 DOI: https://doi.org/10.15388/PhDStudentsConference.2023.6

THE CONVERGENCE OF JUDICIAL AND ADMINISTRATIVE INVESTIGATION TECHNIQUES IN FRENCH LAW

Antonin Guillard[1]

Keywords: repression, prevention, criminal procedure, intelligence law, investigation technique, privacy.
Abstract. Unsurprisingly, some of the prerogatives of the judicial police and the intelligence services are common. This is the case of human sources. Other acts, particularly those involving deprivation of liberty or intrusion into private life, are usually the responsibility of the judicial police. The commission of an offence and the control of the judicial authority justify restrictions on fundamental rights. This pattern is now disrupted because intelligence law is copying privacy-invasive mechanisms from the criminal procedure code. The convergence of these fields also has an interactive character, since techniques specifically developed for preventive law have recently been borrowed by repressive law. The legislator therefore uses the investigative techniques of each field to improve the other. This movement has an increasingly competitive character which seems to benefit the intelligence services. At this point, they have the most complex and intrusive acts at their disposal, which erodes the distinction between preventive and repressive action.

INTRODUCTION

French legal system knows a major distinction (Loi des 16-24 août 1790) (Code du 3 brumaire an IV) between administrative and judicial polices[2] (Matsopoulou, 1996, p. 17). The identification of their respective domains is mainly based on a finalist criterion[3] (Picard, 1984, p. 143) established by the State Council (Conseil d'Etat, Section, 11 mai 1951). An administrative police operation occurs when a general surveillance mission is conducted. In contrast, a judicial police activity is carried out when the operation's object or goal is to seek a precisely defined offence. In the first case, it's mostly a preventive objective which is followed whereas, in the second case, it's more generally a repressive finality.

The knowledge of a public order disturbance constituting a criminal offence and the search of information about the offender motivates the recourse to mechanisms interfering with liberties. Intrusive and especially coercive acts are in principle excluded in administrative law because the

1 PhD candidate, Paris Nanterre University, Faculty of Law, Penal Law and Criminology Center (CDPC-EA 3982), with a dissertation on "Criminal procedure and intelligence : a study of the hybridization of repression and prevention". antoninguillard@gmail.com, ORCID i-D : 0000-0002-8696-1763.

2 Starting from the etymology of police, Haritini Matsopoulou explains that "the term police etymologically derives from the greek word polis (city) which means 'art of governing the city'".

3 According to Etienne Picard, the finalist criteria can be used to overcome the difficulties resulting from the application of formal and material criteria. It was developed by the government commissioner Delvolve and taken up by the High Administrative Court in its judgment of 11 May 1951.

position of the suspect on iter criminis[4] is less advanced (Parizot, 2015). The person may think about the offence, may elaborate it in various ways but there is no sufficient manifestation of an action against a protected social value. The Constitution also states that restrictions on personal liberty must be authorized by the judicial authority (Article 66 de la Constitution du 4 octobre 1958). This notion included violations of privacy (Conseil constitutionnel, Décision n° 76-75 DC, 12 janvier 1977) until the constitutional Council adopted a stricter interpretation (Conseil constitutionnel, Décision n° 2013-357 QPC, 29 novembre 2013). This case law has paved the way for administrative competence over some intrusive measures.

On this basis, the legislation has been giving to the judicial police a "clear advantage in terms of investigative capacity"[5] for a long time (Vadillo, 2018, p. 58). It has thus integrated several technical investigative measures since the beginning of the 21st century (Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice…) in order to fight organized crime (Pradel, 1998, p. 57). These acts are characterized by their confidentiality, intrusion into privacy, complexity and efficiency. Without drawing up an exhaustive list, it is possible to mention geolocation (Article 230-32 du code de procédure pénale), access to connection data (Articles 60-2, 77-1-2, 99-4 du code de procédure pénale) or access to stored correspondence (Articles 706-95-1, 706-95-2 du code de procédure pénale).

The techniques of administrative prevention of threats to the Nation's fundamental interests[6] have been kept in an "embryonic" state during this phase of judicial growth (Desaulnay, Ollard, 2015). Intelligence services had few prerogatives[7] (Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances…) and sometimes operated in the silence of law (Deprau, 2017, p. 35). Intelligence law was nevertheless improved from the second half of the 2000s to avoid this pitfall and to respond to the terrorist threat[8] (Touillier, 2017a, p. 160). Access to connection data for the prevention of terrorism[9] (Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme…) and geolocation of mobile terminals[10] (Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire…) have thus been authorized.

Now, reading the dispositions of the criminal procedure code and the interior security code relating to investigative acts leaves a strange feeling of proximity. Some authors state that it's "normal" for the administration to use intrusive procedures (Latour, 2018, p. 431). Others even point out that "it's rather believed" that particularly intrusive techniques are "the prerogative of the intelligence services" (Vadillo, 2018, p. 58). This is surely not a reversal of the role assigned to each police but perhaps an overlapping of them or "the emergence of a 'para-criminal' procedure" (Touillier, 2017a, p. 159).

4 It is the author's path from conceptualisation of the offence to its consumption.

5 Floran Vadillo explain that this position is derived from a study of constitutional case law.

6 This notion is present in book IV of the penal code, but it also has an administrative application in articles L. 801-1, L. 811-1 and L. 811-3 of the interior security code.

7 This is the case of the security interceptions.

8 Marc Touillier used the notion of "sprouts" to describe the development of intelligence law before the law of 24 july 2015.

9 See Article 6 of the law and L. 34-1-1 of the posts and electronic communications code.

10 See article 20 of the law.

The most effective way to check this is to compare the approved procedures in the two domains[11]. It will be necessary to look at their definition and legal regimes. This will allow us to determine the nature of the interactions between the disciplines. Is one field particularly inspired by the other? Is there a complementarity between them? Can we talk about mutual influences? Can the notion of competition be used to describe the respective development of legal frameworks?

We will proceed in three steps. First, we will have to look for the influences of the criminal procedure code on intelligence law. Second, it will be interesting to see if administrative law is also a source of inspiration for repressive law. Finally, we will try to identify the (temporary ?) overtaking by intelligence law on the most complex and intrusive operations.

1. THE APPROPRIATION BY ADMINISTRATIVE INTELLIGENCE OF JUDICIAL INVESTIGATION TECHNIQUES

The lawmaker often looks for ways to extend the scope of investigation acts in the criminal procedure code. To achieve this, it has three quite effective levers. To begin, some procedures are reserved for the "instruction" phase under the control of the "instruction" judge, which provides greater guarantees[12]. Parliamentarians have extended their scope by authorizing them in the investigative phase while the case is considerably less mature[13] (Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice…).

Then, the use of certain acts is only possible to prosecute offences listed in the criminal procedure code and committed by organized groups (Articles 706-73, 706-73-1 du code de procédure pénale). The legislator increases their range by extending the lists of offences[14] (Loi n° 2015-993 du 17 août 2015 portant adaptation de la procédure pénale…). The last channel for parliament to develop the field of investigative measures is the most contested. The idea is to transpose acts reserved for the fight against organized crime into ordinary law[15] (Conseil constitutionnel, Décision n°2019-778 DC, 21 mars 2019).

On the sidelines of these mechanisms, which only concern the criminal procedure code, a new channel of diffusion seems to be open since 2015 (Delmas-Marty, 2015) (Loi n° 2015-912 du 24 juillet 2015 relative au renseignement). For a part of the doctrine, the "penal coloration" of intelligence techniques remains "unavowed" or even "rejected" (Touillier, 2017a, p. 163) with the support of the constitutional Council (Conseil constitutionnel, Décision n° 2015-713 DC, 23 juillet 2015). In his

11 The study of procedural safeguards could also be interesting, but it should be done as a separate study. The same is true about the finalities of intelligence, which seems to be gradually moving into areas usually covered by judicial action.

12 This phase should not be confused with the investigation. She is mandatory for felonies and optional for misdemeanors.

13 Example of correspondence interceptions opened to investigation in the fight against organized crime.

14 Example of sound recording and image fixation with the creation of article 706-73-1 of the criminal procedure code.

15 The reticence of the constitutional Council must be considered. Example of the category of "other special investigation techniques", whose extension to all crimes in the project n° 463 de programmation 2018-2022 et de réforme pour la justice was censured by the constitutional Council in paragraphs 164 to 166 of its decision.

view, the new legislation is "a purely administrative issue"[16]. However, the parliament's intelligence delegation has advised that judicial techniques should be "transposed" (Délégation parlementaire au renseignement, Rapport n° 2482 et n° 201, 2014, p. 87) into administrative law[17] and after welcomed their integration into this field[18] (Délégation parlementaire au renseignement, Rapport n° 3524 et n° 423, 2016, p. 29). An examination of two of them confirms this hypothesis.

First, access to computer data is framed by the criminal procedure code since 2011[19] (Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure) and by the interior security code since 2015[20] (Loi n° 2015-912 du 24 juillet 2015 relative au renseignement). The name of the technique is the same in both legal instruments (Article 706-102-1 du code de procédure pénale. Article L. 853-2 du code de la sécurité intérieure). The way it is executed is also described in a similar way. It takes place at distance or on the spot without the knowledge of the involved person. Regarding the information collected on the targeted terminals, the drafting of the texts is once again comparable. The data concerned are those stored in the system but also those displayed on the screen, entered via the keyboard and transmitted or received by the devices. If the system needs to be installed in a private place outside the legal search hours, the judge of freedoms and detention is competent to deliver the authorization (Articles 59, 706-102-5 du code de procédure pénale). The interior security code is even stricter because it requires a special procedure if a private place or a vehicle is concerned (Article L. 853-3 du code de la sécurité intérieure).

The proximity of the legal systems leaves no doubt, although it should be kept in mind that there are still some differences. A principle of subsidiarity must be respected in administrative law and the agents and the authorities responsible for control are different[21]. The defence of the identity of the legal systems must be set aside in favour of the idea of "quasi-gemellity" (Roussel, 2016, p. 520) which is reinforced by the study of another investigation technique.

Second, the criminal procedure code has allowed the recording of sounds and images of certain places and vehicles since 2004[22] (Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice…). The interior security code has replicated this concept since 2015[23] (Loi n° 2015-912 du 24 juillet 2015 relative au renseignement). It is once again a secret operation, this time based on the use of a miniaturized device able to record and transmit data (Article 706-96 du code de procédure pénale. Article L. 853-1 du code de la sécurité intérieure). In both legal systems, this includes private or confidential speech in any place and images from a private place or from a vehicle. As for the access to computer

16 Paragraph 9 of the décision.

17 These included sound and image recording, access to computer data and infiltration.

18 Excluding infiltration.

19 See article 36 of the law.

20 See article 6 of the law.

21 Intelligence law refers to intelligence officers, whereas repressive law refers to judicial police officers. Control is granted by the Prime minister, an independent administrative authority and the State Council in the interior security code. It is based on the judicial judge in the criminal procedure code.

22 See article 1 of the law.

23 See article 6 of the law.

data, special rules apply in judicial cases when the surveillance concerns a private place outside the legal search hours (Article 706-96-1 du code de procédure pénale). In the administrative field, the control is once again reinforced as soon as the surveillance is done on a private place or on a vehicle (Article L. 853-3 du code de la sécurité intérieure).

The specificities mentioned earlier are also valid for audio and image fixing technique. Despite this, there are important similarities between them which show that intelligence services have borrowed intrusive procedures from the criminal procedure code. However, the relationship between the systems seems less and less unilateral. Indeed, it appears that the legislator is now adopting dispositions from the interior security code for the benefit of repressive law.

2. THE INSPIRATION OF CRIMINAL PROCEDURE BY INTELLIGENCE LAW

Intelligence law is not a simple copy of the criminal procedure applied to organized crime and terrorism. Some techniques such as IMSI-catcher have no judicial roots[24] (Loi n° 2015-912 du 24 juillet 2015 relative au renseignement). Judges and investigators have noticed this situation and have protested against these disparities in favour of the preventive services (Capdevielle, Popelin, Rapport n° 3515, 2016, p. 96). In their opinion, it was not understandable that the powers available to track down offenders were less than those available to prevent threats from occurring.

The government[25] (Projet de loi n° 3473 renforçant la lutte contre le crime organisé…, 2016) and parliamentarians (Mercier, Rapport n° 491, 2016, p. 55) were sensitive to this argument and they have supported the inclusion of IMSI-catcher in the criminal procedure code[26] (Loi n° 2016-73 du 3 juin 2016 renforçant la lutte contre le crime organisé…). This concept describes "a fake mobile relay tower that replaces, in a specific area, the operator's relay towers, allowing the services to have information on the terminals that are connected to them" (Bas, Rapport n° 460, 2015, p. 83). Part of the doctrine has welcomed this atypical interaction of preventive law with repressive law in a rather positive way[27] (Dreyer, 2016, p. 39). It was seen as an essential rebalancing to prevent a devaluation of the criminal investigations. However, some hesitations persist because difficulties noted in the interior security code have been partly transposed into the criminal procedure code[28] (Touillier, 2017b, p. 312).

24 See article 5 of the law. This procedure is inspired by United States law.

25 See article 2 of the law.

26 See article 3 of the law.

27 According to Emmanuel Dreyer, "We can be satisfied that, from now on, the judicial police have the same surveillance techniques as the intelligence services, which are part of the administrative police. There was no reason to restrict the access of the judicial police to these techniques, while their necessary and proportionate nature was affirmed, as regards the administrative police, in view of the "new threats" affecting our country".

28 According to Marc Touillier, the legislator has "more recently chosen to pick new numeric investigation techniques, such as IMSI-catcher, directly from the administrative arsenal even if their regulation raises questions".

Thus, the legislator did not consider it necessary to define the name of the investigation measure. It simply used the generic term "technical device"[29], without referring to the notion of IMSI-catcher. This terminology is criticized because it doesn't exactly identify the electronic devices that could be used to execute the surveillance (Commission nationale consultative des droits de l'Homme, 2015, p. 9). The modalities of execution are quite similar and less contested. The computer system takes advantage of a vulnerability in the 2G network[30] (Larrive et al., Rapport d'information n° 3069, 2020, p. 109) to force mobile terminals to reveal their international mobile subscriber identity and other information. Both legal regimes provide for the detection of connection data[31] (article L. 851-6 du code de la sécurité intérieure. Article 706-95-20 du code de procédure pénale) and the content of correspondence under stricter rules (Article L. 852-1 du code de la sécurité intérieure. Article 706-95-20 du code de procédure pénale). In this case, the time limits for authorization are two days renewable once in both systems[32]. On the contrary, the time limits for the collection of other information are different. One month, renewable once, during the judicial investigation and four months, renewable for a maximum of two years, during "instruction" (Article 706-95-16 du code de procédure pénale). Administrative surveillance is limited to two renewable months without a maximum number of renewals. However, a maximum number of simultaneous operations is set for access to connection data (Article L. 851-6 du code de la sécurité intérieure) (Commission nationale de contrôle des techniques de renseignement, 2020, p. 21).

Despite their specific characteristics, there is a concurrent convergence between the legal frameworks. It is possible to speak about convergence because the same mechanisms are allowed in both domains. Their definitions are identical and their regimes have many similarities. It is also appropriate to speak of a concurrence since a competition for the most modern and complex measures is under way[33] (Ribeyre, 2016). New developments in one area are quickly taken up by parliamentarians to the benefit of the other area under the influence of certain practitioners (magistrates, investigators, intelligence officers). In this dynamic supported by the government, intelligence seems to progressively take the lead.

3. THE INTELLIGENCE TAKEOVER ON THE MOST COMPLEX AND INTRUSIVE ACTS

A group of five techniques recognized by the interior security code is not included in the criminal procedure code. The surveillance of international electronic communications (Article L. 854-1 du code de la sécurité intérieure) does not really seem to interest the judicial services. Apart from the

29 It is mentioned in the articles 226-3 of the penal code, L. 851-6 and L. 852-1 II of the interior security code, 706-96 of the criminal procedure code.

30 Note the risks of efficiency loss caused by the deployment of 5G network.

31 This includes the identification of a terminal equipment (IMSI) or the subscription number of its user and data relating to the location of a terminal equipment.

32 Renewal is limited to one time. There is no specification in administrative law.

33 For Cédric Ribeyre, this movement represents "an escalation in the growth of intrusive powers".

case of international operational cooperation, their competence is limited to the Republic territory[34]. On the opposite, the other procedures could contribute to the conduct of criminal investigations. Even if some members of parliament deny it (Délégation parlementaire au renseignement, Rapport n° 3524 et n° 423, 2016, p. 29), interceptions on certain radio networks (Article L. 855-1 A du code de la sécurité intérieure), satellite interceptions (Article L. 852-3 du code de la sécurité intérieure), immediate access to connection data (Article L. 851-2 du code de la sécurité intérieure) and algorithms (Article L. 851-3 du code de la sécurité intérieure) are able to provide clues to investigators.

The intelligence services have an advantage over the judicial police services because they are the only ones to use these mechanisms which have two characteristics. On the one hand, they are complex because they require high-performance computers and assistance of specially qualified agents. On the other hand, they are intrusive because they allow access to the content of communications or to large data flows analysed in real time. The study of algorithm is the best illustration of the loss of gradation between preventive and repressive investigation acts.

This technology allows for generalized surveillance of traffic[35] on networks with software that acts as a filter (Abiteboul, 2015). "Behavioural parameters, keyword parameters" (Roussel, 2016, p. 520) and other pre-determined criteria permit "automated processing"[36] to detect activities presenting a terrorist threat. The intrusiveness of this device is counterbalanced by what some deputies call an "especially strict legal framework" (Gauvin, Kervran,Rapport n° 4185, 2021, p. 82). Indeed, it is authorized on an experimental basis[37] (Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme…), only for the prevention of terrorism, for the benefit of specialized intelligence services (Article L. 811-2 du code de la sécurité intérieure), for a renewable period of two months (Article L. 851-3 du code de la sécurité intérieure) and without revealing the identity of the persons concerned except when a threat is identified. On this point, national and European case law on the conservation of connection data must be considered[38] (Cour de justice de l'Union européenne, La Quadrature du Net et autres, 6 octobre 2020) (Conseil d'Etat, Assemblée, 21 avril 2021) (Bertrand, 2021, p. 175).

The National Digital Council has nevertheless alerted the legislator of the uncertain reliability of this technique which has been tested with difficulty in the United States (Conseil national du numérique, 2015, p. 1). Its efficiency is very dependent on the criteria governing the operations of the system. For the doctrine, it marks a loss of human control over investigations. Suspicion can be based on an "equation" leading to a "quasi-certainty" (Latour, 2018, p. 431) of the detectives. The result of algorithmic analysis can be perceived as infallible. This can lead intelligence officers to neglect the

34 Note also the specificities linked to the Schengen convention.

35 These are the connection data mentioned in article L. 851-1 of the interior security code and the full addresses of resources used on the internet.

36 The notion of algorithm is not included in the interior security code which uses the term "automated processing" in the article L. 851-3.

37 See article 15 of the law.

38 According to the European Court of Justice, general and undifferentiated retention of traffic and location data is allowed for the defense of national security. It's conditioned on the identification of a serious threat to national security which must be actual or predictable. Renewal of the authorization is possible only if the threat persists. Control by a judge or an administrative authority with binding powers is required.

clues provided by other investigative methods. Prevention also seems to become prediction (Latour, 2018, p. 431). It's no longer a question of following a dangerous person but a question of searching a mass of data to find indications of a potential attack. These doubts reduce the probability of algorithm extension to the criminal procedure code in a near future. The intelligence services have access to a more invasive instrument than judicial techniques, even though they are only responsible for threat prevention. The use of this process is still quite limited for the moment due to its complexity and cost[39] (Larrive et al., Rapport d'information n° 3069, 2020, p. 39).

CONCLUSIONS

Finally, there are three levels of communication between preventive and repressive law which alter their specificities. The privacy-invasive acts of the criminal procedure code are used by the legislator to develop intelligence law which has been neglected for a long time. Some quite new measures allowed to prevent violations of public order are included in repressive law to avoid an imbalance of the disciplines. These mutual inspirations are turning into a form of race towards the most complex and efficient procedures. The latest reforms give to the intelligence services an advantage to use techniques whose real effectiveness and control remain to be demonstrated.

These exchanges have two major consequences. On a theoretical level, the occurrence of a crime is no longer the determining criterion for the use of techniques affecting liberties. The prevention of threats to the Nation's fundamental interests allows the recourse to acts which are not subject to judicial control and which strongly affect the right to privacy. On a practical level, the division of procedures over time is less clearly defined. A preventive procedure can continue for more time because it's no longer necessary to initiate a judicial procedure to execute intrusive investigations. The discovery of an offence should normally put an end to preventive investigations, but the risk of procedures overlapping and conflicts of competence between the different services cannot be excluded.

List of sources

Legal acts

1. Code du 3 brumaire an IV.
2. Constitution du 4 octobre 1958.
3. Loi des 16-24 août 1790.
4. Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, JORF, n° 162, 13 juillet 1991.
5. Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, JORF, n° 59, 10 mars 2004, texte n° 1.
6. Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, JORF, n° 0020, 24 janvier 2006, texte n° 1.

39 The technique is still not used very often. It has only been authorized three times between 2015 and 2020.

7. Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, JORF, n° 0294, 19 décembre 2013, texte n° 1.

8. Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, JORF, n° 0171, 26 juillet 2015, texte n° 2.

9. Loi n° 2015-993 du 17 août 2015 portant adaptation de la procédure pénale au droit de l'Union européenne, JORF, n° 0189, 18 août 2015, texte n° 2.

10. Loi n° 2016-73 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, JORF, n° 0129, 4 juin 2016, texte n° 1.

11. Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, JORF, n° 0255, 31 octobre 2017, texte n° 1.

12. Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, JORF, n° 0176, 31 juillet 2021, texte n° 1.

Books and articles

1. Bertrand B., « Chronique droit européen du numérique - Les enjeux de la surveillance numérique », RTD eur., 2021.

2. Buisson J., Guinchard S., Procédure pénale, LexisNexis, 13e éd., 2020.

3. Deprau A., Renseignement public et sécurité nationale, Thèse soutenue à l'Université Paris-II Panthéon-Assas, 2017.

4. Desaulnay O., Ollard R., « Le renseignement français n'est plus hors-la-loi - Commentaire de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement », Droit pénal, n° 9, 2015, Etude 17.

5. Dreyer E., « Bas les masques : retour à la loi du plus fort ! », Gazette du Palais, n° 27, 19 juillet 2016.

6. Forcade O., Warusfel B. (dir.), Le droit du renseignement, La Documentation française, 2020.

7. Latour X., « Sécurité intérieure : un droit « augmenté » ? », AJDA, 2018.

8. Lejins P., « La police, la technologie moderne et les droits de l'Homme », Colloque sur les méthodes scientifiques de recherche de la vérité, Abidjan, 10-16 janvier 1972, RIDP, 1972.

9. Matsopoulou H., Les enquêtes de police, LGDJ, Bibliothèque des sciences criminelles, 1996.

10. Parizot R., « Surveiller et prévenir... à quel prix ? Loi n° 2015-912 du 24 juillet 2015 relative au renseignement », JCP G, n° 41, 5 octobre 2015, Doctrine 1077.

11. Picard E., La notion de police administrative, LGDJ, publications de l'Université de Rouen, 1984.

12. Pradel J., « De l'enquête pénale proactive : suggestions pour un statut légal », Recueil Dalloz, 1998.

13. Ribeyre C., « Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale. Et maintenant ? », Droit pénal, n° 9, septembre 2016, Etude 17.

14. Roussel G., « Le régime des techniques de renseignement », AJ Pénal, 2015.

15. Touillier M., « La loi sur le renseignement traduit-elle l'émergence d'une procédure « para-pénale » ? », in Touillier M. (dir.), Le code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre ?, Dalloz, Les sens du droit, 2017a.

16. Touillier M., « Lumière sur un arsenal de lutte contre une délinquance tapie dans l'ombre », AJ pénal, 2017b.

17. Vadillo F., « Techniques d'enquête numérique judiciaire : les défis d'une survie dans la modernité », Enjeux numériques, n° 3, 2018.

18. Verges E., « Procédure pénale : La procédure pénale au temps des confluences », RSC, 2018.

19. Verny E., Procédure pénale, 6e éd., Dalloz, 2018.

20. Warusfel B., « Les nouveaux enjeux du cadre juridique du renseignement », in Conan M., Thomas-Tual B. (dir.), Annuaire 2016 du droit de la sécurité et de la défense, Mare & Martin, 2016.

21. Warusfel B., « La (re)définition d'un droit du renseignement », in Alix J., Cahn O. (dir.), L'hypothèse de la guerre contre le terrorisme, Dalloz, Thèmes & commentaires, 2017.

Case law

1. Regional courts decisions

1.1. Cour de justice de l'Union européenne, La Quadrature du Net et autres, 6 octobre 2020, C-511/18, C-512/18, C-520/18.

2. National courts decisions

2.1. Conseil constitutionnel, Décision n° 76-75 DC, 12 janvier 1977.

2.2. Conseil constitutionnel, Décision n° 2004-492 DC, 2 mars 2004.

2.3. Conseil constitutionnel, Décision n° 2015-713 DC, 23 juillet 2015.

2.4. Conseil constitutionnel, Décision n° 2013-357 QPC, 29 novembre 2013.

2.5. Conseil constitutionnel, Décision n° 2019-778 DC, 21 mars 2019.

2.6. Conseil d'Etat, Section, 11 mai 1951, Consorts baud.

2.7. Conseil d'Etat, Assemblée, 21 avril 2021, n° 393099.

Others sources

1. Abiteboul S., « Le renseignement numérique pour les nuls », Binaire, 9 avril 2015.

2. Bas P., Rapport n° 460 fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale, Sur le projet de loi, adopté par l'Assemblée nationale après engagement de la procédure accélérée, relatif au renseignement et sur la proposition de loi organique présentée par MM. Jean-Pierre Raffarin et Philippe Bas, relative à la nomination du président de la commission nationale de contrôle des techniques de renseignement, enregistré à la Présidence du Sénat le 20 mai 2015.

3. Capdevielle C., Popelin P., Rapport n° 3515 fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, Sur le projet de loi n° 3473 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, enregistré à la Présidence de l'Assemblée nationale le 18 février 2016.

4. Commission nationale consultative des droits de l'Homme, Avis, Sur le projet de loi relatif au renseignement dans sa version enregistrée le 1er avril 2015 à la Présidence de l'Assemblée nationale, 16 avril 2015, JORF, n° 0171, 26 juillet 2015, texte n° 43.

5. Commission nationale de contrôle des techniques de renseignement, 5ème rapport d'activité, année 2020.

6. Conseil national du numérique, Communiqué de presse, Renseignement : le Conseil national du numérique s'inquiète d'une extension du champ de la surveillance et invite à renforcer les garanties et les moyens du contrôle démocratique, 19 mars 2015.

7. Délégation parlementaire au renseignement, Rapport n° 2482 et n° 201 relatif à l'activité de la délégation parlementaire au renseignement, année 2014, remis à la Présidence de l'Assemblée nationale et du Sénat le 18 décembre 2014.

8. Délégation parlementaire au renseignement, Rapport n° 3524 et n° 423 relatif à l'activité de la délégation parlementaire au renseignement, année 2015, remis à la Présidence de l'Assemblée nationale et du Sénat le 25 février 2016.

9. Delmas-Marty M., « La démocratie dans les bras de Big Brother », Le Monde, 10 juin 2015.

10. Gauvin R., Kervran L., Rapport n° 4185 fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, Sur le projet de loi n° 4104 relatif à la prévention d'actes de terrorisme et au renseignement, enregistré à la Présidence de l'Assemblée nationale le 20 mai 2021.

11. Larrive G., Kervran L., Mis J.-M., Rapport d'information n° 3069, Sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement, enregistré à la Présidence de l'Assemblée nationale le 10 juin 2020.

12. Mercier M., Rapport n° 491 fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale, Sur le projet de loi n° 3473 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, enregistré à la Présidence du Sénat le 23 mars 2016, tome I.

13. Projet de loi n° 3473 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, enregistré à la Présidence de l'Assemblée nationale le 3 février 2016.

14. Projet de loi n° 463 de programmation 2018-2022 et de réforme pour la justice, texte adopté n° 232 en troisième lecture à l'Assemblée nationale le 18 février 2019.

15. Untersinger M., « Que sont les IMSI-catchers, ces valises qui espionnent les téléphones portables ? », Le Monde, 31 mars 2015.