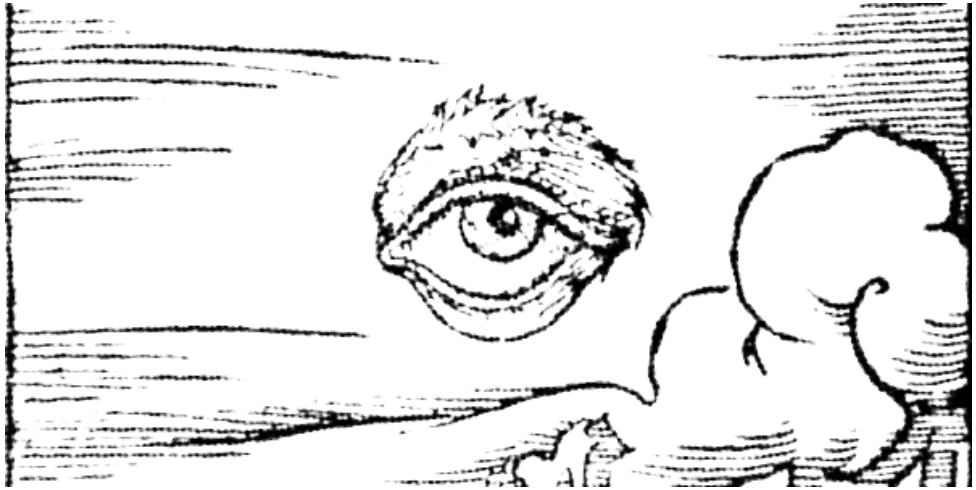
As friends and tech-savvy comrades, we are often approached with questions about what the police and other law enforcement agencies can do. At the same time, we frequently notice behaviors that show a certain carelessness, overlooking the tools these authorities have at their disposal and the growing budgets allocated to advanced surveillance technologies in recent years. For these reasons, among others, we decided to compile this text to provide, in a structured way, some information about what we have seen or read over the past years.

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.

Snooping Eyes

Report on Methods and Tools of Digital Repression



Snooping Eyes: Report on Methods and Tools of Digital Repression

Original text in Italian

Occhi indiscreti: relazione sulle modalità e gli strumenti di repressione digitale

arachidi@autistiche.org

2025

arachidi.noblogs.org

English translation

Snooping Eyes: Report on Methods and Tools of Digital Repression

arachidi@autistiche.org

arachidi.noblogs.org

Layout

No Trace Project

notrace.how/resources/#snooping-eyes

A radio-controlled police automaton. From Hugo Gernsback, "Radio Police Automaton," *Science and Invention* 12, no. 1 (May 1924): 14.

get used to providing online verification whenever requested, just as we got used to accepting cookies.

There's not a single way to practice technological self-defense, nor a way that is definitive and all-inclusive. Each situation and each person needs specific tools and unique balances. Not even the complete refusal of the phone is a perfect solution, because it still exposes to the risks of cameras, or microphones; or simply it requires for all the people around us to be willing to make our same choice, or support us.

Even though this text aims to provide a summary of technical surveillance tools, we would like to emphasize that they are not the only instruments of repression.

Since we truly believe that surveillance is a social problem, even before being a technical one, we research and wish to keep the discussion open between more and less nerdy people, who will evade with creativity the state, big tech and general control mechanisms, included patriarchal ones, building relationship models that allow us to go beyond technologies.

And this evasion process must be expanded and spread outside our bubbles and circles, not just because security is a collective and communal problem, but also because the only way to truly defend ourselves is for this culture to spread and multiply, until the last camera is burned down.

Contents

Intro

Digital technology touches every part of our lives—and the repression of social struggles is no different.

As friends and tech-savvy comrades, we are often approached with questions about what the police and other law enforcement agencies can do. At the same time, we frequently notice behaviors that show a certain carelessness, overlooking the tools these authorities have at their disposal and the growing budgets allocated to advanced surveillance technologies in recent years.

For these reasons, among others, we decided to compile this text to provide, in a structured way, some information about what we have seen or read over the past years.

This text is NOT intended to create paranoia, but rather to foster collective awareness. At the same time, it does not claim to cover all the techniques used by the state, as most only become known after investigations are concluded.

To keep the main text readable, reflections and analyses are placed at the end for those who wish to read them, and can be skipped by others.

Disclaimer: This information mainly concerns operations and techniques used by Italian law enforcement, but we think it can be useful for people living in other territories as well.

Operations/investigations mentioned:

- Diana (2022): notrace.how/resources/read/useful-things-to-know.html
- Scintilla (2019): darknights.noblogs.org/post/2023/01/21/turin-italy-first-degree-sentence-in-the-scintilla-trial
- Sismi (2022-2024): actforfree.noblogs.org/2023/07/31/potenza-italy-the-usual-ones

porn websites through ID checks. Tomorrow, the same mechanism could be extended to websites that provide anonymity tools, or even to those that are perceived as promoting hate and violence. It is easy to see how such restrictions could gradually expand and, over time, turn into forms of censorship affecting information websites, blogs, and other types of online content.

And there's more! Soon the possibility to install open source software (which means that it's possible for everyone to fully read it and modify it) will be limited, for example by making it impossible to spread smartphone apps without authorization from Google and Android.

Even if we believe that these events fit perfectly into a broader picture of increasingly invasive, controlling and repressive technology, we would like to share some thoughts.

Diving into the spyware world during the last year, we realized that Big Tech companies, Google in pole position, are starting to narrate themselves as privacy protectors. This, besides being clearly a lie, is a significant factor at the social level, because it excludes even the possibility of building, using and spreading alternatives. The world ahead of us is becoming increasingly monolithic, with only one possible path: surveillance, whether done by Microsoft or by the states.

All this leads us to believe that using technology in our advantage will be a slippery and complex path, as we have less and less control over it, and all the security drifts will make it even more difficult.

What kind of conclusions can we take from all of this?

Even if they are possible and necessary, what we have to search for are not technical solutions to this enormous problems. It's obvious that 4 crazy scientists will always find the way to elude these controls; the problem is more how to ensure that we won't

Miscellaneous

Controlling bank movements

This is an activity common to different inquiries; it has been used for example to verify the existence of suspicious money movements aimed at helping fugitives, or to verify which transactions were linked to solidarity funds for prisoners.

Considerations

This text has followed quite a long period of sharing reflections, chit-chats, reading and writing on technologies in general. To give an idea of the context in which we are moving and thinking, in the last year spyware have returned to the media spotlight:

- amnesty.org/en/documents/eur70/8814/2024/en
- amnesty.org/en/latest/news/2025/06/italy-new-case-of-journalist-targeted-with-graphite-spyware-confirms-widespread-use-of-unlawful-surveillance

In a more private dimension, we see the increase of usage of stalkerware and parental control apps to stalk partners/exes. Recently the European regulation Chatcontrol has been approved, even if the mandatory requirement for generalized scanning of messaging service has been removed from the text, as a form of protection of privacy and cryptography. This nonetheless does not make us hope that it won't be submitted again, especially given the repeated insistence in the recent years (it was first submitted in 2022).

But here we are not talking "just" about a new Chatcontrol, spyware, stalkerware, artificial intelligence, cameras, microphones–and the list can be long. Recent legislation (for example, look at article 13bis of the Caivano decree) aim at restricting more and more internet use: today we have age verification on

- Carnevale No Ponte (2025): (In Italian) brughiere.noblogs.org/post/2025/09/11/sugli-arresti-moltopost-carnevale-no-ponte
- And others that we forgot or that have no name…

Cameras

Private cameras (with microphones)

In the operation following "Carnevale No Ponte," case files indicate that recordings with audio from a private shop inside a covered market were reviewed. These recordings covered areas where the defendants met and discussed plans for the demonstration, and were used to support charges of premeditation.

Reading PINs via HD cameras

According to "Useful things to know (from the file of the 'Diana' operation),"[1] a high-resolution camera installed inside a car allowed investigators to read a phone PIN as it was typed.

Long-distance video cameras with facial recognition

In Operation Diana, facial recognition cameras were monitored in busy transit areas, such as train and bus stations, to locate a specific individual. If there was reason to believe the person had boarded a bus, the interior cameras of the vehicle were also reviewed.

- (In Italian) irpimedia.irpi.eu/sorveglianze-viminale-riconoscimento-facciale-trasparenza
- (In Italian) web.archive.org/web/20260303140215/https://www.poliziadistato.it/statics/17/lotto-2—sari-sistema-di-acquisizione-e-trasmissione-v23—finale–2-.pdf

[1] https://notrace.how/resources/#things-to-know

Monitoring highway cameras

During Operation Sismi, investigators checked highway license plates to identify who had hung a banner from a bridge, and later attempted to estimate individuals' heights from the footage. Urban and highway cameras are frequently used in many operations.

Phones

Forensic extraction (local attack)

One case involved three phones seized on March 20, 2024, during an action at Malpensa Airport. These phones, protected by PINs and encryption, were returned showing clear signs of compromise: two had the PIN written on a sticker on the back, indicating they had been unlocked and analyzed.

As far as we know, the devices were powered off and fairly up to date, requiring a Before First Unlock (BFU) attack—one of the most complex and expensive forensic procedures according to the security company Cellebrite.

How to protect ourselves?

Mobile device security depends heavily on model and software/hardware updates, which can be costly.

- GrapheneOS is an open-source project providing strong security, but it requires a specific phone model (as of November 2025, the cheapest is Google Pixel 6, ~€100).
- For other Android phones, there are no inexpensive fully secure options. However, some apps from alternative app stores (F-Droid) allow data wiping if unauthorized access is attempted. (See apps like Wasted and Duress.)

For further reading:

It is not known whether these requests would have been complied with, but it is known that, following the arrest of Pavel Durov [CEO of Telegram], Telegram updated its privacy policy. It is also possible to verify how many requests have been submitted in each country: for example, in Italy in 2024 there were 158 requests affecting a total of 419 users, while in the first six months of 2025 there were 428 requests involving 1,852 users.

In terms of end-to-end encryption, WhatsApp offers stronger guarantees than Telegram. However, Meta has been subject to investigations in Italy and across Europe concerning privacy issues and the forced integration of artificial intelligence into the WhatsApp application. In addition, chat backups are not encrypted by default.

Each year, Meta receives hundreds of thousands of requests from law enforcement agencies. It is not known how many of these are actually complied with, but the company does hold certain categories of data, including phone numbers, activity duration, connection times, account usage information, and metadata related to messages and calls.

- te-k.github.io/telegram-transparency

How to protect ourselves?

For us the best options, which means the best balance between security, ease of use and popularity is still Signal, but there are many apps that guarantee anonymity that can be used when needed.

- notrace.how/resources/#the-guide-to-peer-to-peer-encryption-and-tor

- transparencyreport.google.com/user-data/overview

GAIA ID

Operation Diana: analysis of the GAIA (Google Account and ID Administration) ID is mentioned; when there's an attempt to connect to a Gmail account from a different device than the usual, there's a request for an additional verification through SMS. Given that the number linked with the user receives this code, the investigators searched for data related to this account. After having obtained the GAIA ID for the account, through the url https://google.com/maps/contrib/GAIAID (with "GAIAID" replaced with the GAIA ID) they saw all the reviews of that account, and through that traced back the connected email addresses. They requested from Google all log files for each connection to the account. It seems that they never received an answer.

Essentially, each GAIA ID can have multiple email addresses and phone numbers referencing it, and once that the police has obtained a piece of this data it can try to recover the rest.

Social media and blog monitoring

It's almost as if cops follow them as a soap opera… They are most certainly more informed than all of us are.

In many court documents they cite a constant monitoring activity.

Whatsapp and Telegram chats

Operation Diana: although there is no trace of this in the interceptions, on several occasions the DIGOS [Italian law enforcement agency] has requested authorization to download WhatsApp chats, and in at least one case also Telegram data.

- search.f-droid.org/?q=wasted
- osservatorionessuno.org/blog/2025/03/cellebrite-and-the-routine-use-of-digital-surveillance-in-italy
- anarsec.guide/posts/grapheneos
- opsec.riotmedicine.net/downloads#mobile-phone-security
- (In Italian) nocprtorino.noblogs.org/post/2025/02/11/da-malpensa-a-tel-aviv-come-le-aziende-di-sicurezza-informatica-israeliane-collaborano-con-le-autorita-italiane-per-accedere-ai-dispositivi-mobili
- (In Spanish) quematumovil.pimienta.org

"Preview" procedure

Once a phone is unlocked, its contents (chats, photos) are manually reviewed while recording screen and audio.

How to protect ourselves?

- Do not provide your PIN. In Italy, it is legal to "forget" it when requested by police (though this is not a guarantee).
- Check the rules carefully if abroad—laws vary, and authorities may justify seizure depending on the alleged offense.
- Avoid short or easily guessable PINs. Using a PIN like "1312" is the same as handing it over willingly. The recommended PIN should consist of 8–10 alphanumeric characters.
- archerpoint.com/wp-content/uploads/2025/06/blog-2025-cybersecurity-brute-force-update-01.jpg

Location tracking (via cell towers)

There are two main ways to track phones via cell towers: **aggregated traffic** and **disaggregated traffic**.

- **Aggregated traffic**: the operator reports the main cell a phone connects to. Transit cells (while moving) are generally not visible, unless events such as signal loss, phone shutdown, or connection to Wi-Fi occur, so movement cannot be precisely tracked.
- **Disaggregated traffic**: shows transit and disconnection cells, allowing more precise movement tracking.

In the documents we reviewed, there was no evidence of disaggregated traffic, though some providers may provide it in certain cases.

How to protect ourselves?

Depending on risk level, it may be safer to leave the phone at home or enable airplane mode.

However, not carrying a phone at all may also be considered an aggravating factor.

Targeted interceptions

At this link it's possible to see data relating to various types of interceptions in Italy, from 2014 to 2024:

- datiestatistiche.giustizia.it/it/intercettazioni.page

"Normal" calls and SMS

Remember we always have something to hide, because every piece of information can be useful during an investigation; we cannot predict what will be used against us, and analyzing unencrypted traffic is very easy and inexpensive.

Data retention by telephone providers is regulated according to article 132 of the Privacy Code, with some specific differences depending on the data type:

How to protect ourselves? Use email providers that do not collaborate with police or state forces,[4] or use systems that mask your IP (Tor, VPN, proxy).

Gmail, Microsoft, Meta, Proton, etc, do they always give out the requested information?

Operation Diana: after an environmental wiretapping where an email address is mentioned, they (police) ask Microsoft the registry, the account billing data, the connection IP logs, all email addresses and phone numbers associated with that address, as well as all the users that registered with a name connected to that email. They also asked the provider "subito.it" the records of the log file and IP addresses used by that email.

Although collaboration between Italian providers and law enforcement agencies is well established and mathematical, the same cannot be said for big tech companies.

Protonmail is considered, and presents itself, as a valid and privacy-oriented alternative; but it's important to remember that in 2020 the company has provided information on the IP address of a French climate activist, who was later arrested.

In the same year, Proton Technologies received 3572 orders (compared to 13 in 2017) from Swiss authorities to share information on users. Of those 3572 orders, 195 where coming from abroad. The company contested 750 orders and complied with 2017 requests.

Remember, companies cannot provide data they don't actually have!

- proton.me/blog/climate-activist-arrest
- privacyradar.com/news/privacy/proton-mail-payment-data-stop-cop-city-activist-identified

[4] https://riseup.net/en/security/resources/radical-servers

4. Obtained IP addresses that visited a website in certain hours (data was given by the provider without notifying the website managers).
5. Requested to an ISP (Fastweb, Tim, Vodafone, etc.) to identify the IP addresses by associating them with a user (account holder, address).
6. Correlated data with telephone wiretapping and other phone records to strengthen the attribution of articles to a specific person.
7. Obtained the authorization for a possible technical analysis of a website (research for vulnerabilities) to evaluate the possibility of intrusion or to acquire further technical evidence.

How to protect ourselves?

In this case as well, having used the Tor network or a VPN would have made the inquiries much more complex for the investigators; moreover, on Wordpress it's possible to hide the name of whoever is uploading the articles.

Watch out for metadata and services we use!

Meta (Facebook) can provide the account that created a specific page or group

In Operation Scintilla the management of a Facebook page was used as evidence; the page was linked to certain people through email addresses associated with the accounts that had created or managed the page.

Subsequently, a request was made to Google to obtain the IP addresses linked with the email. The IP address was then associated with a user thanks to the collaboration of the telephone provider.

- Data relating to phone traffic (not the content of the calls, but how long, when and who): retained for 24 months starting from the date of the communication.
- Data relating to electronic traffic (excluding the content of the communications, such as internet connection data or SMS): retained for 12 months.
- Data relating to unanswered calls: retained for 30 days.

Some recent laws have discussed extending this period to 6 years for security reasons; the retention would also apply to cell tower connection data, which falls under the category of electronic traffic.

During Operation Diana, records from public payphones were also reviewed.

How to protect ourselves?

Don't use calls and SMS! Use encrypted messaging apps such as Signal, we'll talk about this more in the section “Whatsapp and Telegram chats”, p. 17.

Passive electronic interception (remote attack)

Operation Sismi: In the pricelist, passive electronic interception (which cost €30/day in 2022) is described as “passive interception of the electronic data flow relating to fixed ADSL or mobile users (data transmission via 2G, 3G, and 4G) for operators capable of autonomously capturing such data.” If the operator does not provide this service, the cost increases to €60/day.

Essentially, this type of interception enables law enforcement to access and monitor data traffic, including DNS requests, the current operating system version, the presence of antivirus software, installed applications, and device usage patterns.

In the 2023 pricelist, it was extensively emphasized that this form of interception is instrumental to active electronic inter-

ception (i.e., spyware deployment), both because successfully infecting a device requires prior knowledge of the user's habits, and because it helps determine whether deploying spyware (which is significantly more expensive) is actually necessary.

How to protect ourselves?

Using Tor[2] or a VPN will encrypt the information mentioned above.

For the curious ones: We still need to pay attention to various nuances. For example, if we use Tails[3] within a network that is being monitored (whether a home network or a hotspot), it will not be possible to observe any unencrypted traffic. By contrast, if we use Tor Browser outside of Tails, only the websites accessed through Tor Browser will be protected from surveillance.

Active electronic interception (spyware)

Disclaimer

The cases we were able to analyze all involved smartphones, but similar techniques could also be used to infect laptops. Moreover, attack methods may now be different and more sophisticated.

In Operation Sismi, devices were infected with spyware called "Spyrtacus." Based on the information available, this appears to have been the third occurrence in recent years, and several elements of the attack are consistent across all the cases we were able to examine.

In 2023, the cost was €250 for the infection (charged only if successful), plus €170 per day to rent a PC workstation equipped with the relevant management software.

[2]https://torproject.org
[3]https://tails.net

How to protect ourselves?

To detect bugs, a manual search is best, as technological tools are often expensive or ineffective. In cars, they are usually connected to the battery and hidden inside the passenger compartment; in homes, they are found near outlets or inside appliances such as refrigerators and microwaves. Battery-powered versions exist as well, for short-term surveillance, and they are usually harder to find. They often include a SIM card for connectivity and an internal memory/microSD to save recordings.

- notrace.how/earsandeyes
- hackrf.readthedocs.io/en/latest/hackrf_one.html

Blogs, social media and other services

Attacks on websites

Some court documents state: "activity aimed, with OSINT techniques and Ethical Hacking, at analyzing the structure of the platform… to highlight vulnerabilities useful for a subsequent intrusion." It's not said whether the intrusion actually happened, but that it could have been authorized if necessary.

We will try to briefly describe here what has happened. Police has:

1. Carried out OSINT analysis on a website and its contents (research on public information on the website and its infrastructure).
2. Identified names and nicknames of the authors of articles (public information, but concealable on Wordpress (!)).
3. Collected data on users visiting a blog, requesting access logs to the website provider (Aruba, Hostinger, etc.)

Is it possible for the spyware to survive a reboot?

Most likely yes.

IMSI-catchers ("spy" cell towers)

An IMSI-catcher mimics a cell tower, tricking nearby phones into connecting to it. This allows it to intercept IMSI, IMEI, calls, messages, location data, and internet traffic, as well as enable machine-in-the-middle attacks. At this time, there is no evidence of its use, but it could be used for eavesdropping and traffic diversion. In Italy, the State Police and the Finance Police have issued warrants for mobile and fixed IMSI-catchers.

How can we protect ourselves?

Some phones allow disabling 2G calls in the network settings, reducing the risk of unauthorized interception. In any case, a device that is turned on—with or without a SIM card and not in airplane mode—will still connect to a cell tower, making it possible to track its location.

- (In Italian) lanotiziagiornale.it/tempi-duri-per-gli-evasori-la-guardia-di-finanza-acquista-gli-imsi-catcher-per-rintracciare-i-cellulari
- efforg.github.io/rayhunter

Ambient and directional microphones

If cops know the usual meeting places, they can install cameras and microphones there. Even if you change location, remember that it's not always easy to tell if you are being followed; therefore, it's essential to verify the safety of the meeting places and check whether the use of an ambient microphone is possible.

Bugs, with microphone or GPS tracker, were found during many investigations in cars, homes and even bicycles.

How does the infection happen?

Cooperation from the telecommunications provider and the creation of tailored social engineering attacks are vital.

The target is studied—to a greater or lesser extent—through traditional telephone wiretaps or via the passive electronic surveillance mentioned above.

The most commonly used procedure is as follows:

1. Data and/or phone connectivity to the targeted device is interrupted, if necessary for days.
2. To seek clarification, the targeted user then voluntarily calls customer support, or all outgoing calls are automatically redirected to customer support. In reality, they will be put in contact with a technical department that will instead install the malware.
3. The technical support team will prompt the targeted user to install an application either from the Play Store or from a seemingly legitimate website, which may also be delivered via text message, potentially appearing to come from the mobile operator's number. The user will then be guided through granting the permissions required for the installation and proper functioning of the app, such as enabling installation from unknown sources, allowing the app to run in the background, exempting it from Google Play Protect checks, and granting access to the microphone, location, and other system features.

During Operation Sismi, however, the attackers chose to impersonate the train operator Trenitalia and, using various promises, convinced the victim to install the malicious app.

Is it possible they use other methods to install the spyware?

There are installation methods which are more expensive and more effective as well, such as a one-click attack (a message

containing a malicious link, a PDF or an excel file that, if clicked, installs a spyware without the user noticing).

Even more expensive and sophisticated attacks are called zero-click, because no interaction is needed from the user, as was the case for the spyware "Graphite" of the "Paragon Solutions" company, or "Pegasus" of "NSO Group" from some years ago.

It's also possible for this software to be installed during a more or less prolonged police seizure, even thought in Italy we still have no evidence of this.

- amnesty.org/en/latest/news/2024/12/serbia-authorities-using-spyware-and-cellebrite-forensic-extraction-tools-to-hack-journalists-and-activists
- citizenlab.ca/research/a-first-look-at-paragons-proliferating-spyware-operations
- notrace.how/resources/read/it-could-be-harmful-spyware-installation-through-social-engineering-attacks-in-italy.html
- techcrunch.com/2025/02/13/spyware-maker-caught-distributing-malicious-android-apps-for-years

What can spyware usually do?

- Remotely activate the microphone.
- Read notifications.
- View the screen in real time.
- Take screenshots.
- Determine the device's exact location.
- Potentially gain full control of the device.
- For an additional fee, it may also be possible to access messaging applications such as WhatsApp, Telegram, and Messenger, although there is no evidence that this actually occurred.

How to protect ourselves?

We should not underestimate social engineering attacks. When they are carefully tailored to a specific individual, falling for them is far easier than one might expect.

Take the Trenitalia case, for example. Would it really seem suspicious if, during the call, the attacker listed your recent trips to establish credibility? Or if the call came immediately after you had purchased a ticket?

If the call arrives at a moment when your guard is down, and everything sounds entirely plausible, falling for it becomes much more likely.

Even in such cases, operating systems like GrapheneOS can provide a higher level of protection, though not complete security. Avoiding suspicious links and not trusting questionable "support" teams remain the first—and often only—line of defense.

How to know whether a phone is infected?

The application can be hidden or appear as something else, but it will probably use a lot of battery and, as mentioned above, we will install it ourselves, so we just need to remember whether we have been guided to install any application.

If you happen to notice any infection attempt, or if your phone has been seized by police, there's a network of people that is interested in analyzing potentially compromised phones. You can contact them through this email address: cispiano@anche.no. Keep in contact with your trusted hacklab (because you have one, right?) as well.

Is it possible for the spyware to survive a factory reset?

Most likely no.