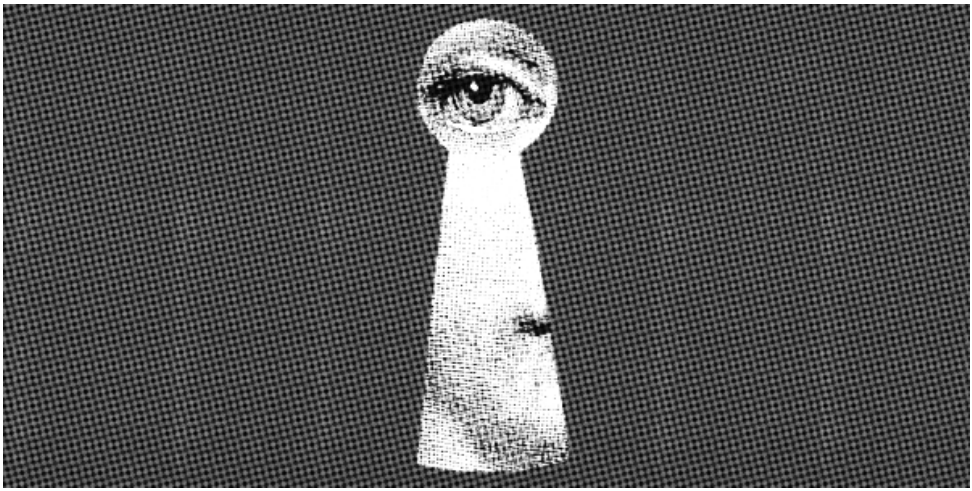
Des choses bonnes à savoir

(tirées du dossier de l'opération « Diana »)



Des choses bonnes à savoir (tirées du dossier de l'opération « Diana »)

Texte d'origine en italien

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

Traduction française

attaque.noblogs.org/post/2025/08/28/italie-des-choses-bonnes-a-savoir

Mise en page

No Trace Project

notrace.how/resources/fr/#choses-a-savoir

Dans le dossier de l'opération Diana[1] sont reproduits, intégralement ou en partie, les dossiers de différentes procédures pénales. L'une d'entre elles est celle en vertu de l'article 270 bis,[3] contre plusieurs compagnons, compagnonnes et proches de notre ami et compagnon Stecco.[4]

Ce que l'État a mis en œuvre pour l'interpeller est plutôt impressionnant. Si l'on garde à l'esprit que Stecco, quand il s'est mis au vert, devait purger une peine définitive de trois ans et six mois, la disproportion entre sa condamnation et l'acharnement des flics pour le trouver révèle à quel point l'État considère insupportable que l'on puisse se soustraire à ses prisons et à quel point le traitement réservé aux anarchistes est caractérisé, bien que dans le cadre d'un durcissement répressif général, par une nature sans doute spéciale.

Très souvent, c'est par la lecture des dossiers des enquêtes policières-judiciaires qu'on acquiert une connaissance actualisée des techniques utilisées par la police politique contre des compagnons et des compagnonnes. Il est donc important que les indications qu'on peut en tirer soient partagées.

Au moment de le faire, il est toujours nécessaire de garder à l'esprit deux aspects : le premier est qu'il s'agit là d'un matériel fourni par l'ennemi ; le deuxième est que le partage de ce matériel (bien entendu sélectionné et en enlevant les noms qui apparaissent dans le dossier) peut involontairement produire le sentiment d'une sorte de toute-puissance de l'ennemi, avec son accompagnement de paranoïa et de manque de confiance dans nos propres moyens. Il convient donc de rappeler que le déploiement d'hommes et de moyens pour chercher des personnes en cavale n'est pas le même qu'ils adoptent pour la surveillance/les enquêtes dans d'autres circonstances des mouvements et des luttes ; que, malgré le progrès policier-technologique, certains compagnons recherchés ont savouré la liberté pendant des mois ou des années ; qu'en ce moment même, en Europe et dans le monde, il y a des compagnonnes et des compagnons en cavale.

---

[1] *Note du No Trace Project (NdNTP) :* Opération répressive contre des anarchistes italiens. Plus d'informations ici.[2]

[2] https://attaque.noblogs.org/post/2023/09/09/trentino-italie-enieme-enquete-pour-270-bis-le-parquet-demande-12-mesures-preventives-non-accordees

[3] *NdNTP :* Article du code pénal italien punissant les associations de malfaiteurs à caractère terroriste.

[4] *NdNTP :* Arrêté en 2023 après une cavale de presque deux ans.

Savoir comment l'adversaire agit est nécessaire pour adopter les contre-mesures les plus opportunes, en apprenant des erreurs et en tirant profit des expériences.

Commençons par quelques données quantitatives, pour donner une idée de l'étendue de l'intervention policière :

- Des caméras devant six habitations.
- Des sonorisations à l'intérieur de la maison d'une personne proche de Stecco, dans celle d'autres personnes en lien avec un individu qui faisait l'objet de leurs « attentions » spéciales et dans l'espace anarchiste « El Tavan ».
- Des écoutes téléphoniques sur les lignes de plus de quarante personnes : des compagnonnes et des compagnons, mais aussi des ami·es et des proches.
- Dans un cas, des sonorisations « ponctuelles », quand ils pensaient qu'une personne proche de Stecco aurait pu rencontrer une personne qui, selon la DIGOS,[5] aurait pu lui fournir des informations sur ce dernier.
- Une personne qui faisait l'objet de leurs « attentions » spéciales a été suivie au moins une fois par des agents du Renseignement (l'en-tête du PV est « Ministère de l'Intérieur », alors que toutes les autres sont celles des différentes Préfectures de police).
- L'analyse de l'historique des fadettes téléphoniques de 69 personnes et d'une cabine téléphonique (la durée maximale d'analyse rétroactive est de 72 mois).
- Des GPS installés sur 12 voitures. Pour certains proches de Stecco, dans les voitures il y avait aussi des micros et des caméras-espions.
- Une « attention » spéciale prêtée aux plaques d'immatriculation de 311 voitures.
- La requête des historiques des comptes bancaires de 59 personnes, pour vérifier l'existence de mouvements « suspects », qu'on pourrait relier à un appui économique à sa fuite.

[5] *NdNTP :* La *Divisione Investigazioni Generali e Operazioni Speciali* (DIGOS) est une unité de police italienne qui enquête notamment sur le crime organisé et les anarchistes.

- L'installation d'un dispositif de suivi (plus précisément un dispositif GSM, donc non satellitaire mais de type téléphonique, nommé « Spora », un traceur miniature qui communique en temps réel à un téléphone utilisé par la police quelle cellule radio il utilise) sur un vélo qu'ils pensaient que Stecco pouvait utiliser, car identifié par une caméra de surveillance dans un village où il avait été filmé pendant sa cavale.
- Dans ce cas, comme dans le cas de la cavale d'un autre compagnon, les flics ont retrouvé des documents d'identité falsifiés, avec des états civils de personnes réellement existantes. Ils ont donc recherché et interrogé les personnes en question, dans le but de comparer leurs déplacements et les nuits passées dans des hôtels et de contrôler les mouvements de certains comptes bancaires (et aussi, au moins dans un cas, de contrôler une carte de fidélité Decathlon, où est mémorisée une chronologie des achats effectués), pour des périodes de plusieurs années (plus de dix) dans le passé.
- Ils ont mobilisé la police politique des provinces de Trévise, Padoue, Vérone, Brescia, Bergame, Milan, Trente, Trieste et Gênes. Du moment où ils ont commencé à « resserrer l'étau », la DIGOS de Trente a reçu du personnel supplémentaire en permanence, sûrement au moins un agent venant de Trieste.

Pour une analyse plus qualitative, par contre, il faut examiner le détail des techniques utilisées. Pour résumer, les enquêtes ont avancé selon deux lignes : l'analyse d'une quantité énorme de données téléphoniques et la surveillance presque constante de certaines personnes, avec une attention particulière à leurs absences de leurs lieux de résidence. Quand ces personnes sont repérées à nouveau, les flics reconstruisent à rebours, autant que possible, leurs déplacements. La collecte des données est effectuée avec calme et de manière systématique. Voici quelques exemples :

- Deux compagnons qui font un voyage en train sont filés par quatre agents de la DIGOS, qui se placent, deux par deux, à chaque bout du train. Dans chacune des stations intermédiaires, il y a aussi deux policiers en civil, au cas où les compagnons descendent du train ; pour ce faire, c'est la police politique de sept provinces qui a été mise à contribution. En lisant le dossier, il semblerait que cette filature ait été

décidée à la dernière minute, quand, la veille, la police a appris, par le biais des micros installés dans la maison de personnes proches de l'un des deux compagnons, que celui-ci partirait en train le lendemain.

- En lisant le dossier, on apprend que les flics, en plus de demander à RFI[6] d'avoir accès aux enregistrements des caméras des gares, ont demandé au juge d'instruction l'autorisation d'installer des caméras à eux dans la gare de Rovereto, pour pouvoir avoir un accès immédiat aux images, depuis le commissariat. Ils ont aussi pu voir quels tickets ont été émis par chacun des distributeurs automatiques de tickets, les recherches qui y ont été effectuées, même sans que des tickets aient été achetés, et avoir accès aux caméras qui, parfois, sont installées directement sur les distributeurs. Ces caméras conservent leurs vidéos pendant un maximum de dix jours (malgré le fait que la durée maximale générale, pour les « infrastructures nécessitant d'être particulièrement protégées », soit de sept jours, sauf cas exceptionnels, selon le décret de 2010 de l'Autorité de garantie de la vie privée).
- Étant donné que les flics ont vu qu'une personne qui faisait l'objet de leurs « attentions » spéciales avait cherché les horaires des trains pour une ville donnée sur un distributeur automatique de tickets, quand cette personne est partie, ils ont visionné les vidéos des caméras de la gare de cette ville et d'au moins quatre autres gares. Il est probable qu'ils aient analysé les données de plusieurs gares qui se trouvent le long des lignes menant à la ville pour laquelle la recherche avait été effectuée. Étant donné que ces données sont effacées après sept jours, la DIGOS de Trente s'est précipitée aux bureaux de RFI Lombardia, à Milan, parce qu'ils pensaient avoir repéré la personne en question dans une gare (qui n'était ni celle recherchée sur le distributeur automatique, ni l'une de celles proches de son habitation) où elle était passée sept jours auparavant et il y avait le risque d'une réécriture des vidéos, avant qu'ils aient pu les télécharger.
- Dans une tentative de reconstruire le parcours d'une personne, les flics regardent les images de vidéosurveillance d'un commerce situé à l'extérieur d'une gare où ils pensent l'avoir repérée, en plus des

[6] *NdNTP :* Rete Ferroviaria Italiana (RFI) est l'entreprise publique gestionnaire du réseau ferroviaire italien.

caméras du train dans lequel ils pensent qu'elle est montée à cette station. Étant donné que, grâce à ces dernières vidéos, ils voient que, pendant le voyage, la personne en question lit le dernier numéro d'une revue anarchiste sortie depuis peu, ils demandent aussi l'historique du compte bancaire de la revue.

- Pour reconstruire à rebours le parcours qui l'a amenée à cette gare, ils se concentrent au début sur les trains Intercity, puisque le ticket est obligatoirement nominatif. Dans la liste obtenue par FSI,[7] ils identifient un acronyme qu'ils pensent relié à cette personne, alors ils vérifient où le ticket a été émis. Les vidéos de la gare où le ticket a été acheté ne sont plus disponibles, car la durée de leur conservation a été dépassée, alors ils essayent de reconstruire la manière dont la personne en question est arrivée dans la gare où elle a acheté le ticket.
- Après avoir mis de côté les Intercity, parce qu'ils n'ont pas trouvé de noms possiblement liés aux personnes sous surveillance, ils se concentrent sur les trains régionaux et ils demandent à FSI de leur communiquer le nombre de tickets émis, pour chaque train, par les distributeurs automatiques des gares de départ, de celles intermédiaires et d'autres, proches des localités « habituellement fréquentées » par des anarchistes : FSI leur transmet 150 pages de listes. Ils vérifient aussi les ferrys et les bus. Étant donné qu'ils ne trouvent rien, ils demandent les mêmes informations à propos de 69 autres gares, ainsi que la liste des amendes émises dans cinq trains régionaux. En même temps, ils demandent à FSI la liste de tous les tickets achetés, au cours des mois précédents, au nom de l'acronyme qu'ils ont remarqué, ainsi que d'activer une « alerte de signalisation automatique » au cas où celui-ci devait être à nouveau utilisé lors de l'achat de billets.
- Pour reconstruire les déplacements de certaines voitures, ils regardent les vidéos des caméras de différents péages autoroutiers ; quand ils repèrent une voiture jugée suspecte à un péage ils vérifient aussi les caméras des villes (qui filment la voie publique).

[7] *NdNTP :* Ferrovie dello Stato Italiane (FSI) est l'entreprise publique exploitant le réseau ferroviaire italien.

- Après avoir identifié le secteur où ils pensent que Stecco aurait pu se trouver, la DIGOS a demandé à installer cinq caméras de type « vidéo à longue distance », avec reconnaissance faciale, et dix caméras pour « enregistrement vidéo intérieur/extérieur » aux alentours d'une gare donnée, y compris aux arrêts de bus (urbains et extra-urbains). Il n'y a aucune trace de la demande faite par le procureur au juge, du coup nous ne savons pas si elles ont été effectivement installées ou pas. Les flics analysent aussi les vidéos des caméras présentes dans les bus. Ils demandent l'autorisation de mettre sous surveillance le téléphone d'une personne et de sa mère et d'avoir accès à leurs fadettes, parce que, par le passé, ils avaient loué des maisons à des compagnons dans ce secteur.
- Après avoir interpellé Stecco, ils montrent sa photo et posent des questions à de nombreux habitants du coin, jusqu'à ce qu'ils trouvent la maison où il aurait vécu. Ils prélèvent des empreintes digitales et des traces ADN sur tout ce qu'ils saisissent dans la maison.
- En ce qui concerne les recherches sur la téléphonie, il faut signaler que ce ne sont pas seulement les numéros de téléphone qui sont mis sous surveillance, mais aussi les boîtiers dans lesquels certaines cartes SIM ont été insérées, par le biais de leurs numéros IMEI.[8] Cela n'a pas lieu pour tous les numéros de téléphone, mais seulement pour ceux considérés comme plus « intéressants » et il semble qu'il suffise que la carte SIM soit insérée une seule fois (et utilisée). De plus, comme on le sait déjà, la surveillance inclut aussi la géolocalisation du téléphone, même si ce n'est pas un smartphone (bien que, dans ce cas, ils puissent connaître seulement les cellules radio auxquelles il se connecte et non sa position exacte).
- En ce qui concerne l'analyse de la téléphonie, une fois qu'ils ont resserré l'étau sur une zone géographique donnée, ils cherchent dans les listes déjà obtenues d'éventuels numéros d'anarchistes qui y habitent (c'est-à-dire si l'une des 69 personnes dont ils ont les fadettes a appelé quelqu'un qui habitait dans ce secteur, au cours des six années précé-

[8] *NdNTP :* Un numéro International Mobile Equipment Identity (IMEI, *identité internationale d'équipement mobile*) est un numéro qui identifie un téléphone de manière unique.

dentes), puis tous les appels effectués par Stecco au cours des cinq années précédentes (avant qu'il ne se mette au vert) à des numéros se trouvant dans cette zone.

- Ils cherchent dans les fadettes s'il y a eu des appels reçus de cabines téléphoniques. Ensuite, ils cherchent si, de la cabine dont ils ont les « fadettes », ont été passés des appels à des numéros de téléphone étrangers ; une fois qu'ils les ont trouvés, ils vérifient si ces numéros ont appelé les numéros apparaissant dans les fadettes. De plus, ils vérifient si, de cette cabine, ont été appelés des numéros de téléphone fixe ou mobile dans quatre régions italiennes données.
- Ils analysent les données du trafic téléphonique qui est passé par les cellules des opérateurs Tim, Wind, Vodafone et Iliad de neuf endroits, à des moments précis, quand ils pensent qu'il y aurait pu y avoir des connexions avec un hypothétique téléphone utilisé par Stecco. Étant donné que la quantité de données est énorme, ils essayent de les croiser avec les numéros qu'ils ont mis sous surveillance, puis avec tous les numéros qui ressortent des fadettes en leur possession. Ce type de recherche (le croisement de données issues de certaines cellules radio avec des numéros de téléphone repérés par l'analyse des fadettes) est répétée d'autres fois. En général, à plusieurs reprises on trouve l'analyse de fadettes téléphoniques, même très anciennes, et des tentatives de croiser les numéros ainsi obtenus avec les données qui sont progressivement collectées au cours de l'enquête.
- Malgré le fait qu'on ne les trouve pas dans le dossier, à de maintes reprises la DIGOS demande l'autorisation de télécharger les historiques de conversations Whatsapp et, dans un cas, aussi de Telegram.
- En ce qui concerne les enquêtes numériques, il faut signaler la tentative d'installer un logiciel espion (un virus informatique qui permet d'avoir un accès complet à l'appareil « infecté ») « par procédure en 1 clic », pour permettre de transformer le smartphone d'un proche de Stecco en micro pour des écoutes de discussions (définition technique : « autoriser la surveillance numérique active, avec d'éventuelles écoutes de discussions, par l'activation du micro du mobile de type Android, sans accès root »). Concrètement, ils envoient à cette personne un SMS avec un lien, qui, si elle l'avait ouvert, aurait installé

le virus. Étant donné que la personne n'a pas cliqué sur le lien, la DIGOS trouve le code PIN de son téléphone grâce à une caméra à haute définition installée à l'intérieur d'une voiture (ce qui leur permet de lire le code pendant qu'il est tapé sur le téléphone) et ils reçoivent l'autorisation d'installer directement le virus quand ils auront momentanément le téléphone en leur possession. Il ne semble pas que cela ait eu lieu, parce que, entre-temps, les enquêtes ont pris une autre direction.

- En ce qui concerne les emails, il semble que seul le fournisseur libero.it ait fourni les données sur les adresses email (y compris les fichiers de log), alors que d'autres fournisseurs n'auraient même pas répondu aux requêtes de la police (du moins, il n'y a pas de mention à ce sujet dans le dossier).
- En plus des emails, ils essayent d'obtenir toutes les données relatives aux services Microsoft Account et Google, y compris les achats effectués par le biais de ces plateformes.

À ce sujet, il est intéressant de noter l'analyse qu'ils font d'un GAIA ID,[9] pour lequel un numéro qu'ils pensent utilisé par Stecco reçoit un SMS. Quand on essaye d'accéder à la messagerie électronique Gmail depuis un appareil diffèrent de celui utilisé habituellement, Google demande une vérification additionnelle, en plus du mot de passe, en envoyant un SMS avec un code au numéro de téléphone lié à l'adresse email. Étant donné qu'un numéro lié à Stecco reçoit ce code, ils essayent de récupérer les données du compte Google en question. Pour ce faire, ils ont tapé ce numéro de téléphone dans la page de connexion de Gmail et, dans la page où on leur demande le mot de passe, ils ont cliqué avec le bouton droit de la souris et choisi « Code source de la page ». Une page avec le code HTML[10] s'est ouverte, ils ont tapé CTRL+F (recherche) et, dans l'espace pour la recherche, ils ont tapé les caractères « ,[" » pour trouver les 21

[9] *NdNTP :* Google Account and Id Administration (GAIA) est le système centralisé de connexion aux services de Google. Un GAIA ID est un identifiant de ce système de connexion, qui permet d'identifier chaque utilisateur·ice de services Google de manière unique.

[10] *NdNTP :* HyperText Markup Language (HTML) est le langage dans lequel sont écrites les pages web.

chiffres constituant le GAIA ID.[11] Pour savoir à qui est associé cet ID, ils ont utilisé l'un des services de Google, Google Maps (selon ce qu'ils disent, il semblerait qu'ils auraient pu utiliser n'importe quel service de Google, mais probablement Google Maps est celui où on laisse le plus souvent des avis ou des commentaires).

Concrètement, dans la barre d'adresse ils ont tapé « https://google.com/maps/contrib/ » suivi du GAIA ID pour visualiser tous les avis laissés par ce compte Google et identifier les adresses email reliées. Ils ont donc demandé à Google toutes les données liées aux adresses email, les numéros de téléphone, la date à laquelle ceux-ci ont été associés aux adresses email, les données personnelles liées au GAIA ID, ainsi que tous les fichiers de log de toute connexion à ce compte. Il semble qu'ils n'aient pas reçu de réponse.

Pour essayer de faire une synthèse compréhensible : à chaque GAIA ID peuvent être liées plusieurs adresses email et plusieurs numéros de téléphone et une fois que la police en connaît un, elle peut essayer de remonter aux autres.

Reprenons :

- À la suite d'une écoute pendant laquelle une adresse email est nommée, les flics demandent à Microsoft l'état civil, les données de facturation du compte au cas où il y aurait eu des achats sur le Microsoft Online Store, les fichiers de log des connexions, toutes les adresses email et les numéros de téléphone liés à l'adresse, ainsi que tous les clients qui se sont enregistrés avec un nom en lien avec cet email. De plus, ils demandent au site subito.it[12] la liste des fichiers de log et les adresses IP correspondant à cette adresse email.
- Dans un autre dossier, concernant la recherche d'un autre compagnon en cavale, nous avons trouvé ce passage à propos de la surveillance numérique, active et passive, d'un ordinateur : « Comme on le sait, au vu des technologies actuelles, il est assez difficile d'effectuer l'infection d'un ordinateur, puisque les variables qui déterminent le succès ou

[11] *NdNTP :* En 2025, cette technique pour trouver le GAIA ID correspondant à une adresse email ne semble plus fonctionner.

[12] *NdNTP :* Un site italien de petites annonces entre particuliers.

pas d'une telle opération (système d'exploitation, antivirus, carte réseau) sont nombreuses. Il est donc, comme d'habitude, indispensable d'effectuer d'abord une étude de faisabilité, par une surveillance passive, pour établir la typologie du système d'exploitation utilisé et les éventuels antivirus actifs, et ensuite effectuer la surveillance numérique active. Le modalités de l'installation du logiciel espion seront discutées ensuite avec les techniciens de l'entreprise chargée de l'installation. Lors des filatures, on a remarqué que […] laisse parfois son ordinateur dans le coffre de sa voiture […] quand il se rend au travail à […]. Avec l'autorisation du magistrat, le technicien pourrait installer un fichier, avec l'ordinateur éteint (cela est faisable rien qu'en laissant une clé USB ou un autre périphérique de stockage inséré dans l'ordinateur), et une fois l'ordinateur démarré, ce fichier serait automatiquement exécuté par l'ordinateur et installera d'autres petits logiciels malveillants, nécessaires pour effectuer l'étude des logiciels présents sur l'ordinateur, de façon à optimiser, par la suite, le logiciel espion qui permettra la surveillance numérique demandée. »

- Après la saisie d'une clé Tails, ils essayent d'en trouver le mot de passe avec le logiciel « bruteforce-luks ». Ils précisent qu'il n'est pas possible de donner une estimation de la durée d'une telle opération.

Chose remarquable, le seul des onze dossiers qui composent le dossier « Diana » qui est vide est celui avec le titre « Dépenses ». Il y a néanmoins quelques devis pour la location des dispositifs de surveillance, d'où, d'ailleurs, ressort que ceux pour la géolocalisation offrent souvent aussi l'« option écoute » ; il s'agit donc d'un seul objet, polyvalent. De plus, il semble que, depuis le Covid, il y ait aussi des postes d'écoute qu'ils peuvent utiliser depuis chez eux, en télétravail.

L'ouverture d'un dossier auprès du ministère de l'Intérieur et quelques notes qui en portent l'en-tête suggèrent l'implication des services secrets.

Dernière chose, mais non la moindre : pendant que l'enquête pour trouver Stecco était ouverte, les flics menaient au moins une autre enquête en vertu de l'article 270 bis, qui concernait aussi une partie des personnes sous enquête pour la cavale de Stecco. Juste pour donner une idée du caractère envahissant et quotidien du contrôle auquel certains compagnons sont soumis.

Il est utile de savoir que les flics peuvent passer des semaines à regarder les vidéos des caméras de gares, de trains, de péages autoroutiers, d'autobus, à la recherche d'images qui puissent suggérer des parcours et des destinations. Il essayent de le faire aussi à rebours, quand il s'agit d'un voyage qu'ils considèrent comme suspect, en reconstruisant une bonne partie d'un parcours à partir de sa fin, en cherchant les coïncidences entre les moments de « disparition », les jours, les horaires, les moyens utilisés.

Chacun·e en tirera les conséquences.

Qu'on se mette de manière encore plus incisive à la critique pratique du monde de la vidéosurveillance et du contrôle numérique, en tant que camp d'intervention essentiel pour que des rêves et des projets de subversion et de liberté soient encore possibles.

Que la chance soit avec ceux/celles qui sont en cavale, avec celles/ceux qui, dans la lutte pour la liberté, défient toute identification.

Dans le dossier de l'opération Diana sont reproduits, intégralement ou en partie, les dossiers de différentes procédures pénales. L'une d'entre elles est celle en vertu de l'article 270 bis, contre plusieurs compagnons, compagnonnes et proches de notre ami et compagnon Stecco. Ce que l'État a mis en œuvre pour l'interpeller est plutôt impressionnant.

No Trace Project / Pas de trace, pas de procès. Un ensemble d'outils pour aider les anarchistes et autres rebelles à **comprendre** les capacités de leurs ennemis, **saper** les efforts de surveillance, et au final **agir** sans se faire attraper.

Selon votre contexte, la possession de certains documents peut être criminalisée ou attirer une attention indésirable. Faites attention aux brochures que vous imprimez et à l'endroit où vous les conservez.