Digital criminal investigation techniques: Modernity and survival

Floran Vadillo,
associate researcher at IRM (Bordeaux University), former adviser to the Garde des Sceaux

Abstract:
The techniques used by criminal investigators in France have been neglected politically and overlooked by industry and the media. They have to be adjusted to new forms of criminality, adapted to the digital environment and modernized, whence three nearly vital challenges: an ontological challenge, for reasons of survival, for criminal investigators to cope with the competition, both political and technological; a legal challenge owing to the state of legislation and case law; and the technological challenge of modernization and project management.

When imagining state-of-the-art techniques for departments of criminal investigation,[1] we generally think of fingerprints, DNA tests and, for the most technology-minded among us, wire-tapping, the surveillance of communications or even behavior prediction software. Few among us would mention IMSI catchers,[2] Trojan horse programs, geolocation (by telephony or tags) — equipment used, we imagine, by intelligence services.

The techniques used to conduct criminal investigations in France are the neglected child of politics, industry and the media. To cope with new forms of criminality and to modernize and adapt to the digital environment, departments of criminal investigation have to take up three nearly vital challenges: the ontological challenge of coping with the competition (both political and technological); a legal challenge owing to the state of legislation and case law; and the technological challenge of modernization and project management.

[1] This article, including any quotations from French sources, has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references.
This translation maintains the distinction between "administrative police" and "judicial police", the latter often translated as "criminal investigators" or "department of criminal investigation". For a general description of the types of police in France, see https://en.wikipedia.org/wiki/Law_enforcement_in_France#Judicial_police English-speaking

[2] Material for intercepting a SIM card's international mobile subscriber identity (**IMSI**) and the international mobile equipment identity (IMEI).

Stiff political and technological competition

In France, the institutional system makes a top-level division between the "judicial police" and "administrative police", as the Constitutional Council has steadfastly recalled: the first has the assignment of "*establishing the facts of a given penal offense, […] pursuing perpetrators, […] gathering evidence*" whereas the second is to "*keep law and order, put an end to disturbances that have already broken out and […] prevent offenses*".[3] This separation is supposed to make these two types of police complementary. The Constitutional Council has long seen to this distinction but while granting a clear advantage to the "judicial police" for conducting criminal inquiries (in particular, into the private lives of individuals under investigation): all the necessary safeguards can apparently be inferred from the fact that this police is under the control of judicial authorities.

In March 2004, lawmakers diligently provided the "judicial police", criminal investigators, with a modern legal framework — modern in terms of technology.[4] An act of 10 July 1991 had already defined a legal framework for "interceptions", but the new act introduced in the Code of Penal Procedure special, useful techniques of investigation such as physical surveillance, undercover agents, or sound engineering. An act of 14 March 2011 on domestic security added the capturing of computer data, a provision updated by an act of 13 November 2014, which, given the scope of electronic communications and the social media, introduced in French law "pseudonymous investigations". Meanwhile, an act of 28 March 2014 had laid down the conditions for using geolocation techniques. Finally, an act of 3 June 2016 provided for using IMSI catchers to capture both metadata and communications.

This body of legislation comes out of laws that were voted to cover gaps in existing texts, to respond to unfavorable court rulings (as explained hereafter) and, too, to imitate foreign examples (in particular the United States). It stands out owing to its modernity and completeness in comparison with the lack of legal texts on the activities of the administrative police (apart from "administrative interceptions" authorized under the aforementioned act of 1991).

The emphasis on terrorism has slowly undermined this advance both legislatively and technologically. The necessity of preventing the perpetration of terrorist actions has shifted attention to the previously neglected administrative police and to domestic intelligence services. Faced with the impact of such attacks on society and in the media, political office-holders have preferred stacking legal arrangements on top of each other and maintaining competition between services — so many efforts for warding off accusations that they have not done enough. This explanation deserves more attention than it can be given herein. The legislation against terrorism, as it took shape between 1986 and 1996, gave priority to criminal investigations to the point of upsetting the top-level division made between the judicial and administrative police. This trend has been furthered by the dual qualification — administrative and judicial — of the services of domestic intelligence (DST, DCRI, and then DGSI) and by political office-holders evoking the work of intelligence services as proof of their commitment to fighting against terrorism.

The shift started with an act of 23 January 2006 "*on the fight against terrorism and diverse measures about security and border controls*". To the insufficient arsenal of measures available to intelligence services, this act added the possibility of collecting data on telephone connections for the purpose of geolocation. In the years thereafter, other measures followed, mainly about consulting files. Then, the armed forces program act of 18 December 2013 authorized real-time geolocation. Above all, an act of 24 July 2015 set up a full, modern legal framework for the

[3] "Commentaire de la décision n°2005-532 DC du 19 janvier 2006", *Les Cahiers du Conseil constitutionnel*, 20. Consultable at https://www.conseil-constitutionnel.fr/decision/2006/2005532DC.htm.

[4] Under an act of 9 March 2004 on adapting justice to trends in criminality, a bill of law presented by Dominique Perben, minister of Justice at the time. Texts of French law are available at https://www.legifrance.gouv.fr/Droit-francais.

activities of intelligence services.[5] Conceived as a balanced text on the activities of the judicial police, this act established a parity that had been deeply and durably thrown out of balance by the laws passed following terrorist attacks in November 2015 (in particular the legislation for prolonging the state of emergency). The disequilibrium wobbled even more when considerable investments in technology, as of 2008, enabled intelligence services to not only implement the provisions foreseen by the law but also to develop a high level of skills in decryption and informatics. The Interministerial Group of Control (GIC), which, under the prime minister's office, has the assignment of carrying out interceptions, soon became a major center of technology.

In contrast, the judicial police has never benefitted from such structures or means for implementing all the measures that have been voted for criminal investigations.[6] To illustrate the lag that has accumulated in spite of all this legislation: the measure for capturing computer data adopted in 2011 has not yet been implemented for want of investments and of the appropriate organization. To make up for this, the ministries of Justice and of Interior, after working together for several months, reached an agreement in March 2017 on the "spy software" offered to criminal investigators. This agreement provides for setting up a national technical service to capture data and develop computerized solutions for criminal investigators. After a long wait, this agreement has finally been published.[7]

Snags of the law and case law

Besides this political and technological competition with the administrative police, digital criminal investigation techniques are also subject to changes in the law (domestic or European) and case law. These changes often amount to snags that suddenly keep us from advancing.

The act of 10 July 1991 (the first of its kind) was adopted only after a ruling against France by the European Court of Human Rights that accumulated with similar decisions by the country's final Court of Appeals.[8] In a similar vein, the act of 28 March 2014 had suddenly become necessary owing to a decision by the final Court of Appeals declaring that geolocation techniques in criminal investigations lacked any legal grounds.[9]

Intrusions of privacy, even under the control of judicial authorities, have to satisfy strict conditions related, for example, to the intelligibility and predictability of the law and the existence of sufficient safeguards (the nature of the intrusion, its duration, the admissibility of evidence, etc.). Digital criminal investigation techniques are impeded by these snags that have cropped up out of needs, criticisms or gaps in the law. The instability of the body of law regulating these techniques has been a holdback. For instance, the act of 3 June 2016 considerably modified the conditions for using digital investigative techniques, but the future Ministry of Justice program act will make further modifications. A framework act will probably be missing that could unify procedural systems in order to simplify the general conditions for using digital investigative

[5] I was personally involved in this legislation with Jean-Jacques Urvoas, chairman of the National Assembly's Law Committee and rapporteur of the bill of law on intelligence. *Cf.* VADILLO F. (2012) "Une loi relative aux services de renseignement. L'utopie d'une démocratie adulte?", *Les Notes de la Fondation Jean Jaurès*, 130, 20p.

[6] Even thought the SIAT and IRCGN have experts capable of proving their mettle! SIAT: Service Interministériel d'Assistance Technique (SIAT) of the DCPJ (Direction Centrale de la Police Judiciaire, part of the Direction Générale de la Police Nationale). IRCGN: Institut de Recherche Criminelle de la Gendarmerie Nationale.

[7] Decision of 9 May 2018 available at: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000036887904&dateTexte=&categorieLien=id.

[8] Respectively: ECHR, 24 April 1990, Huvig & Kruslin c/France; and Cour de Cassation, plenary assembly of 24 November 1989, affair Baribeau; or Cour de Cassation, Criminal Chamber, 13 June 1989.

[9] Cour de Cassation, Criminal Chamber, 22 October 2013.

techniques and to make the system more stable without running the risk of technical obsolescence (objectives of the intelligence act adopted on 24 July 2015).

Although national law is decisive, it should not lead us to overlook the prime importance of European rules and regulations. The ruling by the Court of Justice of the European Union on 21 December 2016 was a harsh reminder of this, since it created confusion about how long telephone companies have to keep connection data and about the grounds for accessing the data.[10] This made it necessary to draft a new directive, now on the drawing board.

Moreover, only European law can prevent the digital giants (in particular, Facebook and Google) from evading requisitions from national courts of law by arguing that there is a conflict of legislation and that only American law is applicable. These firms too often choose the court orders to which they will respond (usually those related to child pornography and terrorism), even though they do not have this right to choose. It is necessary to foresee, at the European level, legal provisions for criminal investigations. Elsewhere, we have suggested:[11]

- forcing these firms to have a pool of encryption keys that investigating magistrates may request to access the data of individuals under surveillance;
- granting the status of electronic communications operator to certain firms (WhatsApp, Hangouts, Messenger, Skype…) in order for criminal investigators to be able intercept data; and
- considerably increase the sanctions for refusals to respond to requisitions (in particular, fines in proportion to the firm's sales).

Digital investigation techniques should be examined globally from a judicial viewpoint, at both the national and European levels, so as to guarantee their effectiveness and stability.

The technological challenge

The most evident challenge to criminal investigators is to keep up on technological trends instead of being pursued by them, as if by fate, and, above all, instead of falling ever farther behind. This could be an argument for relying exclusively on the administrative police, a shift that would upset the rules of evidence and the judicial system as it exists in France.

Digital investigatory techniques must be measured against three major trends.

The first is the generalized use of encoded electronic communications, a technique indispensable for protecting privacy. Nothing should be done to hamper or breach it (the "back doors" used by foreign intelligence services or criminal networks). However encoding electronic communications is a major impediment to criminal investigations. For example, 80% of intercepted data are encrypted, and this considerably restricts the ability of investigators to collect information useful for judicial proceedings. It is essential to improve for investigating magistrates the conditions of access to plaintext data. The acts of 13 November 2014 and of 3 June 2016 have opened to them the possibility to contact the DGSI's technical assistance center for decrypting software that is more robust than the programs offered by certain firms.[12] These initial efforts must now lead to a much broader reflection on placing at the disposal of these magistrates the means used by other state institutions to decipher messages (the legal framework of authorizations and controls, the admissibility of evidence, confidentiality including during proceedings). It is also essential to allow for "judicial Trojan horses" that can sidestep encryption and transmit to investigators the data directly entered at a terminal before they are sent.

[10] CJUE, 21 December 2016, Tele2.

[11] BERTHOUMIEU C., FARDE G., FOVEAU T. & VADILLO F. (2017) "Projet de loi Collomb. L'injustifiable agonie de nos droits", *L'Hétairie*, 22 September available via https://www.lhetairie.fr/single-post/projet-loi-collomb.

[12] CTA (Centre Technique d'Assistance) of the DGSI (Direction Générale de la Sécurité Intérieure): General Directorate for Internal Security. Article 230-2 of the Code of Penal Procedure.

The second trend is the processing and storing of big data. The legal framework for digital techniques of investigation along with the mass of files and of open sources (not to mention the foregoing reservation about decrypting data) have considerably limited the strategic value of data as such. Nonetheless, these factors have also underscored the problems of managing and analyzing big data. People spend too much time obtaining unsatisfactory results. All the data are not processed, and all prospects are not explored.

While intelligence services have slowly advanced on this question,[13] the judicial police cannot be spared making advances too. This calls for partnerships with firms based on guarantees about the indispensable "digital sovereignty" — a subject that is both strategic and legal (given the requirements of the rules of evidence). Any delay in making this decision inevitably results in a decisive technological lag.

Processing big data raises, of course, the sensitive question of data storage. Current rules of evidence do not allow for selecting the relevant data. This implies either having a storage capacity on par with the best social media (a solution out of reach and a source of malfunctions later on, such as those experienced by the National Platform of Judicial Interceptions, PNIJ) or modifying the law so that, by joint agreement with the parties to a case, only pertinent data are stored.

The third trend is linked to malfunctions in the state's conduct of big technological projects. As the director of DINSIC stated, "*We desperately lack, in the state, persons capable of heading projects, persons with a background in digital production processes. We have become clumsy when making purchases, because we are no longer able to clearly specify, negotiate or supervise suppliers. We must, therefore, work on human resources by bringing in new profiles, relearning how to design and steer big projects.*"[14] As a consequence, the state has to equip itself not by massively bringing back into its administration certain technological functions but by holding its own in dealings with industrialists and coping with technological progress.

This preoccupation led to setting up ANTENJ in April 2017.[15] Under a magistrate with solid experience in the fields of organized crime and criminal investigations, this new agency has a budget for setting up a "competence center" in the Ministry of Justice. The means appropriated make it a creditable reference for criminal investigators and corporate executives. This center is to become one of the major forces for coping with the trends (in particular technological) under way in this strategic domain. For the sake of justice, it must have the necessary means, in particular for conducting investigations. Technological progress is both a fabulous opportunity for efficiency and a major peril if the current lag were to widen.

Involving a mixture of considerations — political, strategic, legal and technological — this subject is utterly complex. It summons our imagination and responsiveness. It invokes a critical spirit that does not lead to desperation. And too, it evokes a certain idea of the state. The objective is to offer to criminal investigators the Alphonse Bertillon of the 21st century.[16]

---

[13] Evidence of this being the DGSI's recent acquisition of Palantir technology, or the Artémis Project launched by the Ministry of Armed Forces.

[14] VERDIER H. (2017) "Le vrai sujet: faire advenir l'État d'après la révolution numérique", *Chronik*, 19 December 2017 at https://chronik.fr/henri-verdier-vrai-cest-de-faire-advenir-letat-dapres-revolution-numerique.html.
DINSIC: Direction Interministérielle du Numérique et du Système d'Information et de Communication de l'État.

[15] Decree n°2017-614 of 24 April 2017 on creating a national service, the Agence Nationale des Techniques d'Enquêtes Numériques Judiciaires (ANTENJ) and a committee on digital techniques for criminal investigations.

[16] In 1882, Alphonse Bertillon (1853-1914) founded the first police laboratory for identifying criminals and applied anthropometry for this purpose. The "Bertillon system" was adopted everywhere in Europe, then in the United States. It was used in France till 1970.