In this case, the Marseille Gendarmerie's Research Section was reinforced by the SDAT (Anti-Terrorist Subdivision) […] under the vague notion of "extreme violence". The means at their disposal are considerable—telephony, wiretapping, physical surveillance, spyware, facial recognition, GPS tracking, etc.

No Trace Project / No trace, no case. A collection of tools to help anarchists and other rebels **understand** the capabilities of their enemies, **undermine** surveillance efforts, and ultimately **act** without getting caught.

Depending on your context, possession of certain documents may be criminalized or attract unwanted attention—be careful about what zines you print and where you store them.

The "Lafarge" Case

The Investigation Methods Used and Some Lessons to Be Learned

The "Lafarge" Case: The Investigation Methods Used and Some Lessons to Be Learned

Original text in French

Affaire "Lafarge" : Les moyens d'enquête utilisés et quelques attentions à en tirer

lesmoyens@systemli.org

2023

expansive.info/Affaire-Lafarge-Les-moyens-d-enquete-utilises-et-quelques-attentions-a-en-tirer-4130

Translation and layout

No Trace Project

notrace.how/resources/#lafarge

Note from the No Trace Project:

On December 10, 2022, between 100 and 200 activists invaded the Lafarge armaments factory in Bouc-Bel-Air, France, in a surprise daytime sabotage action that caused around 6 million euros in damage. This text presents the methods used by authorities to investigate this action. The sections "Some answers: practices to adopt" and "Resources" from the original text have not been reproduced here.

Contents

Conclusion

When it comes to security, it's tempting to give up quickly and assume that the police already know a lot and that there's no point in implementing this or that security practice.

Ongoing or completed investigations show that police officers, even the elite of the criminal investigation department, don't know everything, make mistakes, but are able to spend months or mobilize dozens of people to analyze large amounts of data. It is with classic investigation methods (video surveillance analysis, fadette analysis) that the police services feed their files the most. Using these investigative tools, the police draw up a first list of suspects, then suspect contacts and/or contacts of contacts. In general, many of the errors and clumsiness that lead them to suspect people can be corrected. The very advanced techniques that the police wanted to use (audio recording, spyware) still seem quite complex for them to put in place.

It seems important to us to succeed in implementing shared security practices. Developing a shared security culture means giving ourselves the means to understand risks, build trust, and integrate reflexes that protect both people and their ability to act. And these reflexes don't have to be overly burdensome! Using Signal instead of SMS, avoiding gossip and misplaced curiosity about who did what, getting into the habit of communicating sensitive information only with those who need it…

Without falling into the fantasy of permanent, omnipresent surveillance, we can also take a number of steps to protect ourselves from police tracking, while making sure it doesn't make our lives too miserable or prevent us from organizing ourselves collectively.

We are working on a more detailed analysis of these and other preliminary elements. You can reach us at lesmoyens@systemli.org.

Introduction

This text concerns the 35 arrests made on June 5 and 20, and in particular the 31 arrests related to the "decommissioning" of the Lafarge factory in Bouc-Bel-Air on December 10, 2022.

Two of these people were charged in early July. The following analyses are based on interviews with the arrestees, who were able to share information gathered during the hearings and in their interviews with the investigating authorities, and with the defendants, who are forbidden to contact each other.

They give us an idea of the lengths to which the State is willing to go to track down those who oppose ecological devastation. In this case, the Marseille Gendarmerie's Research Section was reinforced by the SDAT (Anti-Terrorist Subdivision), even though the acts were not characterized as terrorism, but only under the vague notion of "extreme violence". The means at their disposal are considerable—telephony, wiretapping, physical surveillance, spyware, facial recognition, GPS tracking, etc.

These means are not a reflection of the majority of investigations into political actions. Some are common, others much less so. In all likelihood, not all of them were used against all of the people targeted in the Lafarge case, but rather in a gradual manner, depending on the specific interest that a particular person seemed to represent for their investigation. To our knowledge, the use of all these tools is still relatively unique, complex, costly and therefore relatively rare.

Resisting surveillance protects us all. We'd like to see these bad experiences used to promote practices and a shared security culture, far beyond the people directly targeted by this investigation.

General Organization of the Investigation

The Marseille Gendarmerie Research Section was mobilized as early as the evening of December 10, 2022. Based on an initial analysis of CCTV footage, DNA, fingerprints and telephone records, an initial list of people suspected of having been present at the scene was quickly drawn up.

The SDAT was jointly assigned to the investigation. It obtained information on the sites/groups that had mentioned the December 10 action and sent requests to Twitter, Instagram and Facebook to obtain the identities associated with these sites and groups. After 14 days, the maximum time allowed for an investigation into a recent crime, a preliminary investigation is opened. Items for DNA sampling are sent to the forensic police for analysis, which takes some time. The analysis of video surveillance footage involves processing hundreds of hours of footage and therefore takes several months.

So, the first phase of the investigation, which was essentially based on on-the-spot research (video surveillance, analysis of the telephony at the scene and DNA sampling), was completed before the opening of the judicial investigation on February 2.

In the second phase, they tried to establish a second circle of people (close to the suspects) by studying "fadettes" (detailed telephone bills) and bank transfers, and sometimes, but only for a limited number of people, they used or requested the use of physical surveillance (tailing) or technical surveillance (GPS trackers, telephone tapping, spyware).

The data collected on the social circles of the initial suspects is compared with the initial findings of the investigation, so that certain people can be added to the list of suspects. Almost systematically, for each suspect, they search for their 5 most regular contacts, request their *fadettes* and, depending on the telephone activity observed (in

were accused of preparing violent actions against law enforcement personnel in France. One of the factors that triggered the investigation was a trip by one of the accused to Kurdistan to fight with the People's Defense Units (YPG), un groupe militant kurde en Syrie.

[18] *N.T.P. note:* On June 15, 2021, several people were arrested in France, including in the Creuse region, as part of an investigation into the burning of vehicles belonging to the French electricity company Enedis and a large TV and radio antenna.

Investigation Methods That Do Not Appear in the File at This Stage, but Exist Legally

We would like to briefly mention certain investigation methods that are not currently included in the file, but which are legal and are known to be occasionally used by investigative services such as the SDAT or the DGSI. In fact, the opening of a judicial investigation means, above all, a new investigative framework after the preliminary investigation, so the investigation continues.

At this stage, there is no evidence of the use of information obtained by undercover police officers or informants.

There is also no evidence of microphones hidden in homes or gardens. But this technique was used as part of a judicial investigation into an antenna arson in the Creuse region of France. It's also an intelligence technique: for example, a microphone was discovered in a photocopier at the Libertad anarchist social center in Paris. For an overview of these discoveries, including on a European scale, see Ears and Eyes[15].

At this stage, there is no trace of hidden cameras in front of or inside homes. However, such procedures have recently appeared against a member of the anti-bassines movement or collective spaces such as Les Tanneries or Les Lentillères in Dijon[16], without seeming to be part of an investigation for the time being. We can assume that this is a matter of intelligence gathering.

At this stage, there is no trace of spyware being introduced into computers. This was used in the 8/12[17] or Creuse[18] cases.

[15] https://notrace.how/earsandeyes

[16] https://dijoncter.info/surveillance-policiere-des-cameras-decouvertes-aux-tanneries-et-aux-lentilleres-4299

[17] *N.T.P. note:* On December 8, 2020, several house raids took place in France, as part of an anti-terrorist investigation against several people, some of whom

particular on the day of the alleged acts), decide whether or not to add new people to their list of suspects.

Finally, through surveillance and the study of various data sources, the police attempted to flesh out the files on the suspects, adding anything that could be used as a clue or that could establish links between the individuals, thus demonstrating the formation of an "organized gang".

Prior to arrests, but not systematically, they appear to have conducted physical surveillance, probably to confirm the residences of those under surveillance.

Investigation Methods

Investigation methods based on data collected on site

Searching for DNA and fingerprints

The National Guard conducted searches in the forest in a very large area around the factory, and various objects with DNA on them were recovered. According to the police, some of these samples "matched" DNA already registered in the FNAEG (Automated National File of Genetic Prints). DNA and fingerprints were found on a burned object and plastic wrapping.

The presence of DNA also allowed investigators to take someone into custody, who was subsequently removed from the case.

DNA that did not "match" was entered into the FNAEG database without being linked to an identity. If similar DNA is added at a later date, the individual's identity will be linked to the investigation.

DNA is inherently mobile and undated, meaning that no expert would be able to say whether it was present for one day, ten days, a month, whether it resulted from direct contact between the individual and the object or whether it was transferred, and finally, whether the object was transported by the person whose DNA was found or by a third party.

Requesting CCTV footage

Immediately after December 10, police officers requested footage from public transportation (buses, train stations, etc.), businesses, home surveillance systems and municipal cameras, all within an extended perimeter around the Lafarge site in Bouc-Bel-Air. Since CCTV footage is generally not stored for more than two weeks, the police needed to recover as much footage as possible in a short pe-

An up-to-date phone with a password/pin code of sufficient length greatly reduces the risk of unlocking a phone[13].

Taking DNA

During arrests, police officers insisted that arrestees wear surgical masks during transport for their own protection. These masks were then bagged and given to the forensic services. Toothbrushes, hairbrushes and underwear were also taken during the house raids. The underwear worn by a person who refused to wear a mask during transport was confiscated while in police custody.

The police offered one person to become a paid informant at the end of his police custody. The person obviously refused and was unable to find out how much money was involved or what the surveillance objectives were[14].

---

and even if it's recovered switched off. In this case, however, it asks the police to supply the device directly and charges quite a premium for the service.

[13] The police use the UFED device from Cellebrite (a cybersecurity company), a data "vacuum cleaner" that lists security flaws in all phone models and operating systems in use. It is the use of UFED that allows them to bypass the encryption systems of phones recovered switched on, but UFED also offers brute-force solutions for physical extractions or brute-force directly on the phone. The UFED is only used by specialized services: for police custodies at the SDAT, the Sub-Directorate for Cybercrime Control (SDLC) is mobilized; for custodies handled by the Gendarmerie, either the National Center for Digital Analysis in Cergy or the departmental cyber-threat operational sections carry out the analyses. Once the contents of the phone's memory have been made readable, this data is transmitted to the investigating services (SDAT or SR), in a file where the data is sorted by category (SMS, messages from encrypted messaging applications, photos, videos, audio recordings, etc.).

[14] In France, blackmail to obtain regular information on ZADs, squats, environmental and anti-fascist movements, etc., in exchange for supposed leniency or financial rewards, has been regularly carried out in police custody or other settings. All the more despicably, in recent years, migrants have been regularly blackmailed during appointments at the prefecture or in public places, to make them understand that they would have to provide regular information on groups and individuals with whom they might come into contact, in order to obtain papers or, on the contrary, to be deported.

the content of messages not yet deleted at the time of access, or by SIM card activity (SMS, unencrypted calls, and localization through antennas).

- The police were able to access the encrypted data of some smartphones when they were turned on, taking advantage of the security loopholes that exist when the phone is turned on. For phones that were found turned off, they also tried brute-forcing the password (attempting possible passwords until they find the right one). This can be done from the phone, but the system often imposes a delay between two attempts, making the technique extremely time-consuming. To get around this problem, police officers can extract the encrypted partition and try to brute-force it from a computer. Whether or not this is possible depends on the individual smartphone.

It should be noted that on recent Android phones, is doesn't seem to make much difference whether the phone is recovered turned on or off. On all Android phones, a physical extraction was performed, extracting the encrypted partition and keys, allowing a brute-force attack. On the iPhones (the latest being an iPhone SE 2020), the fact that the phone was turned on allowed the investigators to bypass the lock screen and not even need to bruteforce the password. An iPhone SE 1st generation (2016) that was recovered turned off could not be decrypted, even though police officers tried to brute-force the extraction they recovered from the iPhone's memory for 2 days[12].

[12]The iPhone's memory is encrypted by default. To decrypt it, two keys are required: one is derived from the user's password (often a 6-digit password), the other is a key physically embedded in the iPhone's electronic components and designed so that it cannot be removed from them. The first option for an attacker trying to access the memory would be to brute-force the iPhone's password directly using the phone. But the system imposes a delay between two attempts, which increases with each failed attempt. So brute-forcing a 6-digit password (which usually doesn't take long) becomes quite inefficient. The other option is to physically extract the iPhone's memory and brute-force it. But then they have to find both the password and the key that is physically embedded in the electronics. The latter is very long, so brute-forcing also becomes very long. Cellebrite, a company that provides French law enforcement agencies with forensic analysis tools, claims to be able to access data from any iPhone, even if it's up-to-date,

riod of time. They began by requesting and analyzing CCTV footage in the vicinity of the site, and expanded their requests to include footage along the routes they believed were taken by people who might have been involved in the action. In the first few weeks of the investigation, the police collected several hundred hours of video footage, which took several months to analyze.

As is often the case with CCTV footage, it should be noted that the images presented to people in police custody are of poor quality.

Facial recognition

Facial recognition software was used to compare images of people on buses or in an area relatively close to the site who were considered suspects with the TAJ (Criminal Record Processing) file, which contains identification photos taken during police custody.

Police officers also noted the clothing and bags worn by suspects they thought they recognized on CCTV images. During searches, they tried to find similar clothing/accessories.

Police officers from the Marseille Research Section also asked telephone operators for telephone data that had passed through antennas near the Lafarge site in order to identify people who had been on the site and thus possible suspects. We'll come back to this in the "Requesting Network Events" section below.

Telephony-based investigation methods

Much of this investigation is based on telephony. Investigators rely on the analysis of contacts and phone activity (location tracking) to create suspect profiles.

To establish these links, they sometimes analyze the phone activity of people who are totally uninvolved, which is why it is important to have shared practices that protect privacy. The various means are ordered from the most common (*fadettes*) to the less common (geolocation) to the most exceptional (spyware).

This analysis does not take into account any human factor, loaning one's phone, forgetting it, or technically anything related to load shedding, i.e. when an antenna needs to handle excessive traffic, mobilizing another antenna.

Study of fadettes *(detailed telephone bills)*

Fadettes are requested almost systematically when a number is of interest in an investigation—it's a tool to gather a very large amount of information. As they are not considered very intrusive in terms of privacy, their request does not need to be validated by a judge beforehand; it is made by an automated platform in contact with the operators, the National Platform for Judicial Interception (PNIJ). The results are obtained in a few minutes and cost a few euros per number. Our interviews led us to believe that more than a hundred numbers were requested in connection with the Lafarge case.

To communicate on the network, a phone must connect to antennas. To do this, it systematically communicates two pieces of information: its IMEI, which identifies the GSM chip, and the number of the SIM card (IMSI number). The *fadettes* include a table containing the following data:

- The IMEI: the unique number of the chip that allows the phone to communicate data, which makes it possible to identify its model. If your phone has 2 SIM slots, it has 2 IMEI numbers, which are not easy to associate.
- Communication type (SMS, call, data)
- Day and time
- The antenna through which this traffic passes
- The other party's number and the direction of the traffic (outgoing or incoming)
- Call duration or SMS size

Unless the phone has been tapped or spyware installed, it is not possible to know the content of calls/SMS or Internet traffic.

Fadettes are kept by the telephone operator for 1 year, so that police officers have access to data from the 12 months prior to their

tion of these two pieces of information made it possible to identify a person accused of taking the photos.

Investigation methods linked to arrests

House raids

During the house raids, police officers searched for clothing and accessories that appeared on the CCTV footage they used to identify the individuals. They also searched for digital equipment (computers, phones, USB sticks, hard drives), notebooks and other items that could be linked to the December 10 action. They also took items that could contain the suspects' DNA (toothbrushes, underwear, etc.).

Access to phone contents during and after police custody

Some smartphones could be decrypted by the Anti-Terrorist Subdivision (SDAT) or other police forces during police custody. Others have withstood the brute-force operations carried out during custody, but are likely to be subject to further attempts using other tools after custody.

In cases where investigators have been able to access the contents of phones that were in Signal groups with a large number of members, they have been able to access all the numbers in those groups, as well as disappearing messages that had not yet disappeared when the phones were taken.

- In cases where the Signal number is linked to a personal phone number that is used for civil bureaucracies, this allows investigators to directly identify the person to whom the number belongs. This person may be placed on file.
- If the Signal number is linked to a SIM card or a more anonymous number, they will have a number that can be entered into a file without reference to an identified person. However, investigators can try to identify a number by their Signal name, by

Requests for photos of vehicles at highway toll booths

Highway companies have been asked to provide photos of vehicles they are interested in at toll booths, so they can identify the occupants.

- To find out which vehicle and driver are transporting a person under investigation. If your phone is geolocated or you pay at the toll booth, the time window for photos to look at can be very narrow.
- To find out who the occupants are of vehicles known to have been used to go to a demonstration. They will requisition photos to try to identify the occupants of these vehicles.

Open-Source Intelligence

Of course, police officers search the Internet for texts, social media posts, speeches made at public conferences by groups they are investigating, and personal information about suspects. They also analyze television coverage of the invasion-sabotage of the Lafarge site.

Various critiques of *Soulèvements de la Terre*[11] that were published on militant websites seem to have been used by police officers to support their idea of a separation between "instigators" and "perpetrators" and to project roles implying specific guilt for some of those in police custody. These texts were also distributed to some of those in police custody, perhaps in an attempt to divide the accused during the hearings.

From the beginning of the investigation, police officers analyzed photos of the action against Lafarge published on the website of *Soulèvements de la Terre*, which contained metadata including the name and serial number of a camera. They asked the manufacturer to disclose the name of the buyer. The manufacturer provided the name of the store where the camera was sold. Within days, the combina-

[11] *N.T.P. note:* Mainstream media reported that some of the people arrested for the action against the Lafarge site were members of the political organization *Soulèvements de la Terre* ("Earth Uprisings"), which has publicly expressed support for the action.

request. Once a number has been requested, *fadettes* can be stored in the Criminal Analysis (AnaCrim) file for cross-checking with criminal investigations. Future investigations may therefore have access to *fadettes* older than 12 months.

Fadettes are used to:

- Analyze the breakdown between data and SMS/call traffic, enabling them to deduce, for example, the predominant use of messaging via the Internet.
- Create networks of connections between people who exchange SMS/calls, for example, assuming that two people know each other because they are in contact with the same person (these processes are facilitated by the software Analyst Notebook / AnaCrim).
- Track people's movements thanks to frequent data communications from a smartphone. Depending on which antennas are activated, they can deduce whether the person is traveling by train, car, or hitchhiking[1].

Requesting network events

Police officers can request a list of all communications made via an antenna between two dates. In Bouc-Bel-Air, for example, they requested all traffic that passed through the antennas near the Lafarge site between 12 pm and 8 pm on December 10.

Even when a phone isn't sending or receiving any telephone communications (SMS, MMS, calls, mobile data), it regularly exchanges information with nearby antennas, in particular so that the network knows where to send any communications the phone may receive (this exchange of information allows the phone to display a network

[1] The accuracy of the location derived from *fadettes* depends on the density of antennas in the vicinity. In rural areas, it's common to have only one antenna every 10-20 km, so being connected to that antenna will place you in a circle half that distance. In very dense urban areas, it's possible to have antennas from the same operator within 100 meters of each other, allowing for much greater precision in terms of movement. You can see the location and density of relay antennas here[2].

[2] https://antennesmobiles.fr

level, for example, which appears in the top right or left corner of the screen). This data is not considered "telephone communications", so it does not appear on the *fadettes*, and operators call it "network events[3]".

They therefore receive a list of phone communications (SMS, MMS, calls, mobile data), their senders, recipients and the IMEI numbers used. The amount of data is far too large to try to identify every single person in the vicinity. The gendarmes even compared a list of phone numbers of people who visited the ZAP occupation in Pertuis[4] with the list of phone numbers that passed near the Lafarge site. Then they asked for the *fadettes* of people who had visited the Pertuis ZAP, which they used to obtain their contacts, and compared the list of the ZAP and their contacts with the list of phones that communicated with the antennas near the Lafarge site.

Live geolocation

This investigative measure must be justified by the investigators and then validated by a judge. The phones of about twenty people targeted in the "Lafarge" case were geolocated in real time. The data collected is not necessarily analyzed by the investigating services, which suggests that this measure is sometimes taken as part of the

[3]Network events provide much more detailed information than *fadettes*: while in *fadettes* several minutes or hours may separate two communications (two lines), less than a minute separates each exchange of network events. As a result, investigators can know more or less to the second whether a person is present in the area covered by an antenna and whether they have moved to another antenna. A presence of only a few seconds in this area, or even a long presence but without any communication, will therefore be noticed with network events and not with *fadettes*. To obtain network events, police officers visit the site and take measurements to find out, for each of the 4 main operators, which antennas cover the area before requisitioning them. The operator Free does not record (or communicate) its network events. Like *fadettes*, network events are accessible for 1 year.

[4]*No Trace Project (N.T.P.) note:* In Pertuis, France, the ZAP ("Potatoes Zone") was a squat against the expansion of a business park, started in 2021 and evicted in 2022.

Surveillance devices

Request for a microphone in at least one vehicle.

A particularly intrusive investigative tool, hidden microphones can be used with a judge's approval, and can be installed in either a vehicle or a home. The goal is to capture speech, but the microphone installation does not appear to have been carried out yet.

Placement of GPS trackers under vehicles

At least 3 GPS trackers were used in the investigation. One arrestee found a tracker on his car after being released from custody, which is not currently mentioned in the file. These trackers are manufactured by the company Track Cars (known for selling such devices to French police forces).

Physical surveillance

Police officers have followed people on the street, on public transport and in their cars. This physical surveillance is used both to identify new suspects by noting the social relations of people under investigation, and to confirm an identity or to "house" a suspect (find someone's address, in police jargon), before a house raid.

Police officers also comment on behavior at public meetings. For example: so-and-so doesn't talk to so-and-so at such-and-such a public meeting, even though they know each other. They are therefore pretending not to know each other and are hiding something[10].

[10]It should also be noted that other recent investigative files—on the Sainte-Soline protests or the intelligence note on the Soulèvements de la Terre ("Earth Uprisings")—contain information and/or photos that probably stem from the presence of plainclothes policemen at occupations, rallies and public demonstrations.

- Banks, to check the banking activities of suspects (both individuals and associations), to obtain the names of the senders or recipients of transfers, to interpret withdrawals, or to make other requests to online shopping sites for details of purchases made from this account.
- Social networks, which can send them the IP addresses used to connect to or create the accounts under investigation. Requests were sent to Twitter, Facebook and Instagram accounts, but Facebook refused to provide this information.

It should be noted that several of the people targeted by these requisitions have had their bank accounts closed without explanation, or have undergone very thorough home inspections by the CAF. An unexplained closure of a bank account may therefore be a sign of surveillance.

The police say they don't send requests to Riseup due to concern that they'll warn the suspects, and considering that Riseup is unlikely to ever respond. This seems to confirm that using militant mail providers that implement a number of protections and encryption systems, such as Riseup, poses far more access problems for them than in the case of commercial providers[8]. (It goes without saying that the use of PGP encryption provides an additional layer of protection).

Data from Intelligence Services

There is mention of information from "partner services", a term that refers to different types of intelligence services: General Directorate for Internal Security (DGSI), Territorial Intelligence (SCRT) or Gendarmerie Intelligence (SCRCGN). Certain names thus appear in the file without it being clear where the police officers obtained them, and have given rise to questions in police custody, during hearings or "off the record".

[8]For example, Protonmail has already provided[9] the IP address used to create an account.

[9]https://paris-luttes.info/recit-policier-de-sainte-marthe-15258

arrest phase to ensure that they know where the suspects are when the time comes to arrest them[5].

Use of IMSI catchers

An IMSI catcher is a device that masquerades as an antenna in order to capture phone numbers communicating within its range. It can also be used to intercept communications, but as far as we know this was not the case in this investigation. The smallest ones fit in a suitcase.

IMSI catchers were used as part of the investigation. In one case, we suspect that the IMSI catcher was used to find out if the person under surveillance was using a second phone. To do this, they tail the person with the IMSI catcher and repeatedly record all the phones that communicate in the vicinity of the person. They get several lists taken from different geographical locations. The phone numbers found on every list must move with the person under surveillance, and it can be assumed that these are the numbers the target is using. In other cases, IMSI catchers appear to have been used to confirm or narrow down a person's address. They assume that the person lives at one address, but could live at another address covered by the same antenna, so they use an IMSI catcher (which in most cases has a much smaller range than a real antenna) that they activate outside the target's home to confirm their address.

[5]This geolocation is not GPS-based. Silent SMS messages are sent to the number to generate traffic on a regular basis (e.g. every few minutes), so that the phone connects to different antennas and the signal strength is measured at each one, giving an approximation of the distance to it. By triangulating this information, it's possible to get a much more accurate location than just the information from the antenna that the communication passes through, which is what is recorded in *fadettes*. This location is transmitted to the police automatically and in real time, unlike *fadettes* which only refer to past traffic. Accuracy can range from a few meters in dense urban areas to several hundred meters in rural areas. Live geolocation does not always allow the police to physically intercept people, as several recent examples have shown.

Telephone interception ("wiretapping")

This investigative measure must be justified by the investigators and then validated by a judge. A priori, only some of the many people involved in the case at any given time had a request for interception. These interceptions allow access to the content of SMS communications, unencrypted telephone calls and data traffic. The calls are recorded for future manual transcription, but are also relayed live to a dedicated line for an investigating officer to be able to follow up very effectively.

Interception also provides details of "Internet traffic", i.e. timestamps of sites visited, or of any server with which an application communicates[6].

Using a VPN permanently on a phone (and on a computer if you're not using Tails) protects you from Internet traffic analysis during phone interception.

Installation of spyware (referred to in the investigation as "keyloggers")

After requesting an interception, the analysis of Internet traffic revealed the predominant use of Signal as a means of communication. In some cases, the investigating judge requested the installation of spyware on phones. However, such requests are still very rare, and there are few reports of similar techniques in the press.

The purpose of this software is to gain access to the phone's data storage, to what is typed and displayed on the screen, and to encrypted messages such as those used by Signal. In this investigation, at least five requests for remote installation of spyware were made,

[6] Since all web traffic is now encrypted in transit using TLS (HTTPS), it is not possible to know what content is being accessed or even the exact page viewed. Only the domain name is visible: google.com, signal.org, wikipedia.fr or caf.fr. This can be used to find out if there is any WhatsApp or Signal traffic, and to date this traffic. It could also be used to find out the time when an email was sent or a connection was made, and to make correlations between several people in this way (even if it wasn't used in the investigation).

but as far as the case file shows at this stage, only one installation was successful (on an iPhone SE 2020).

This installation may have been accomplished through physical access to the phone. It certainly provided access to a Signal group conversation. The content of the conversation and the participants would be known to the investigators.

This number was registered to other Signal groups, so it is very likely that the investigators had access to these other groups as well[7].

Miscellaneous requests for information

Various requests to gather broad information on the suspects

Requisitions were sent to the CAF (Caisse d'Allocations Familiales, part of the French social security system), the employment office, the tax authorities, etc., in order to obtain, among other things, home addresses and telephone numbers, as well as information on the personal situation of the suspects. These requisitions are sent to :

- Public administrations such as ANTS (National Agency for Secure Documents) to obtain photos of ID cards. If a person appears to be a suspect, for example, because they are a regular phone contact of another person allegedly identified by facial recognition, and their own telephone appears to be inactive or in the vicinity of the site on December 10, investigators will request the photos used to request identity documents and then compare them with video surveillance images.
- Private transportation companies, such as Blablacar, SNCF and FlixBus, to obtain information on suspected trips (note that Blablacar has a dedicated police contact and discloses all IP addresses used to book a trip).

[7] These spyware programs are developed and installed by the Service Technique National de Captation Judiciaire (STNCJ), a department of the DGSI.