecution Office has stated this provision to solely allow access to data, not to the modification or spoiling of data.[48]

CONCLUSION

The proposal that foresees an amendment to the FPPC intends to regulate the methods for remote activation that supplements the classical means of geolocation, as well as for sound and image recording, by implementing additional limitations and guarantees. This proposal allows police forces to be able to access data and location information from electronic devices in use by persons through the new and modern investigation tool of remote activation, especially in relation to investigations concerning terrorism and organized crime. Although this proposal aims at public interest, explicit and severe violations of individual fundamental rights and freedoms may occur if public interest cannot justify the utilization of such a measure.

Secret monitoring measures that collect evidence by collecting sound and image recordings from electronic devices and that permit access to electronic devices for geolocation through remote activation should only be authorized if they clearly function to protect democratic institutions. Control of technical monitoring must be addressed under exceptional cases. This method should be applied when needed in democratic societies for national security and/or for protecting

[47] "Durchsicht von Papieren und elektronischen Speichermedien" Strafprozeßordnung (StPO) § 110/3: "Nach Maßgabe der Absätze 1 und 2 ist auch die Durchsicht von elektronischen Speichermedien bei dem von der Durchsuchung Betroffenen zulässig. Diese Durchsicht darf auch auf hiervon räumlich getrennte Speichermedien erstreckt werden, soweit auf sie von dem elektronischen Speichermedium aus zugegriffen werden kann, wenn andernfalls der Verlust der gesuchten Daten zu befürchten ist. Daten, die für die Untersuchung von Bedeutung sein können, dürfen gesichert werden."

[48] Weisburd, Kate, Sentenced to Surveillance: Fourth Amendment Limits on Electronic Monitoring, 98 N.C. L. REV. 717 (2020): 727.

order or preventing crime. However, for these precautions to be in compliance with the convention, they must be endowed with effective guarantees. States shall not be granted a wide margin of appreciation regarding which method to use. Guarantees that will serve compliance with Article 8 may vary depending on the conditions of the case; for instance, they can involve the qualities of potential measures, their scope and duration, the reasons that necessitate these measures, which competent authorities are allowed to carry it out, its practice and monitoring, and appeal options in national law. Because the necessary guarantees are not present for avoiding abuses when obtaining evidence from sound and image recordings and geolocation data from electronic devices through remote activation for the purposes of national security, protecting order, and preventing crime, we should indicate that the French proposal presumes significant restrictions such as violations of privacy of private life and of defense rights. As a matter of fact, when taking into consideration the technical developments in espionage and monitoring methods alongside the rise of terrorism in Europe, the ECtHR has concluded that the German regulation regarding the control of secret monitoring satisfies the prerogatives of Article 8.

Electronic devices have become an inseparable part of human routines and are used in almost every sector; hence, these devices contain unimaginably large data sets about people's private lives. Accessing this information without the knowledge of the concerned people, as well as breaches of the principle of privacy of private life, while matching possessed data with the purpose of an investigation using the trial-and-error method goes against the principle of states' respect for fundamental rights and freedoms. Moreover, keeping in mind that the people around the targeted person would likely be affected by these monitoring activities, the intrusive character of remote activation methods should be reduced at both the national and cross-border levels.

In order to strike the right balance between states' interests in protecting national security with secret monitoring measures and the seriousness of intervening in the right for respect of citizens' private lives, national authorities have a discretionary power to some extent in choosing the instruments for achieving the legitimate purpose of defending national security. Nonetheless, sufficient and effective guarantees must be found against abuses. Therefore, lawmakers must take into consideration conditions such as the character of measures, their scope and duration, which competent authorities will have permission, and how these methods are practiced and supervised, as well as the paths for appeals as recognized by national law.

Lastly, we can indicate that the methods to be addressed for balancing the right to respect for private life with effective investigations can avert eventual violations by determining frameworks for the duration and by cataloguing which crimes and the people to whom these measures may be applied.

REFERENCES

Abraha, Halefom H. "Regulating Law Enforcement Access to Electronic Evidence Across Borders: The United States Approach." *Information & Communications Technology Law*, vol. 29, no. 3 (2020): 326.

Assemblée Natıonale-Rapport (23 juin 2023) Tome I.

Assemblée Natıonale-Rapport (23 juin 2023) Tome II.

Avocats Barreau Paris, Communiqué du Conseil de l'Ordre (17 mai 2023), https://www.avocatparis.org/communique-du-conseil-de-lordre.

Ceffinato, Tobias, Aktuelles-Internetstrafrecht, JuS 2021, 311, BeckOnline.

Goodison, Sean E., Robert C. Davis, Brian A. Jackson. "Digital Evidence and the U.S. Criminal Justice System." A Project of the RAND Corporation (2005).

Kardell, Nicole. "Remote Search Warrants and the Continued Threat to Privacy Rights." (December 2014). https://www.ifrahlaw.com/crime-in-the-suites/remote-search-warrants-continued-loss-privacy/.

Osula, Anna-Maria. "Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study." International Journal of Law and Information Technology vol. 24, no. 4 (Winter 2016): 343–373.

Pfeifle, Anne, Alexa. "What Should We Do about Privacy: Protecting Privacy for Users of Voice-Activated Devices", Washington Law Review vol. 93, no. 1 (March 2018): 421-458.

The Impact of Pegasus on Fundamental Rights and Democratic Processes, European Parliament (January 2023).

Weisburd, Kate, Sentenced to Surveillance: Fourth Amendment Limits on Electronic Monitoring, 98 N.C. L. REV. 717 (2020).

Hakem Değerlendirmesi: Çift kör hakem.

Finansal Destek: Yazar bu çalışma için finansal destek alıp almadığını belirtmemiştir.

Çıkar Çatışması: Yazar çıkar çatışması bildirmemiştir.

Etik Kurul Onayı: Yazar etik kurul onayının gerekmediğini belirtmiştir.

Peer Review: Double peer-reviewed.

Financial Support: The author has not declared whether this work has received any financial support.

Conflict of Interest: The author has no conflict of interest to declare.

Ethics Committee Approval: The author stated that ethics committee approval is not require