PQM
IL Riformista
LA GIUSTIZIA CHE NON VI RACCONTANO

Sabato 7 dicembre 2024

Anno II - numero **QUARANTASEI**

Direttore: **Gian Domenico Caiazza**

Minority Report (svegliatevi, c'è poco da scherzare)

Gian Domenico Caiazza

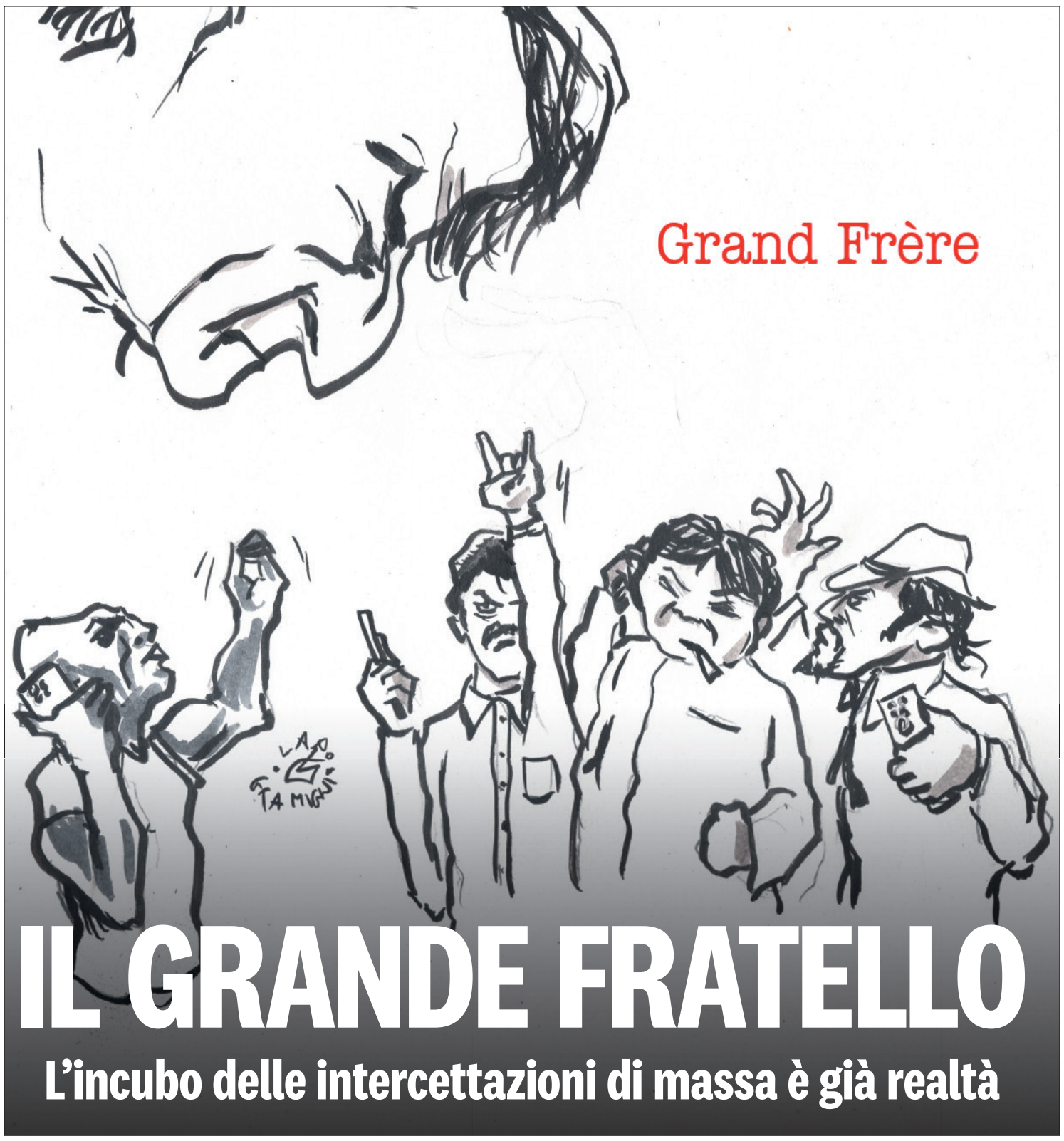
Questa storia dei cripto-telefonini, della quale sembra non interessare granché a nessuno (nella politica, nel mondo della giustizia, nell'accademia, nel giornalismo), può essere -forse già lo è - la porta di ingresso nel mondo del Grande Fratello. Non c'è un filo di retorica in quello che sto dicendo, e vi basterà leggere con attenzione questo numero di PQM per comprenderlo.

È accaduto nel 2020 un terremoto di grado altissimo, epicentro a Lille, piccola cittadina francese, poi rovinosamente propagatosi già in tutta Europa; ma è un terremoto silenzioso, del quale solo ora ci stiamo rendendo conto. Il Giudice di Lille dispone, come se niente fosse, non intercettazioni di persone sospettate di commettere gravi reati, ma direttamente l'inoculazione di un trojan nel server di una società che produce e gestisce (senza autorizzazione) telefonia criptata. Se qualcuno usa telefoni criptati per non essere intercettato - questo è il ragionamento velenoso - beh vuol dire che ha qualcosa da nascondere; e dato che i clienti di quella società di telefonia sono quasi duecentomila, faccio una bella cosa, intercetto direttamente il server. Me li ascolto tutti (in realtà sono soprattutto chat). Poi convoco le Polizie di tutta Europa, e ci mettiamo a selezionare le cose brutte, un cherry-picking, come direbbero gli inglesi: traffico internazionale di stupefacenti, pedopornografia, omicidi, e così via.

Poi le Procure territorialmente interessate mi mandano una bella letterina (OIE, ordine di investigazione europeo), "mi mandi quella roba su quelle cose brutte che abbiamo insieme selezionato?", e io gliele mando (si chiama cooperazione internazionale), così loro ci impacchettano bei processi, con la prova comodamente pronta e servita per essere utilizzata. In Europa qualche giudice insorge, ma non vi starete mica illudendo spero, la nostra Magistratura non ha formazione, indole, riflessi di tipo garantista. Reagisce il Tribunale di Berlino che dice: ma che roba è questa porcheria, siete impazziti?! E chiede alla Corte di Giustizia Europea (sì, proprio quella della vicenda Paesi Sicuri, che però qui da noi diventa un oracolo o carta straccia a seconda di come ci torna comodo) di dire preventivamente la sua. E la CGUE dice: teoricamente e a condizioni rigorosissime - per esempio in materia di allarme terrorismo - si può anche fare, ma naturalmente occorre che siano rispettate le regole di acquisizione della prova fissate dagli ordinamenti degli Stati nazionali.

Allora siamo salvi, pensiamo noi poveri ingenui, visto che in Italia (e in tutta Europa grosso modo) le intercettazioni preventive a strascico non sono processualmente utilizzabili, ma solo quelle disposte su persone già raggiunte da gravi indizi di reato. Si, buonanotte. Ci pensano le Sezioni Unite della Cassazione, che trovano una bella soluzione pilatesca tipicamente italica - sono documenti, non sono intercettazioni, e poi se anche fossero, guardate bene che le preventive in Europa non sono vietate, quindi distinguiamo, valutiamo, e bla bla bla - e tra tante belle parole e riflessioni, alla fine della fiera danno il via libera. Ed infatti cominciano a fioccare condanne a go-go, dove i soliti avvocati rompiballe invocano inutilmente la Corte di Giustizia Europea, ricevendone sonore pernacchie. Abbiamo per le mani tutta questa bella roba per condannare comodamente, senza sforzo, senza indagini, dei criminali, e voi mi tirate fuori queste chiacchiere sui princìpi e sulle regole? Suvvia!

Nel frattempo, sempre in Francia (una volta patria della rivoluzione contro la tirannia) scoppia il caso Telegram (leggete la nostra Quarta Pagina). Se - come si dice a Roma - non ci diamo tutti una svegliata, mentre discettiamo serafici del limite dei 45 giorni di durata delle nostre intercettazioni, siamo già tutti dentro Minority Report. Buona lettura!



Rigurgiti inquisitori

SKY-ECC, COME NASCE IL GRANDE FRATELLO

Francesco Catanzaro

Francesco Iacopino

La vicenda *Sky-Ecc*, dal nome della società canadese finita nel mirino degli inquirenti francesi, nasce nel 2016. Per conoscerla in dettaglio, però, bisogna partire dal Belgio e dall'Olanda. È in quei paesi che gli investigatori, nel corso di un'indagine congiunta di contrasto al narcotraffico transnazionale, effettuano perquisizioni e sequestri rinvenendo anche i c.d. "criptotelefonini". Si tratta di dispositivi fino ad allora sconosciuti alla polizia giudiziaria procedente. Avviati i primi accertamenti informatici, gli inquirenti scoprono che gli apparecchi sono collegati alla rete telematica di *Sky-Ecc*, azienda operante in Europa mediante *servers* ubicati a Roubaix, cittadina francese ricadente nel distretto giudiziario di Lille. Scoprono, ancora, che quei "criptotelefonini" hanno ricevuto una larga diffusione in Belgio.

Segue a pag. 2

La nuova schiavitù

CHAT CRIPTATE E TIRANNIE TECNOLOGICHE SULLA PROVA

Luca Marafioti

Quanti erano in fervente attesa di letture giurisprudenziali garantiste del rapporto tra criptofonini e processo penale sono rimasti delusi quest'anno. Dispositivi impenetrabili per definizione; eppure i francesi erano entrati da *hacker* nel *server* che ne conteneva i dati, forse con un *trojan horse*, mettendo sostanzialmente a disposizione di varie autorità giudiziarie una messe di *chat* altrimenti inaccessibili. La Cassazione a Sezioni Unite doveva chiarire tra l'altro due cose: strumento processuale per acquisire i dati digitali e tipo di controllo giurisdizionale italiano per l'ingresso di quanto decriptato. Si lascia, invece, aperto l'inquadramento giuridico delle *chat* criptate, senza chiarire se si tratta di "documenti" o "dati di traffico", adottandosi una pilatesca motivazione "in ipotesi". E, comunque, cambia poco: non sarebbe necessario alcun previo intervento giudiziario italiano.

Segue a pag. 3

Giustizia transnazionale

L'IPOCRISIA DEL MUTUO RICONOSCIMENTO

Oliviero Mazza

La libera circolazione dei cittadini all'interno dell'Unione Europea ha indubbiamente facilitato anche le attività criminose su scala transnazionale. Partendo da questa elementare constatazione, il diritto eurounitario avrebbe potuto imporre un sistema penale e processuale unico, sul modello federale statunitense, ma tale soluzione avrebbe messo in discussione una delle massime prerogative della sovranità nazionale, rappresentata proprio dall'amministrazione della giustizia in ambito penale. Scartata, quindi, tale possibilità, dal 1992 si è intrapresa la strada di promuovere la cooperazione giudiziaria rafforzata tra gli Stati membri, consentendo un dialogo diretto fra i magistrati dei diversi Paesi.

La cooperazione rafforzata presenta, però, il non secondario inconveniente di scontrarsi con il problema della diversità degli ordinamenti di ogni Stato.

Segue a pag. 3

€ 2,00 in Italia
solo per gli acquirenti in edicola
e fino ad esaurimento copie

Redazione e amministrazione
via di Pallacorda 7 - Roma - Tel 06 32876214
Sped. Abb. Post., Art. 1, Legge 46/04 del 27/02/2004 - Roma

RIGURGITI INQUISITORI

SKY-ECC, COME NASCE IL GRANDE FRATELLO

Francesco Catanzaro*
Francesco Iacopino*

SEGUE DALLA PRIMA

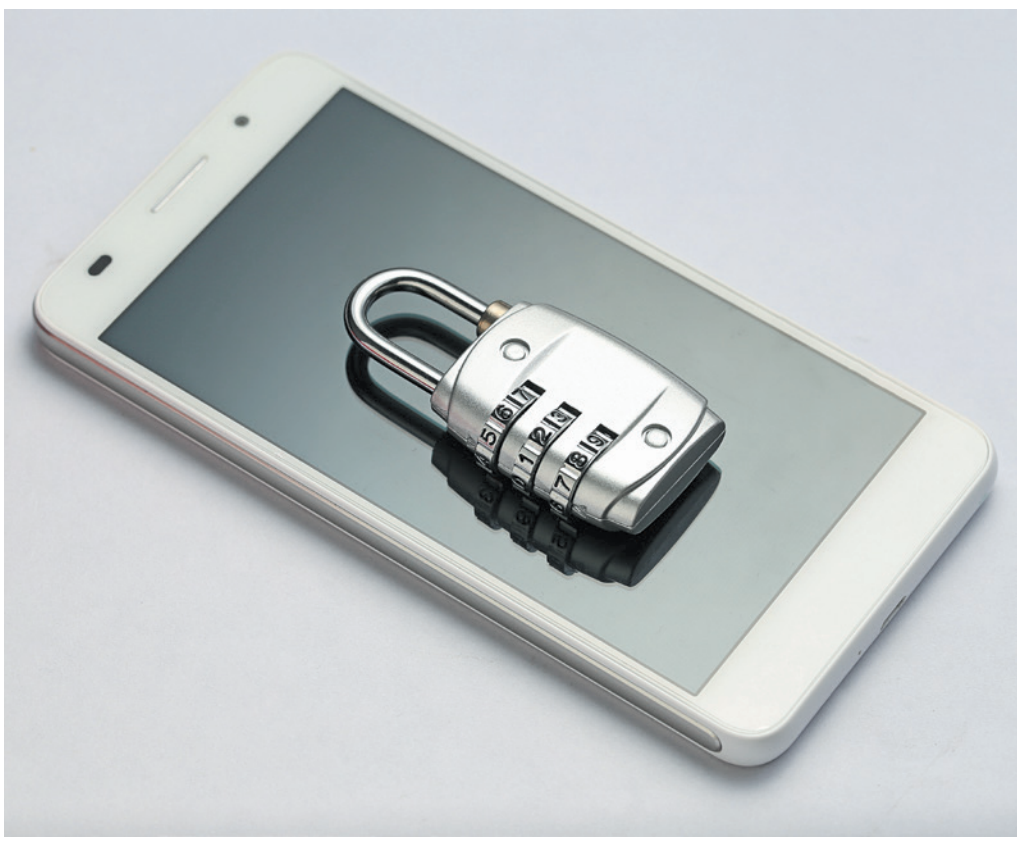
Tant'è che nel dicembre 2018 chiedono assistenza giudiziaria alle autorità francesi. Ed è a questo punto che, nel 2019, parte l'indagine *interna*. Emerge subito un servizio di comunicazioni telematiche abusivo, essendo la società canadese priva di licenze e/o concessioni governative. Emerge, ancora, il largo utilizzo di quei dispositivi anche Oltralpe, tanto da individuare in poco tempo migliaia di messaggi trasmessi da utenti francesi.
Giunti a questo punto, in un sistema penale liberale (fatto di regole poste a tutela dei diritti fondamentali, tra i quali quello alla riservatezza delle comunicazioni), le autorità transalpine avrebbero potuto porre sotto sequestro i *servers*, in modo tale da impedire a quei ripetitori di continuare a funzionare; o, in alternativa, concentrarsi sulle indagini per narcotraffico, disponendo l'intercettazione delle comunicazioni delle (sole) utenze già individuate e censite dalle medesime autorità francesi, belghe e olandesi. La storia, invece, ha preso un'altra piega. I Giudici di Lille, lungi dal selezionare le utenze di interesse investigativo, hanno autorizzato le intercettazioni dei ripetitori della piattaforma telematica di *Sky-Ecc*, ponendo un orecchio digitale sui *servers* ospitanti le conversazioni di tutti gli utenti della società, non solo degli indagati.

Il flusso indiscriminato di comunicazioni così acquisito, però, in quanto "criptato", ha impedito di conoscerne nell'immediato il contenuto. Ed è così che, nel 2020, per scoperchiare il vaso di pandora, è intervenuta in soccorso l'autorizzazione dei Giudici di Parigi all'installazione di un (ulteriore) dispositivo informatico all'interno dei due *servers Sky-Ecc*, in grado di procedere, attraverso la tecnica del "*Man in the middle*" (dell'"Uomo nel mezzo"), alla decodifica dei messaggi, rendendo il testo "in chiaro" e comprensibile (anche) per gli inquirenti.
È di solare evidenza la abbondante pioggia di conversazioni caduta, all'improvviso, sul terreno operativo delle autorità francesi. Un quantitativo enorme di intercettazioni, non solo legate alle indagini di narcotraffico e agli indagati nel procedimento originario, ma estese a tutte le centinaia di migliaia di (ignari) utenti di *Sky-Ecc* e alle loro comunicazioni riservate (non necessariamente illecite), acquisite "fuori" da un'attività investigativa legittimamente avviata. A ciò si aggiunga che sull'algoritmo di decodifica, frutto di sofisticate tecnologie militari in uso all'intelligence transalpina, è stato apposto in Francia il segreto di Stato, legittimato anche dalle Giurisdizioni superiori, con conseguente sbarramento opposto alle difese sulle modalità di acquisizione della relativa informazione probatoria. A questo punto, il vastissimo raccolto investigativo è stato messo a disposizione delle autorità nazionali, le quali, dopo averlo acquisito per quanto di interesse, non hanno esitato a farne largo uso nei processi penali interni.
Così ricostruiti i termini della vicenda *Sky-Ecc* (ma analoghe riflessioni si possono sviluppare anche per *Encro-Chat*), è chiaro che la stessa solleva molteplici e rilevanti interrogativi. L'enorme potenziale sviluppato dalle tecnologie digitali mostra con forza la complessità delle sfide delicate che ci attendono nella regolazione del difficile equilibrio autorità e libertà, tra esigenze investigative e tutela della riservatezza delle comunicazioni. Se, come pare, le prime dovessero prevalere consentendo l'acquisizione di "pacchetti probatori" formati fuori dalle regole processuali e il loro utilizzo "preconfezionato", senza alcun controllo difensivo, allora ci troveremmo di fronte a rigurgiti inquisitori e al congedo del corredo di garanzie che ha segnato il progresso di civiltà delle democrazie occidentali. Un arretramento dell'orologio della storia che avrebbe come effetto tossico l'abbassamento significativo della tutela delle nostre libertà. Cedere sul terreno della civiltà del diritto non ci renderà, però, *individui* più sicuri, ma solo *sorvegliati digitali* meno liberi.

Avvocati penalisti

IL RADIOSO FUTURO DELLE INTERCETTAZIONI DI MASSA

Giuseppe Milicia*



Intorno alle piattaforme di messaggistica per criptofonini, *Encro-Chat* e *Sky-Ecc*, hackerate ed intercettate dalle autorità francesi, si è sviluppato ed è ancora in corso un serrato dibattito giurisprudenziale su scala continentale, che non interessa soltanto la sorte dei numerosi processi di criminalità organizzata basati sui contenuti di milioni di messaggi di oltre 200.000 utenti, catturati, decriptati, selezionati ed offerti alle polizie di mezzo mondo. Le soluzioni fin qui elaborate investono infatti frontalmente questioni assai delicate di agibilità dei diritti di libertà nell'era del dominio delle tecnologie della sorveglianza.
Alla resa dei conti – dopo le decisioni delle Sezioni Unite del febbraio scorso, di altri giudici di ultima istanza di paesi membri UE ed anche della CGUE su questione pregiudiziale sollevata dal Tribunale regionale di Berlino – la partita, che vedeva in gioco diritti fondamentali e la loro tutela, l'hanno vinta gli apparati della sicurezza. È stato tracciato il percorso senza ostacoli per l'impiego giudiziario della raccolta massiva di comunicazioni riservate a mezzo delle più sofisticate tecnologie della sorveglianza digitale, messe a punto dall'industria militare per l'attività di intelligence. Tecniche di intelligence poste a servizio del processo penale. Anzi, più appropriato dire che è il processo penale ad essere messo al servizio dell'intelligence. Perché, secondo la lezione della giurisprudenza interna e sovranazionale, i pacchetti di informazioni preconfezionati dalla *Joint Investigation Team* franco-belga-olandese, si possono utilizzare solo a "scatola chiusa". L'interesse degli apparati a mantenere il segreto sugli strumenti e le tecniche spionistiche prevale sull'esercizio del diritto di difesa; che, si sa, può dispiegarsi se è garantita la conoscenza, non solo del contenuto delle informazioni, ma anche del modo in cui sono state raccolte. È questa l'impostazione che prevale nelle soluzioni acconciate dai giudici della civilissima Europa e dai supremi regolatori dell'interpretazione del diritto interno.
Ma un passo verso l'oscurità, più grave ancora, l'hanno fatto i giudici italiani delle Sezioni Unite della Corte di Cassazione nell'opera di normalizzazione dell'impiego nel processo di intercettazioni di natura chiarissimamente preventiva e per di più praticate massivamente ed indiscriminatamente su decine di migliaia di bersagli in contemporanea. È la parte più sorprendente e al tempo stesso più interessante della sentenza n. 23756 del 29 febbraio 24. In precedenza prevaleva una sorta di sciatto e strumentale negazionismo. Le chat sarebbero semplici documenti perché le autorità francesi le avrebbero recuperate perquisendo un server e non intercettando gli utenti della piattaforma. La distinzione è assai importante, per il cittadino prima che per i tecnici del diritto. Le intercettazioni catturano in tempo reale e in continuo le comunicazioni riservate e rappresentano per ciò stesso lo strumento più potente di violazione dei diritti della riservatezza. Per esse la legge pretende, quindi, molteplici e penetranti garanzie. Ma se si nasconde che di intercettazioni si tratti e si concentra l'attenzione sul solo risultato finale e si racconta che i pacchetti ricevuti dalla Francia contengono nient'altro che documenti di testo registrati su un supporto digitale, lo statuto delle garanzie del cittadino intercettato non sarà più applicabile. Sono diverse decine le sentenze del giudice di legittimità improntate a tale logica.
Il passo successivo lo hanno fatto le Sezioni Unite ed è quello che non ti aspetti. I supremi giudici nazionali - costretti dall'evidenza ad ammettere (anzi, più correttamente, a prendere in considerazione l'ipotesi) che si tratti di intercettazioni - finiscono per sostenere che, siccome di esse non si può fare a meno, a tale necessità conservativa della prova devono piegarsi le garanzie. Anche la più importante, quella che vieta di intercettare a fini giudiziari, massivamente, per appartenenza a categorie di sospetti. Scrive la sentenza delle Sezioni Unite del 29 febbraio 2024 che le intercettazioni di massa, in fondo, sono anche tollerate dalla Corte EDU. Sorvola tuttavia il dettaglio più importante; e cioè che le pronunce dei Giudici di Strasburgo citate a sostegno riguardavano *intercettazioni preventive*, quelle che non possono impiegarsi per reprimere delitti ma sono appannaggio dei servizi segreti per garantire la sicurezza nazionale o delle forze di sicurezza per il controllo di soggetti pericolosi.
D'altro canto nel corso di quel giudizio la Procura Generale della Cassazione, nella sua requisitoria scritta, aveva raccomandato alle Sezioni Unite di non andare troppo per il sottile e di seguire il flusso continentale di decisioni conservative ("*...sarebbe inspiegabile un'enclave di eccezione dello Stato italiano*"); ed aveva anche messo all'indice i ricorrenti che "*da indagati per un massivo traffico intercontinentale di stupefacenti si trasformano in paladini della minacciata legalità*". Sconveniente reclamare legalità a favore degli esecrabili, è il punto di vista di gusto populistico della Procura Generale per niente preoccupata del futuro che va profilandosi, di libertà minorate dalla potenza delle tecnologie della sorveglianza. L'argomento, certo, scalda le maggioranze plaudenti ma non rassicura chi non riesce a togliersi dalla mente un insegnamento negletto della storia del secolo breve, utile per gli abitanti di quello ancor più breve e frammentato che stiamo vivendo. E cioè che ci sono sempre degli zingari da cui cominciare.

Avvocato penalista

PROVE DIGITALI TRANSNAZIONALI

Chat criptate e tirannie tecnologiche sulla prova

Luca Marafioti*

SEGUE DALLA PRIMA

Cosicché il P.M. può chiedere ed ottenere prove già ottenute o formate in un procedimento straniero al fine di produrle in Italia, senza necessità di alcuna autorizzazione del giudice. Per una simile libera circolazione basta che sussistessero le condizioni per emettere un ordine europeo di indagine. Soluzione piattamente "proceduristica" che lascia aperta la strada a pericolose scorciatoie probatorie, in epoche di ampio uso di meccanismi di investigazione oltre i confini. Di fatto il P.M. potrebbe "delegare" ad organi stranieri attività che in Italia andrebbero autorizzate dal giudice. Si legittima, per giunta, l'uso di strumenti privi di adeguata disciplina normativa e ad alto grado di invasività nella sfera privata, quali i captatori informatici "atipici".

Ogni controllo sulla legittimità dell'uso di mezzi tecnologici di ricerca della prova è consegnato in modo poco tranquillizzante nelle mani di una giurisprudenza mica tanto sensibile a fissare regole di utilizzabilità ferree e, soprattutto, ancorate ad un effettivo contraddittorio. Alla fine è il punto più dolente: una volta escluso un controllo nella formazione della prova digitale tutto slitta ad un dibattito postumo sul suo uso. Con il paradosso di dover contestare qualcosa che nessun sa da dove provenga né come sia stato formato. Si procede, così, a mezzo di "atti di fede",

dando per buone prove, sulla base di un malinteso principio del mutuo riconoscimento e attestandosi su posizioni addirittura meno garantiste di quelle assunte dalla Corte di giustizia dell'Unione europea, che pretende che l'imputato possa svolgere *efficacemente* le proprie osservazioni in proposito.

L'impossibilità di accedere all'algoritmo utilizzato per decriptare il contenuto dei dati digitali viene aggirata da un argomento meramente pratico sulla bontà della tecnica seguita: siccome ciascun messaggio è abbinato per forza ad una unica chiave di cifratura sarebbe impossibile qualsiasi errore o violazione in materia. In tal modo, però, il dato tecnico esercita la propria invincibile tirannia sul mondo giuridico a tutela delle garanzie dell'imputato e, più in generale, dell'individuo. Basti pensare che la mancata conoscenza delle tecniche di decodificazione del dato lede di per sé il diritto di difesa. Ogni controllo risulta aleatorio in assenza di un effettivo contraddittorio tecnico. A preoccupare è proprio questo: non sono i dati della legge a condizionare ed orientare le modalità di acquisizione ed utilizzo della prova, quanto assurdamente l'inverso. La dimensione pratica del fenomeno pregiudica la realtà della difesa, del contraddittorio e, in definitiva, del processo.

Senza accettare supinamente la schiavitù derivante dalla tecnologia, occorre, allora, fare leva su un nuovo illuminismo in materia, poco distante dallo spirito volto a superare l'eredità inquisitoria della tortura come mezzo di ricerca della prova. Anziché rassegnarsi a simile tirannia, è giunto, perciò, il momento di ripensare la tavolozza delle garanzie e lo statuto della prova tecnica nel processo penale.

Professore ordinario di procedura penale

Il Macaron

Détournement: importare chat anziché Châteaux

L. Z.

Sky-Ecc e l'ipocrisia del mutuo riconoscimento

Oliviero Mazza*

SEGUE DALLA PRIMA

I magistrati dialogano direttamente tra loro, ma parlano giuridicamente lingue diverse. Per tentare di superare le difficoltà, certamente non meno gravi di quelle che avrebbe implicato l'unificazione dei sistemi penali, si è imposto, per un verso, l'obiettivo dell'armonizzazione delle legislazioni nazionali, una specie di soluzione intermedia basata sulle regole generali delle direttive e dei regolamenti europei, mentre, per altro verso, si è escogitato il principio, apparentemente risolutivo, del mutuo riconoscimento. L'edificio europeo si regge così sul presupposto, invero abbastanza ipocrita, della fiducia reciproca fra Stati che, pur presentando tradizioni culturali e normative eterogenee, sono accomunati dall'appartenenza all'Unione e dal rispetto delle Carte fondamentali (CEDU, Trattati dell'Unione, Carte dei diritti fondamentali). Tali vincoli sarebbero in grado di giustificare la fiducia che ogni Stato può riporre nei confronti non solo della legislazione degli altri contraenti, ma anche nell'operato delle rispettive autorità giudiziarie.

Il mutuo riconoscimento avrebbe così l'effetto taumaturgico di rendere accettabili in Italia decisioni e prove formate all'estero, sulla base di regole, come detto, assai diverse. Armonizzazione, invero ancora molto soft in tema di diritti difensivi, e mutuo riconoscimento hanno solo nascosto, ma non certo risolto, il problema delle profonde diversità dei sistemi penali europei. I magistrati continuano così a dialogare con lingue giuridiche diverse, fidandosi aprioristicamente dei colleghi stranieri e fingendo che gli altri ordinamenti garantiscano livelli di tutela equivalenti a quello nazionale interno. Questa, per sommi capi, è la cornice in cui inquadrare le recenti questioni in tema di circolazione delle prove estratte da *Sky-Ecc*, piattaforma di chat utilizzata in modo assai disinvolto ed esplicito dai trafficanti internazionali di droga, oltre che da milioni di onesti cittadini europei che confidavano sulla segretezza delle comunicazioni. Non vi è dubbio che le chiavi di cifratura, necessarie per decrittare le chat (quali e quante non si sa), siano state ottenute dalla polizia francese, più precisamente dai servizi segreti, mediante l'esecuzione di una perquisizione informatica occulta, compiuta avvalendosi

di un *trojan horse* inoculato nel server della piattaforma *Sky-Ecc*. Il Governo francese, con una operazione di hackeraggio informatico per di più coperta dal segreto di stato, è così entrato nel server centrale della chat, recuperando le chiavi di cifratura che sono servite in un secondo momento per la lettura e la selezione dei dati altrimenti non intellegibili.

Nell'ordinamento processuale italiano, la perquisizione informatica è consentita solo nel rispetto delle forme previste dall'art. 247 comma 1-bis c.p.p., norma che non prevede la possibilità di impiego del captatore informatico e nemmeno l'esecuzione dell'atto in maniera occulta. A ciò si aggiunga che la perquisizione mediante captatore informatico, oltre a non essere prevista dalla legge processuale, finirebbe per aggirare tutta la disciplina codicistica, principalmente le norme a tutela dell'intervento dell'interessato e del difensore: artt. 250, 365, 369 c.p.p., nonché la legge n. 48 del 2008 in tema di acquisizione dei dati informatici. È indiscutibile che un'azione investigativa, come quella compiuta in Francia, sarebbe vietata nel nostro sistema processuale penale e finirebbe per ledere i diritti processuali dell'indagato aventi diretta copertura costituzionale (art. 14 e 15 della Carta).

Poste queste premesse, rimane da interrogarsi sul rispetto del principio di equivalenza, sancito, quale condizione di legittimità dell'ordine di indagine europeo, dall'art. 6, par. 1, lett. a) e b) della Direttiva 2014/41/UE. Davvero possiamo riconoscere come equivalente una prova acquisita dai servizi segreti francesi mediante perquisizione informatica occulta vietata dal nostro ordinamento? Per le Sezioni Unite della Cassazione sostanzialmente sì, *male captum bene retentum*; per chi non crede nell'ipocrisia del mutuo riconoscimento e pretende di rimanere fedele ai princìpi della nostra civiltà giuridica, certamente no.

Professore ordinario di procedura penale

IL CASO DUROV

LA SCHEDA DEL PROCESSO

Maria Vittoria Ambrosone*

L'accusa: reati legati alla pornografia infantile, al traffico di droga e alle transazioni fraudolente sulla piattaforma di messaggistica Telegram.

Gli indagati:
tra gli altri, il russo Pavel Durov, fondatore e amministratore delegato di Telegram, per il suo ruolo nell'agevolazione di reati che vanno dallo scambio di materiale pedopornografico alla condivisione non consensuale di immagini intime, e per la mancata collaborazione dell'azienda nel perseguimento dei responsabili.

Le date:
2024, luglio – avvio delle indagini contro ignoti ad opera dell'unità di criminalità informatica francese;
24 agosto 2024 – arresto del miliardario Durov, fermato di ritorno dall'Azerbaijan all'aeroporto di Le Bourget, a Parigi, dalla gendarmeria aeroportuale;
24-28 agosto 2024 – quattro giorni di fermo, contestazione delle accuse preliminari e interrogatorio; fissazione di una cauzione di 5 milioni di euro;
29 agosto 2024 – rilascio di Durov a seguito del pagamento della cauzione; attualmente l'indagato si trova in stato di libertà vigilata con l'obbligo di presentarsi presso una stazione di polizia due volte alla settimana e non può lasciare la Francia in attesa del processo.

Com'è finita:
Il procedimento è ancora in corso, ma Durov ha annunciato che Telegram, contravvenendo alla politica adottata finora, consegnerà alle autorità giudiziarie gli indirizzi IP delle connessioni per risalire all'identità delle persone e i numeri di telefono degli utenti nel caso di procedimenti nei loro confronti.

***Avvocato penalista**

LA VICENDA TELEGRAM E IL *DÉTOURNEMENT* INTERVISTA ALL'AVVOCATO PAUL LE FÈVRE

«Il rifiuto di collaborare rende Durov complice dei suoi utenti? Questo vìola *in primis* il principio di legalità»

Marianna Caiazza*

Sulla vicenda Telegram-Durov abbiamo intervistato Paul Le Fèvre, avvocato penalista francese iscritto al Barreau di Parigi.

A fine agosto di quest'anno Pavel Durov, giovane fondatore dell'app di messaggistica Telegram, è stato arrestato in Francia. Il Procuratore di Parigi, Laure Beccau, ha riferito che Durov sarebbe coinvolto in un'indagine avviata dall'unità di criminalità informatica sulla piattaforma Telegram, a mezzo della quale si consentirebbe la realizzazione di numerosi illeciti come la pornografia infantile, il traffico di droga, le frodi informatiche, il riciclaggio di denaro. Il fondatore, pur non direttamente coinvolto negli illeciti, vi avrebbe contribuito permettendone la indisturbata realizzazione. Gli viene inoltre contestato il rifiuto di collaborare con governi e forze dell'ordine nelle indagini e nella rimozione di contenuti potenzialmente dannosi. Cosa rischia Pavel Durov?
Oggi Durov deve rispondere di delitti di vario tipo: quelli c.d. "tecnici", come il rifiuto di collaborare, meno gravi, e quelli gravissimi che avrebbero commesso gli utenti di Telegram e che gli sono addebitati quale "complice". Che per il sistema francese significa che risponde del reato come se lo avesse commesso in prima persona e dunque soggiace alla stessa pena. È bene precisare anche che l'accusa ha ritenuto sussistente per tutti i reati l'aggravante della c.d. banda organizzata, e questo ha consentito la sottoposizione di Durov ad un fermo molto lungo, di 4 giorni. Di norma il fermo è di 24 ore, prolungabile di altre 24 al massimo. Nel sistema francese non esiste neppure l'udienza di convalida, non c'è contraddittorio; Durov potrà impugnare nei successivi 6 mesi il fermo dinanzi alla Corte di Appello, e l'eventuale annullamento potrebbe, in astratto, far decadere gli atti successivi ad esso legati.

Ha parlato di "complicità" nei delitti degli utenti. Il sistema penale italiano prevede che più persone possano rispondere di uno stesso reato, ma a condizioni ben precise: occorre efficienza causale delle condotte, ma soprattutto serve il dolo, cioè coscienza e volontà di commettere l'illecito e di concorrere con altri alla sua realizzazione. Questo perché la c.d. connivenza, un atteggiamento passivo che non contribuisca né materialmente né moralmente alla realizzazione dell'illecito, non è punibile. Ci sono poi reati come l'associazione per delinquere, che non richiede il dolo per ogni singolo reato, ma che impone la prova dell'accordo criminoso tra tutti gli associati. Cosa accade invece in Francia? A che condizioni Pavel Durov può rispondere delle attività illecite degli utenti di Telegram?
In Francia la struttura della c.d. "complicità" è molto simile al concorso italiano, il che rende certamente contestabile l'accusa a Durov. Perché si risponda quale complice in Francia devono sussistere un fatto principale punibile (ad esempio, la pedopornografia) e la coscienza e volontà di concorrere a realizzarlo con altri. Nella maggior parte dei casi, quindi, si impone la prova della conoscenza, da parte del concorrente, dell'autore principale e delle sue intenzioni. Su queste basi, allora, si pretenderebbe di sostenere una complicità di Pavel Durov con tutti gli utenti di Telegram (utenti che, in astratto, dovrebbe conoscere uno ad uno!).

Quindi è un'accusa che non regge?
Messa così sì, sembrerebbe un'accusa che non sta in piedi. Però è anche vero che da 10 anni a questa parte la giurisprudenza francese ha mostrato una tendenza a valutare come dolosa anche una condotta negligente: sostanzialmente, di fronte ad una grave negligenza si assume che la persona abbia voluto che quel fatto si realizzasse, e di qui il dolo. E allora, con a mente questo orientamento giurisprudenziale, si potrebbe ipotizzare una solidità dell'accusa a Durov che "non poteva non sapere" che la piattaforma veniva strumentalizzata per commettere reati. La norma non lo consentirebbe, ma la giurisprudenza di fatto lo ammette.

Ma è compatibile con una idea liberale e democratica del diritto penale la pretesa che il gestore di una piattaforma *social* possa essere obbligato a collaborare e poi a rendere individuabili gli utenti dinanzi al sospetto della commissione di un reato, pena l'imputazione quale concorrente nello stesso?
Quel che mi pare totalmente incompatibile con i princìpi dello stato di diritto e soprattutto con il diritto di difesa è che il rifiuto di collaborare renda Durov complice dei suoi utenti. Questo vìola *in primis* il principio di legalità, che è cardine del nostro sistema: è la legge a dirci che il complice deve avere coscienza e volontà di supportare l'autore principale dell'illecito. C'è poi, credo, una violazione del principio di proporzionalità: la tutela delle libertà di comunicazione e di espressione non può che richiedere precise giustificazioni per la sua limitazione.


Paul Le Fèvre

A quest'ultimo proposito, nel corso del procedimento l'Autorità Giudiziaria francese ha autorizzato l'inoculazione di un *trojan* direttamente sul server del gestore, così da intercettare le conversazioni di tutti gli utenti (quasi centomila) per poi distribuirne i risultati in tutta Europa se significativi di possibili reati. Per la gran parte dei sistemi europei, compreso quello italiano, si tratta di una forma di intercettazione preventiva di massa assolutamente inconcepibile. Cosa ne pensa?
In Francia, come in Italia, il diritto ad una corrispondenza privata è tutelato come fondamentale, e subisce limitate eccezioni. Le intercettazioni costituiscono una importante violazione della *privacy* ed in quanto tali devono essere sottoposte a precise condizioni, e ciò è a ancor più vero se si utilizza il *trojan*, strumento fortemente restrittivo e per tale ragione impiegato solo per l'accertamento di alcuni reati, come la banda organizzata. Ciò detto, non c'è dubbio che per giustificare la compressione dei diritti fondamentali dell'individuo debbano esservi una giusta motivazione, una contestazione specifica, un sospetto fondato e una modulazione dello strumento intercettivo che si basi sul principio di proporzionalità. Una intercettazione di massa di questo tipo difficilmente rispetta questi requisiti fondamentali.

Il 23 settembre Durov ha reso noto che Telegram ha effettuato dei controlli sui contenuti, rendendo non più accessibili quelli individuati come potenzialmente illeciti. Ha poi annunciato che gli indirizzi IP e i numeri di telefono di coloro che violeranno le regole della piattaforma potranno essere comunicati alle autorità competenti su richiesta di quest'ultime. Ha vinto il ricatto della contestazione a Durov del rifiuto di collaborare?
È una domanda provocatoria ma legittima: se ragioniamo sul breve periodo non possiamo che constatare che, a seguito dell'imputazione, Telegram ha cambiato repentinamente strategia e obiettivi. Potremmo dire, allora, che il ricatto ha vinto: il procedimento ha dato risultati immediati, la piattaforma ora collabora. Ma credo e confido nel fatto che sia una vittoria solo temporanea: siamo di fronte a quello che chiamiamo il *détournement*, lo sviamento, la deviazione dai confini di ciò che sarebbe consentito. Una contestazione strumentale di un reato (ad esempio, per consentire l'intercettazione delle comunicazioni, oppure un fermo particolarmente lungo) è un *détournement*, e come tale credo sarà contestato dalla difesa nel processo. Perché un procedimento fondato su queste basi non può, nel lungo periodo, sopravvivere.

***Avvocato penalista**