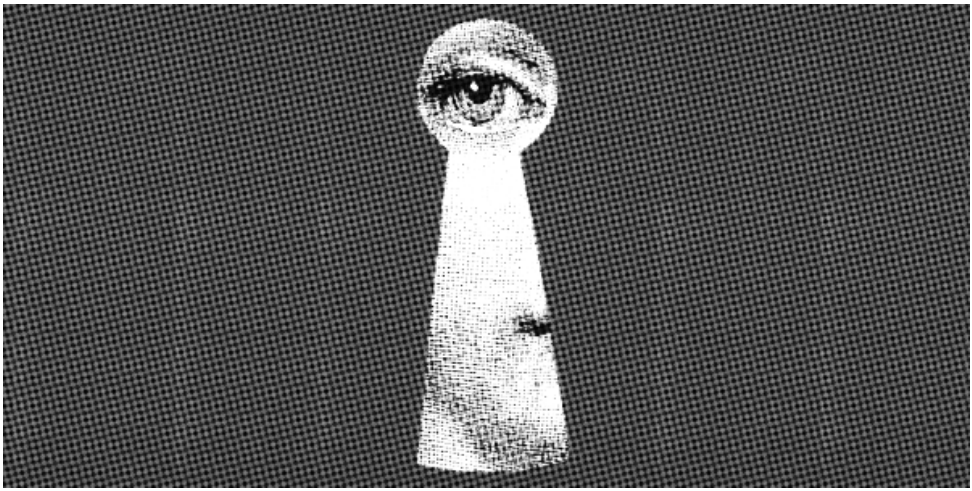
Useful things to know

(from the file of the "Diana" operation)



Useful things to know (from the file of the "Diana" operation)

Original text in Italian

Cose utili da sapere (dalle carte dell'operazione "Diana")

2025

ilrovescio.info/2025/06/28/sulloperazione-diana-contro-lanarchismo-in-trentino-cose-utili-da-sapere

English translation

Blessed Is The Flame

blessed-is-the-flame.espivblogs.net/files/2025/09/ENG-Blessed-Is-The-Flame-Issue-4.pdf

Layout

No Trace Project

notrace.how/resources/#things-to-know

The files of the Diana operation[1] include, in whole or in part, documents relating to several criminal proceedings. One of these concerns a 270-bis[3] case against various comrades and close relatives of our friend and comrade Stecco.[4]

What the State did to arrest him is rather impressive. If we take into account that Stecco, when he went on the run, had a sentence of 3 years and 6 months to serve, the disproportion between his sentence and the police's persistent pursuit of him reveals how unbearable the State finds the fact that one can escape its prisons; and how the treatment reserved for anarchists is clearly special, although it is part of a general repressive tendency.

Up-to-date knowledge of the techniques used by the political police against comrades often comes through reading the police and judicial investigation files. Therefore, it is important to share the information that emerge.

When doing so, it is always necessary to keep two points in mind: first, that this is material provided by the enemy; second, that the disclosure (of course selective and without mentioning names that appear in the documents) of this material may inadvertently produce the feeling of a kind of omnipotence of the enemy, and a corresponding feeling of paranoia and lack of confidence in our means. It is therefore important to remember that the mobilization of personnel and resources to search for fugitives is not the same as that devoted to monitoring or investigating other circumstances arising within movements and struggles; that despite advances in policing technology some wanted comrades have enjoyed freedom for months and years; that there are comrades who remain on the run in Europe and worldwide.

---

[1] *No Trace Project (N.T.P.) note:* Repressive operation against Italian anarchists. More information here.[2]

[2] https://ilrovescio.info/2023/08/04/ennesima-inchiesta-per-270-bis-in-trentino-richieste-e-non-concesse-12-misure-cautelari

[3] *N.T.P. note:* Article of the Italian penal code punishing terrorist criminal associations.

[4] *N.T.P. note:* Arrested in 2023 after almost two years on the run.

Knowing how the opposing side operates is necessary in order to adopt appropriate measures, learning from mistakes and experiences.

Let us start from some quantitative data to give an idea of the extent of the police intervention:

- Cameras in front of 6 residences.
- Ambient audio interception in the home of a person close to Stecco, in the homes of other people connected to a person who was "under close watch" and at the anarchist space "El Tavan."
- Telephone interceptions of more than 40 individuals: comrades and friends and close relatives.
- Targeted ambient audio interceptions were ordered in one case where it was believed that a person close to Stecco might meet someone who, according to the DIGOS,[5] could provide information about him.
- One person "under close watch" was followed on foot at least once by the intelligence services (the letterhead of that report is "Ministry of the Interior," while all the others indicate various Police Directorates).
- Analysis of call records of 69 people and one payphone (the maximum period for which records can be retrieved is 72 months).
- GPS trackers installed in 12 cars. For some people close to Stecco there was even ambient audio interception and video recording.
- License plates of 311 cars were placed "under watch."
- Requests for bank statements for 59 people to check for "suspicious" transactions that could indicate possible financial support for the fugitive.
- Installation of a tracking device (specifically a GSM tracker, i.e., not satellite but cellular, of the "Spora" type, meaning a miniature tracker that communicates in real time via SMS to a phone used by the police) on a bicycle believed to be used by Stecco, located using a camera in a town where he was recorded while on the run.

[5] *N.T.P. note*: The Divisione Investigazioni Generali e Operazioni Speciali (DIGOS) is an Italian police unite that, among other things, investigates organized crime and anarchists.

- In this case, as in that of another comrade on the run, forged documents were found with the personal details of real existing people. From this began a series of searches and interrogations of the people involved, with the intent of comparing movements, overnight stays in hotels and checking the activity on certain bank accounts (and, in at least one case, the activity of a "Decathlon card," which contains a history of purchases) going back several years (over 10).
- The political police of Treviso, Padua, Verona, Brescia, Bergamo, Milan, Trento, Trieste and Genoa were mobilized. From the moment they began to "tighten the circle," the DIGOS in Trento received permanent reinforcement staff, certainly at least one agent from Trieste.

For a more qualitative analysis, however, we need to look at the techniques used. Investigations moved along two axes: the analysis of an enormous amount of telephone data and the almost constant surveillance of certain people, with particular attention to when they were absent from their homes. When those persons are located again, efforts are made to reconstruct their movements as far back as possible. Data collection is carried out slowly and systematically. Some examples:

- Two comrades traveling by train were trailed by four DIGOS agents, who were positioned two at the front and two at the rear of the train. At each intermediate stop there were two plainclothes officers present, in case the comrades got off the train; for this purpose the political police of seven provinces were mobilized. From the files it appears that this trailing was ordered at the last moment, when, the previous evening, the police learned in real time from the microphones installed in the homes of people close to one of the two that he would depart by train the next day.
- The files show that the cops, in addition to asking RFI[6] for access to footage of cameras installed in train stations, asked the examining judge to install special cameras specifically at the Rovereto station, so that monitoring could be done directly from the police station. They were also able to see which tickets had been issued by each

[6] *N.T.P. note:* Rete Ferroviaria Italiana (RFI) is the public company managing Italy's railway network.

ticket machine, which searches had been made without purchasing a ticket and to access the cameras that in some cases are present on the ticket machines. These latter cameras retain footage for a maximum of 10 days (even though the general maximum retention period for infrastructures requiring greater protection is 7 days according to the 2010 provision signed by the Data Protection Authority, outside of exceptional cases).

- Having observed that a person "under close watch" had searched train timetables for a certain city using a ticket machine; when that person was absent from home the cameras of that city's station and of at least four other stations were checked. They likely analyzed data from several stations along routes leading to the city for which the search was made. In fact, because camera footage is erased after 7 days, the DIGOS in Trento rushed to the RFI Lombardy offices in Milan because they believed they had identified the person at a station (which was neither the station searched on the machine, nor one near his home) where he had gone through 7 days earlier and there was a risk that the footage would be overwritten before it could be downloaded.
- In an attempt to reconstruct the person's route, they reviewed footage from a business outside the station where they believed he went through, as well as the cameras on the train they believed he had boarded at that station. Since, from the latter, during his journey they saw him reading the latest issue of an anarchist newspaper that had been released recently, they requested that newspaper's bank records.
- To reconstruct backwards the route that led him to that station, they initially focused on Intercity trains, for which tickets must include the purchaser's name. Having identified from the list provided by FSI[7] an acronym that they believed could be linked to that person, they checked where the corresponding ticket had been issued. Since the camera footage from the station where the ticket was purchased was no longer available due to the expiration of its retention period, they

[7] *N.T.P. note:* Ferrovie dello Stato Italiane (FSI) is the public company operating Italy's railway network.

tried to reconstruct how the person reached the station where the ticket was bought.

- Having ruled out Intercity trains, because they found no identifiable name, they focused on regional trains and asked FSI to provide for each the train number of tickets issued by the ticket machines of departure stations, intermediate stations and others nearby, in locations "frequented" by anarchists: 150 pages of lists are sent by the railway companies. They also checked ferries and buses. Given that they found nothing, they requested the same data as before for the ticket machines of 69 additional stations and for any fines issued onboard trains on five regional lines. At the same time they asked the railways for a list of all tickets purchased with that acronym in previous months and to activate an "automatic alert" in case it was used again to buy tickets.
- To reconstruct the movements of certain cars, footage from various highway toll booths was reviewed; and once a car deemed suspicious was located municipal road cameras were also checked.
- Once they identified the area where they believed Stecco might be, the DIGOS requested the installation of 5 "long-range video" cameras with facial recognition and 10 cameras for "indoor/outdoor video recording" around a given station, including urban and suburban bus stops. There is no record of a request from the public prosecutor to the judge, so we do not know whether they were ultimately installed. They also analyzed images from cameras on buses. They asked to monitor the phone of a person and his mother and to have access to its call records because those people were said to have previously rented apartments in the area to comrades.
- Once Stecco was arrested they showed around his photo and questioned various locals until they identified the house where he had allegedly stayed. They took fingerprints and DNA from everything seized in the house.
- Regarding searches via phones, it should be noted that not only were the phone numbers monitored, but also the devices in which certain SIM cards had been inserted, via the IMEI number.[8] This does not happen for all numbers, but only for those deemed more "interesting"

and it seems enough for the SIM to be inserted only once (and used). Moreover, as we already know, monitoring also involves geolocation of the phone, even for non-smartphones (although in that case one can only trace the radio cells the phone connects to and not its exact position).

- Regarding the analysis of telephone traffic, once they narrowed the circle to a specific area, they searched the already acquired records for any phone numbers of anarchists living there (that is, whether any of the 69 people whose records they have had called someone who was there in the previous six years), and then all calls made by Stecco in the five years prior to his going on the run to numbers located in that area.
- They looked in the history of call records for calls made from payphones. Then they check whether calls from the payphone for which they have records were made to foreign numbers; once identified, they checked whether those numbers ever called numbers in the other records. They also checked whether landlines or mobiles in four Italian regions were called from that payphone.
- They analyzed traffic data passing through cells of the network operators Tim, Wind, Vodafone and Iliad in nine locations at times when they believed there may have been contacts with a phone supposedly used by Stecco. Given the massive volume of data, they try to cross-reference with the monitored numbers and then with all the numbers appearing in the call records they have. This type of search (cross-referencing data extracted from certain cell towers with phone numbers identified through the analysis of call records) is repeated several times. In general, in many places we find analysis of call records, sometimes going very far back in time, and attempts to cross-reference the numbers thus extracted with the data collected as the investigation proceeds.
- Although it does not ultimately appear in the files, at various points the DIGOS requests authorization to download Whatsapp chats and in one case also Telegram chats.

[8] *N.T.P. note:* An International Mobile Equipment Identity (IMEI) number is a number that uniquely identifies a phone.

- Regarding online searches, it is worth noting the attempt to install spyware (a computer virus that allows complete access to the "infected" device) "via a 1-click procedure" that would have enabled the smartphone of a person close to Stecco to act as a microphone for ambient interception (technical definition: "authorize active digital monitoring with possible interception among present people by activating the microphone on an Android mobile terminal without root"). In practice, an SMS containing a link was sent to this person that, if clicked, would have led to the installation of the virus. Since the person did not click the link, and having identified the PIN code of his phone by means of a high-resolution camera installed inside a car (which made it possible to see the code as it was typed on the phone), the DIGOS was authorized to install the virus directly if they managed to temporarily gain physical access to the phone. This does not appear to have occurred because in the meantime the investigations moved in another direction.
- Regarding email, it seems that only libero.it provided data related to email addresses (including log files), while other providers appear not to have even responded to requests (or at least there is no mention of them).
- In addition to emails, they try to obtain all data related to Microsoft Account and Google services, including purchases made via those platforms.

On this last point it is interesting to note the analysis carried out of a GAIA ID,[9] for which a phone number believed to be used by Stecco received an SMS. Basically, when one tries to access a Gmail mailbox from a device different from the one normally used, Google requests a verification step in addition to the password, sending an SMS with a numeric code to a phone number linked to the email address. Since a number linked to Stecco received this code, they tried to retrieve the data related to the corresponding Google account. To do so they entered the phone number on the Gmail login page and, on the page where the password

[9] *N.T.P. note:* Google Account and Id Administration (GAIA) is the centralized authentication system of Google services. A GAIA ID is an identifier of this authentication system that allows to uniquely identify each user of Google services.

is requested, right-clicked and selected "View page source." A window opened containing the HTML code,[10] they typed CTRL+F (find) and in the search box typed the characters ",[" to find the 21 digits that make up the GAIA ID.[11] To find out to whom this ID belonged, they used one of Google's services, Google Maps (from the description it appears they can use any Google service, but Google Maps is probably the one where reviews and contributions are more often left).

In practice, in the address bar they entered "https://google.com/maps/contrib/" followed by the GAIA ID to view all the reviews left via that Google account and thereby identify the email addresses linked to it. They then requested from Google all the registration data related to the email addresses, the phone numbers, the date they were associated with the addresses, the personal data related to the GAIA ID and all log files of every connection to that account. It does not appear that they received a response.

To try to summarize in an understandable way, multiple email addresses and multiple phone numbers can be associated with each GAIA ID; once the police know one of those elements they can try to trace the others.

Let's continue:

- Following an ambient audio interception in which an email address is mentioned, they request from Microsoft the corresponding personal data, the billing details of the account in case purchases were made on the Microsoft Online Store, the IP connection logs, all email addresses and phone numbers associated with that address and all the people who registered with a name linked to that address. In addition they request from the website subito.it[12] the log files and IP addresses corresponding to that email address.
- In another file, related to the search for another comrade on the run, we found the following excerpt regarding the active and passive digital monitoring of a computer: "As is known, in light of current

[10] *N.T.P. note:* HyperText Markup Language (HTML) is the language in which web pages are written.

[11] *N.T.P. note:* As of 2025, this technique to find the GAIA ID corresponding to an email address does not seem to work anymore.

[12] *N.T.P. note:* An Italian classified ads website.

technologies it is very difficult to infect a PC, because there are many variables that determine the success or failure of such an operation (operating system, antivirus, network card, etc.) Therefore, as is customary, it is essential to initially carry out a feasibility study to establish the type of operating system used and any active antivirus through passive monitoring, and only then proceed to the active monitoring. The procedures for installing the spyware will then be decided in agreement with the technicians of the company entrusted with the installation. Through physical surveillance, it was noted that […] sometimes leaves the computer in the trunk of his car […] when he goes to work in […]. With prior authorization from the judge, the technician would proceed to install a file with the computer switched off (this is feasible simply by leaving a USB stick or any other physical memory device inserted in the PC), a file that at startup will be executed automatically by the computer and will proceed to install other small malicious software, necessary to study the software environment present on the device, and then optimize the spyware that will allow the requested monitoring."

- After seizing a Tails USB stick they try to find the password using the program "bruteforce-luks." They note that it is not possible to estimate the time required for this operation.

Significantly, the only one of the 11 files that make up the "Diana" file to be empty is the one labeled "Expenses." There are, however, some quotes for the rental of surveillance devices, from which it also emerges that geolocation devices often offer an "audio monitoring option," so they are multipurpose devices. It also appears that since Covid they can have listening stations at home for teleworking.

The opening of a file at the Ministry of the Interior and some notes bearing that letterhead suggest the involvement of the intelligence services.

Last but not least: simultaneously with the case relating to Stecco at least one other 270-bis investigation was active in which some of the suspects are the same people involved in the 270-bis case relating to Stecco. This gives an idea of the pervasiveness and the everyday nature of the control to which some comrades are subjected.

It is useful to know that the cops may take weeks to review footage from station cameras, trains, toll booths and buses, searching for images that suggest routes and destinations. They try to do this even retroactively with respect to a journey considered suspicious, reconstructing much of a route starting from where it ends, looking for coincidences between moments of "disappearance," days, times, and means of transport.

Everyone will decide for themselves what to make of all of this.

Let us give even more force to practical criticism of the world of surveillance and digital control, as an indispensable area of intervention if dreams and plans of subversion and freedom are to remain possible.

May fortune favor those on the run and those who, in the struggle for freedom, defy any identification.

The files of the Diana operation include, in whole or in part, documents relating to several criminal proceedings. One of these concerns a 270-bis case against various comrades and close relatives of our friend and comrade Stecco. What the State did to arrest him is rather impressive.

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.