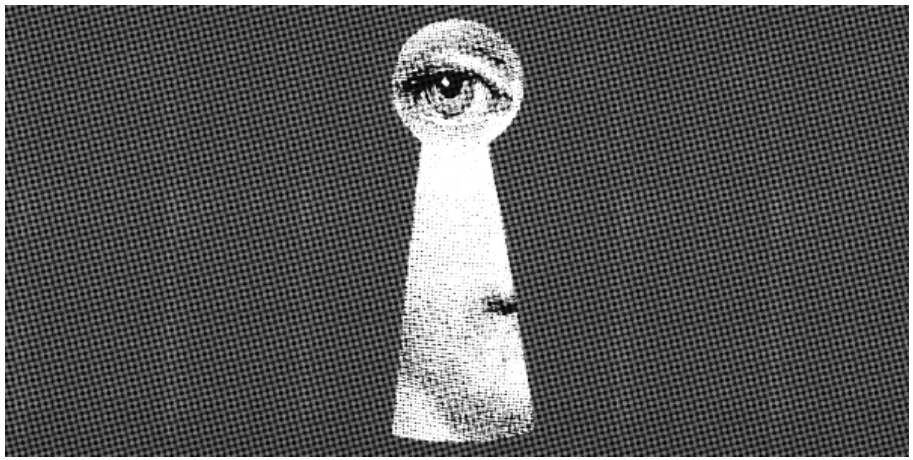
Im Aktenordner der Operation Diana sind die Dokumente zu verschiedenen Strafverfahren vollständig oder teilweise enthalten. Eines davon betrifft einen 270 bis im Fall mehrerer Genoss*innen und Personen, die unserem Freund und Genossen Stecco nahestehen. Was der Staat für seine Festnahme aufgeboten hat, ist ziemlich beeindruckend.

No Trace Project / No trace, no case. Eine Sammlung von Werkzeugen um Anarchist:innen und anderen Rebell:innen zu helfen, die Fähigkeiten ihrer Feinde zu **verstehen**, Überwachungsanstrenungen zu **unterlaufen**, und letztlich zu **handeln** ohne geschnappt zu werden.

Abhängig von deinem Kontext, kann es sein, dass der Besitz bestimmter Dokumente kriminalisiert wird oder ungewollte Aufmerksamkeit auf sich zieht. Sei bedacht bezüglich der Broschüren, die du druckst und wo du sie lagerst.

Nützliche Informationen

(aus den Ermittlungsakten der Operation Diana)



Nützliche Informationen (aus den Ermittlungsakten der Operation Diana)

Originaltext auf Italienisch

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

Deutsche Übersetzung

Blessed Is The Flame

blessed-is-the-flame.espivblogs.net/files/2025/09/DE-Gesegnet-Sei-Die-Flamme-Heft-4.pdf

Layout

No Trace Project

notrace.how/resources/de/#nutzliche-informationen

oft auch die „Überwachungsoption“ bieten. Es handelt sich also um ein einziges multifunktionales Gerät. Außerdem scheint es, dass aufgrund von COVID auch Home-Office-Abhörstationen eingerichtet werden können.

Die Eröffnung eines Dossiers im Innenministerium und einige Notizen, die die Aktenüberschrift enthalten, deuten auf die Beteiligung von Geheimdiensten hin.

Nicht zuletzt: Parallel zu den Ermittlungen zur Suche nach Stecco lief mindestens eine weitere Ermittlung für einen 270 bis, bei der ein Teil der Beschuldigten dieselben Personen wie die im 270 bis von Stecco war. Dies gibt einen Eindruck von der Allgegenwart und der täglichen Überwachung, der einige Genoss*innen unterworfen sind.

Es ist nützlich zu wissen, dass die Bullen auch Wochen damit verbringen können, Kameras von Bahnhöfen, Zügen, Autobahnraststätten und Bussen zu überprüfen, auf der Suche nach Bildern, die auf Routen und Ziele hindeuten. Sie versuchen, dies rückwirkend im Zusammenhang mit einer als verdächtig erachteten Reise zu tun, indem sie einen Großteil eines Weges rekonstruieren, beginnend mit dem Endpunkt der Reise und auf der Suche nach Übereinstimmungen zwischen Momenten des „Verschwindens“, Tagen, Uhrzeiten und genutzten Verkehrsmitteln.

Jede*r wird seine oder ihre eigenen Bewertungen vornehmen.

Möge die Kritik an der Überwachungstechnik und digitalen Kontrolle noch stärker in den Vordergrund rücken, als unentbehrliches Tätigkeitsfeld, um Träume und Projekte der Subversion und der Freiheit weiterhin zu ermöglichen.

Möge das Glück denen zuteilwerden, die Schatten in der Nacht sind, und denen, die in ihrem Kampf um Freiheit jede Identifikation herausfordern.

sehr schwierig, einen PC zu infizieren, da es zahlreiche Variablen gibt, die den Erfolg oder Misserfolg des Verfahrens bestimmen (Betriebssystem, Antivirenprogramme, Netzwerkkarten usw.). Daher ist es wie üblich unerlässlich, zunächst eine Machbarkeitsstudie durchzuführen, um das verwendete Betriebssystem und mögliche aktive Antivirenprogramme durch eine passive Überwachung zu bestimmen, bevor man mit der aktiven elektronischen Überwachung fortfährt. Die Methoden für die Injektion der Spyware werden anschließend mit den Technikern der Firma besprochen, die mit der Virusinstallation beauftragt sind. Aus Beobachtungsaktivitäten wurde festgestellt, dass […] der Computer manchmal im Kofferraum seines Autos zurückgelassen wird […] wenn er zur Arbeit geht in […]. Mit der Genehmigung des zuständigen Gerichts würde der Techniker eine Datei auf einem ausgeschalteten Computer installieren (dies ist nur möglich, wenn ein USB-Stick oder ein anderes Speichermedium im PC belassen wird), die beim Starten des Computers automatisch ausgeführt wird und weitere schadhafte Programme installieren wird, die notwendig sind, um die Softwareumgebung des Geräts zu analysieren und dann die Spyware zu optimieren, die die angeforderte elektronische Überwachung ermöglichen wird."

- Nachdem ein Tails-USB-Stick beschlagnahmt wurde, versuchen sie, das Passwort mit dem Programm „bruteforce-luks" zu ermitteln. In der Kommunikation wird betont, dass die Zeit für diese Operation nicht geschätzt werden kann.

Bemerkenswert ist, dass der einzige Ordner unter den 11, die die „Diana"-Ermittlungen bilden, der leer ist, der mit der Aufschrift „Ausgaben". Es gibt jedoch einige Kostenvoranschläge für die Anmietung von Geräten für die Überwachung, aus denen hervorgeht, dass solche zur Lokalisierung

In Italien, im Rahmen der sogenannten Operation Diana, wurde der Genosse und Flüchtige Luca Dolce, auch bekannt als Stecco, nach einer äußerst hartnäckigen Anstrengung der Polizei gefunden, verhaftet und schließlich im März 2025 zu einer Haftstrafe von 3 Jahren und 6 Monaten verurteilt, weil er gefälschte Dokumente für einen weiteren flüchtigen Genossen, Juan, angefertigt hatte.

Die Anzahl des eingesetzten Personals und der Mittel, die die Polizei für seine Lokalisierung mobilisierte, ist wirklich beeindruckend. Die Ermittlungsakte dieser Operation stellt einen wahren Schatz für Anarchistinnen in Aktion dar und für alle, die sich allgemein dafür interessieren, wie die Polizei vorgeht, um Personen zu überwachen und zu identifizieren. In diesem Artikel präsentieren wir eine Zusammenfassung der Ermittlungsakte der Operation Diana, die von Genossinnen geschrieben und im italienischen Anti-Informationsmedium Il Rovescio veröffentlicht wurde.

Im Aktenordner der Operation Diana sind die Dokumente zu verschiedenen Strafverfahren vollständig oder teilweise enthalten. Eines davon betrifft einen 270 bis im Fall mehrerer Genoss*innen und Personen, die unserem Freund und Genossen Stecco nahestehen.

Was der Staat für seine Festnahme aufgeboten hat, ist ziemlich beeindruckend. Wenn man bedenkt, dass Stecco, als er das Zelt abbrach, noch eine Haftstrafe von 3 Jahren und 6 Monaten zu verbüßen hatte, zeigt die Disproportionalität zwischen seiner Verurteilung und dem behördlichen Eifer, ihn zu finden, wie unerträglich das System es findet, dass sich jemand seinen Gefängnissen entziehen kann; und wie das für Anarchist*innen reservierte Vorgehen unter einem allgemein repressiven Rollout einen unbestreitbar selektiven Charakter hat.

Ein aktuelles Wissen über die von der politischen Polizei gegen Genoss*innen eingesetzten Techniken geht oft durch das Studium der Akten der polizeilichen und gerichtlichen Ermittlungen. Deshalb ist es wichtig, dass die daraus gewonnenen Informationen verbreitet werden.

Dabei muss immer an zwei Aspekte gedacht werden: der erste ist, dass es sich um Material des Feindes handelt; der zweite ist, dass die (natürlich selektierte und ohne die Nennung von Namen und Details, die in den Akten erscheinen) Verbreitung dieses Materials unbeabsichtigt das Gefühl einer Art Allmacht des Feindes erzeugen könnte, verbunden mit Paranoia und einem mangelnden Vertrauen in die eigenen Mittel. Es ist daher gut, daran zu erinnern, dass der Einsatz von Menschen und Mitteln bei der Suche nach Flüchtigen nicht dasselbe ist, wie das Monitoring/Ermitteln von anderen Umständen, die in den Bewegungen und Kämpfen vorkommen; dass, trotz des polizeilich-technologischen Fortschritts, einige gesuchte Genossinnen monatelang und jahrelang die Freiheit genossen haben; dass

zu erlangen. Sie haben die Telefonnummer in die Gmail-Anmeldeseite eingegeben und auf der Passwort-Seite mit der rechten Maustaste auf „Seitenquelle anzeigen“ geklickt. Daraufhin öffnete sich ein Fenster mit dem HTML-Code, sie gaben CTRL+F (Suche) ein und fanden die 21 Ziffern, die die GAIA-ID bilden. Um zu erfahren, zu welchem Konto diese ID gehört, verwendeten sie einen Google-Dienst, speziell Google Maps.

Sie gaben in die Adresszeile „https://google.com/maps/contrib/GAIA-ID“ ein, um alle Bewertungen zu sehen, die mit diesem Google-Konto abgegeben wurden, und so die zugehörigen E-Mail-Adressen zu ermitteln. Anschließend forderten sie von Google alle Registrierungsdaten zu den E-Mails, Telefonnummern, dem Datum der Verknüpfung mit der E-Mail-Adresse sowie alle Log-Dateien der Verbindungen zu diesem Konto an. Es scheint, dass sie keine Antwort erhalten haben.

- Nach einer Umweltüberwachung, bei der eine E-Mail-Adresse genannt wird, fragen sie bei Microsoft nach den Registrierungsdaten, den Rechnungsinformationen des Accounts, falls Käufe im Microsoft Online Store getätigt wurden, den IP-Verbindungs-Logs, allen mit dieser E-Mail-Adresse verbundenen E-Mail-Adressen und Telefonnummern sowie allen Personen, die sich mit einem Namen registriert haben, der mit dieser E-Mail-Adresse verbunden ist. Zudem fragen sie den Standort, die geographischen Verbindungen und spezifische Aktivitäten an, falls sie mit anderen Anarchist*innen zusammenarbeiten.
- In einer anderen Akte, die mit der Suche nach einem anderen flüchtigen Genoss*innen zusammenhängt, haben wir diesen Abschnitt zur aktiven und passiven Überwachung eines Computers gefunden: „Wie bekannt, ist es angesichts der aktuellen Technologien

von Gesprächen durch Aktivierung eines Mikrofons auf einem Android-Gerät ohne Root-Zugang“). Praktisch wurde dieser Person ein SMS mit einem Link geschickt, der, wenn er angeklickt wurde, zur Installation des Virus geführt hätte. Da die Person den Link nicht angeklickt hat, nachdem der PIN-Code ihres Telefons mithilfe einer hochauflösenden Kamera in ihrem Auto ermittelt wurde (die es ermöglichte, den Code zu lesen, während er auf dem Telefon eingegeben wurde), wurde die DIGOS autorisiert, das Virus direkt zu installieren, sobald sie temporären Zugriff auf das Telefon erhalten haben. Dies scheint jedoch nicht geschehen zu sein, da sich die Ermittlungen inzwischen in eine andere Richtung entwickelt haben.

- Bezüglich der E-Mails scheint nur libero.it die Daten zu den E-Mail-Adressen (einschließlich der Log-Dateien) zur Verfügung gestellt zu haben, während andere Anbieter offenbar nicht auf die Anfragen reagierten (oder zumindest keine Erwähnung davon gemacht wurde).
- Neben den E-Mails versuchen sie auch, alle Daten im Zusammenhang mit Microsoft Account und Google-Diensten zu erhalten, einschließlich der über diese Plattformen getätigten Käufe.

In diesem Zusammenhang ist es interessant zu bemerken, dass eine Analyse des GAIA-IDs (Google Account and Id Administration) durchgeführt wurde, bei der eine Nummer, die Stecco zugeordnet wird, eine SMS erhält. Praktisch, wenn versucht wird, auf ein Gmail-Konto von einem Gerät zuzugreifen, das normalerweise nicht genutzt wird, fordert Google eine zusätzliche Bestätigung des Passworts an, indem ein SMS mit einem Code an eine Nummer gesendet wird, die mit der E-Mail-Adresse verbunden ist. Da eine mit Stecco verbundene Nummer diesen Code empfängt, versuchen sie, die Daten des zugehörigen Google-Kontos

es weiterhin Genossinnen gibt, die in Europa und weltweit „uccel di bosco“ (untergetaucht) sind.

Zu wissen, wie sich die Gegenseite bewegt, ist notwendig, um die am besten geeigneten Gegenmaßnahmen zu ergreifen, aus den Fehlern zu lernen und Erfahrungen zu bewahren.

Wir beginnen mit einigen quantitativen Daten, um einen Eindruck vom Ausmaß des polizeilichen Eingreifens zu vermitteln:

- Kameras vor 6 Wohnungen.
- Umweltüberwachungen in der Wohnung einer Person, die Stecco nahesteht, von weiteren Personen, die mit einer Person in Verbindung stehen, die besonders „aufmerksam“ beobachtet wurde, und im anarchistischen Raum „El Tavan“.
- Telefonüberwachungen von über 40 Personen: Genoss*innen, aber auch Freunde und nahe stehende Personen.
- Es wurden gezielte Umweltüberwachungen in einem Fall angeordnet, in dem angenommen wurde, dass eine Person, die Stecco nahesteht, eine Person treffen könnte, die laut der DIGOS [Divisione Investigazioni Generali e Operazioni Speciali] ihm Informationen über ihn geben könnte.
- Eine besonders „aufmerksam“ beobachtete Person wurde mindestens einmal von den Diensten verfolgt (der Berichtstitel lautet „Ministero degli interni“, während alle anderen Berichte von verschiedenen Polizeidienststellen stammen).
- Analyse der historischen Telefonverbindungsdaten von 69 Personen und einer Telefonzelle (die maximale Rückverfolgungszeit beträgt 72 Monate).

- GPS-Tracker wurden in 12 Autos installiert. Für einige nahe Stecco stehende Personen gab es auch Umwelt- und Videoüberwachung.
- Die Kennzeichen von 311 Autos wurden „beobachtet".
- Bankauszüge von 59 Personen wurden angefordert, um „verdächtige" Bewegungen zu überprüfen, die auf mögliche finanzielle Unterstützung für die Flucht hindeuten könnten.
- Ein Trackinggerät (ein GSM-Tracker, nicht satellitengestützt, sondern mobiltelefonbasiert, vom Typ „Spora", ein miniaturisierter Tracker, der in Echtzeit per SMS an ein bei der Polizei verwendetes Telefon die angehängte Funkzelle meldet) wurde an einem Fahrrad installiert, von dem angenommen wurde, dass es Stecco gehörte, nachdem es mit einer Kamera in einem Land, in dem er während seiner Fluchtzeit gesehen wurde, lokalisiert wurde.
- In diesem Fall, wie auch im Fall eines anderen untergetauchten Genossen, wurden gefälschte Dokumente gefunden, deren Personalien echten existierenden Personen zugeordnet wurden. Dies führte zu einer Reihe von Ermittlungen und Befragungen der betreffenden Personen, mit dem Ziel, Bewegungen, Hotelübernachtungen, Kontobewegungen zu vergleichen (und auch beispielsweise die „Decathlon-Karte", auf der die Historie der getätigten Einkäufe hinterlassen wurde) über mehrere Jahre zurück (mehr als 10 Jahre).
- Die politische Polizei von Treviso, Padua, Verona, Brescia, Bergamo, Mailand, Trient, Triest, Genua wurde mobilisiert. Ab dem Zeitpunkt, an dem sie begannen, „den Kreis zu ziehen", erhielt die DIGOS in Trient dauerhaft Unterstützungspersonal, sicher mindestens einen Agenten aus Triest.

ob diese Nummern jemals die Nummern angerufen haben, die aus den historischen Aufzeichnungen hervorgegangen sind. Sie überprüfen außerdem, ob von der Zelle aus Festnetz- oder Mobilfunknummern in vier italienischen Regionen angerufen wurden.

- Sie analysieren die Mobilfunkdaten von Tim, Wind, Vodafone und Iliad in neun Städten zu bestimmten Zeiten, in denen sie vermuten, dass es Kontakt mit einem möglichen Telefon von Stecco gegeben haben könnte. Da das Datenvolumen enorm ist, versuchen sie, diese mit den überwachten Nummern zu kombinieren und dann mit allen Nummern, die aus den erfassten Aufzeichnungen hervorgehen. Diese Art der Recherche (Datenabgleich zwischen bestimmten Funkzellen und Telefonnummern, die durch die Analyse von historischen Aufzeichnungen ermittelt wurden) wird mehrfach wiederholt. Im Allgemeinen finden sich an mehreren Stellen im Verlauf die Analyse von historischen Aufzeichnungen, auch weit in der Vergangenheit, und Versuche, diese extrahierten Nummern mit den fortlaufend gesammelten Daten aus der Ermittlung abzugleichen.
- Obwohl es in den Überwachungen keine Hinweise darauf gibt, hat die DIGOS mehrfach um die Genehmigung gebeten, WhatsApp-Chats herunterzuladen und in einem Fall auch Telegram-Chats.
- Was die elektronischen Suchen betrifft, ist es bemerkenswert, dass der Versuch unternommen wurde, Spyware zu installieren (ein Computervirus, der vollständigen Zugriff auf das „infizierte" Gerät ermöglicht) „mittels des 1-Klick-Verfahrens", das es ermöglicht, das Smartphone einer Person, die Stecco nahesteht, in ein Überwachungsmikrofon zu verwandeln (technische Definition: „Autorisierung der aktiven elektronischen Überwachung, möglicherweise auch der Überwachung

sind. Sie fordern die Überwachung einer Person und ihrer Mutter sowie Zugang zu deren Telefondaten an, weil sie in der Vergangenheit in der Nähe Wohnungen an Genoss*innen vermietet haben sollen.

- Nachdem Stecco verhaftet wurde, zeigen sie sein Foto und befragen verschiedene Personen vor Ort, bis sie das Haus finden, in dem er sich aufgehalten haben soll. Sie nehmen Fingerabdrücke und DNA von allem, was sie im Haus beschlagnahmt haben.
- Was die Suche über Telefone betrifft, so wird nicht nur die Telefonnummer überwacht, sondern auch die Geräte, in die einige SIM-Karten eingelegt wurden, anhand der IMEI-Nummer. Dies geschieht nicht für alle Nummern, sondern nur für die, die als „interessanter" erachtet werden, und es scheint ausreichend zu sein, dass die SIM-Karte nur einmal eingelegt (und verwendet) wird. Zudem, wie bereitsbekannt, erfolgt bei der Überwachung auch die Geolokalisierung des Telefons, auch bei Nicht-Smartphones (obwohl in diesem Fall nur die Funkzellen identifiziert werden, mit denen das Gerät verbunden war, und nicht der genaue Standort).
- Auf der Grundlage der Analyse der Telefondaten suchen sie in den bereits gesammelten Aufzeichnungen nach Telefonnummern von Anarchist*innen, die in der gleichen Region wohnen (d.h., ob eine der 69 Personen, deren Telefonaufzeichnungen sie haben, in den letzten 6 Jahren jemanden angerufen hat, der dort lebt). Dann suchen sie alle Anrufe, die Stecco in den 5 Jahren vor seiner Flucht an Nummern gemacht hat, die in dieser Region waren.
- Sie suchen in den historischen Daten nach Anrufen, die von Telefonzellen getätigt wurden. Dann suchen sie, ob von der Telefonzelle, deren Aufzeichnungen sie haben, Anrufe an ausländische Nummern getätigt wurden. Nachdem sie diese gefunden haben, sehen sie,

Für eine qualitativere Analyse müssen wir die verwendeten Techniken näher betrachten. Es sei gesagt, dass die Ermittlungen in zwei Richtungen laufen: die Analyse einer riesigen Menge an Telefondaten und die fast ständige Überwachung bestimmter Personen, mit besonderem Augenmerk auf deren Abwesenheit an ihren jeweiligen Wohnorten. Wenn diese Personen wieder lokalisiert werden, wird versucht, ihre Bewegungen so weit wie möglich rückwirkend zu rekonstruieren. Die Datensammlung erfolgt ruhig und systematisch. Hier einige Beispiele:

- Zwei Genossinnen, die mit dem Zug reisen, werden von vier Agentinnen der DIGOS verfolgt, die sich jeweils vorne und hinten im Zug positionieren. In jedem Zwischenhalt stehen dann zwei Polizistinnen in Zivil bereit, falls die Genossinnen den Zug verlassen; zu diesem Zweck wurde die politische Polizei aus sieben Provinzen mobilisiert. Laut den Akten wurde diese Verfolgung auf den letzten Drücker angeordnet, als die Polizei am Abend zuvor in Echtzeit aus den Mikrofonen, die in der Wohnung einer der beiden betroffenen Personen installiert waren, hörte, dass diese am nächsten Tag mit dem Zug fahren würde.
- Aus den Akten geht hervor, dass die Polizist*innen neben der Anfrage an RFI [italienischer Bahn-Infrastrukturanbieter] zur Einsicht der Kameras in den Bahnhöfen auch den Haftrichter um die Installation spezieller Kameras im Bahnhof Rovereto baten, um sie direkt in der Polizeiinspektion einsehen zu können. Sie konnten auch einsehen, welche Tickets an den Automaten verkauft wurden, welche Suchanfragen auch ohne Ticketkauf durchgeführt wurden und auf welche Kameras, die teils direkt an den Automaten installiert sind, zugegriffen wurde. Diese Kameras speichern die Aufnahmen für maximal 10 Tage (obwohl die allgemeine Speicherdauer für sicherheitsrelevante Infrastruktu-

ren laut einer Verordnung von 2010 nur 7 Tage beträgt, es sei denn, es gibt spezifische Anfragen).

- Nachdem sie festgestellt haben, dass eine besonders „aufmerksam“ beobachtete Person die Fahrpläne für Züge zu einer bestimmten Stadt über einen Ticketautomaten abgerufen hatte, wurden die Kameras des Bahnhofs dieser Stadt und von mindestens vier anderen Bahnhöfen ausgewertet, nachdem diese Person das Haus verlassen hatte. Es ist wahrscheinlich, dass auch die Daten anderer Bahnhöfe entlang der Strecken, die zu der Stadt führen, überprüft wurden. Da die Daten nach 7 Tagen gelöscht werden, fuhr die DIGOS eilig zu den RFI-Büros in Lombardei, weil sie glaubten, die Person in einem Bahnhof identifiziert zu haben (der weder der gesuchte noch der nahegelegene Bahnhof war), in dem sie 7 Tage zuvor gewesen war und wo die Gefahr bestand, dass die Bilder überschrieben werden, bevor der Download abgeschlossen war.
- Im Versuch, den Weg der Person nachzuvollziehen, werden auch die Daten eines Geschäfts außerhalb des Bahnhofs überprüft, in dem sie angenommen wird, sowie die Kameras des Zuges, von dem angenommen wird, dass sie in diesem Bahnhof eingestiegen ist. Da sie während der Reise in den Aufnahmen ein Genoss*innen-Magazin las, das gerade erschienen war, fragen sie nach den Bankdaten auch für dieses Magazin.
- Um rückwirkend den Weg zu rekonstruieren, der sie zu diesem Bahnhof geführt hat, konzentrieren sie sich zunächst auf die Intercity-Züge, da diese Tickets mit Namen erfordern. Nachdem sie anhand der Liste von FSI ein Akronym gefunden haben, das sie für diese Person halten, überprüfen sie, wo das Ticket dafür ausgestellt wurde. Da sie aufgrund der Ablaufzeit der Aufbewahrung der Aufnahmen die Videos des Bahnhofs, an dem das Ticket gekauft wurde, nicht mehr

einsehen konnten, versuchen sie, zu rekonstruieren, wie die Person zu diesem Bahnhof gekommen ist.

- Nachdem sie die Intercity-Züge ausgeschlossen haben, weil sie keinen zutreffenden Namen finden konnten, konzentrieren sie sich auf die Regionalzüge und fordern von FSI Informationen zu den ausgestellten Tickets aus den Automaten an den Abfahrtsstationen, an den Zwischenstationen und an weiteren in der Nähe gelegenen, die „häufig von Anarchist*innen frequentiert“ werden: 150 Seiten Listen, die von den Eisenbahngesellschaften übermittelt wurden. Sie überprüfen auch Fähren und Busse. Da sie nichts finden, bitten sie erneut um die gleichen Daten von 69 weiteren Bahnhöfen und über eventuell auf den Zügen verhängte Bußgelder für 5 Regionalzüge. Parallel dazu fordern sie von den Eisenbahngesellschaften eine Liste aller Tickets an, die in den vergangenen Monaten mit diesem Akronym gekauft wurden, und aktivieren einen „Automatischen Warnhinweis“, falls dieses Akronym wieder für den Ticketkauf verwendet wird.
- Zur Rekonstruktion der Bewegungen bestimmter Autos werden Kameras an verschiedenen Autobahnraststätten überprüft. Sobald ein Auto an einer Raststätte lokalisiert wird, das verdächtig erscheint, werden auch die Straßenkameras der Stadt überprüft.
- Nachdem sie die Gegend ermittelt haben, in der Stecco vermutet wird, fordert die DIGOS die Installation von 5 „Langstrecken-Videokameras“ mit Gesichtserkennung und 10 Kameras für „Innen-/Außenaufnahmen“ rund um einen bestimmten Bahnhof, einschließlich städtischer und überregionaler Bushaltestellen. Es gibt keine Aufzeichnungen über die Anfrage des Staatsanwalts an den Richter, sodass nicht bekannt ist, ob diese Kameras schließlich installiert wurden. Sie analysieren auch die Bilder von Kameras, die an Bussen installiert