Social network e sicurezza urbana: la nuova frontiera del controllo del territorio.

Sergio Bedessi

(da Polnews – editore Maggioli – 2015)

Il 20 marzo presso l'auditorium del Consiglio Regionale della Toscana si è tenuto il convegno "**SOCIAL NETWORK E SICUREZZA URBANA**" nel quale si è affrontato un tema che è ormai una vera e propria terra di frontiera per gli organi di polizia: i *social network* e il loro rapporto con la sicurezza urbana.
I *social network* sono un nuovo strumento di comunicazione (recentissimo il caso degli spacciatori che utilizzavano *Whatsapp* per il loro commercio) e una miniera di informazione tanto per chi commette crimini, quanto per la polizia.
Infatti i social network è, in modo più ampio, **i *social media*, stanno cambiando le abitudini sociali, coinvolgendo in questo cambiamento anche chi si dedica ai reati e, di conseguenza, chi questi reati deve reprimere**[1].
Sempre più spesso il ladro utilizza i *social network* per poter avere informazioni sul comportamento di quello che poi sarà il derubato: se vuole svaligiarvi la casa il malvivente non passa più ore ed ore appostandosi camuffato per comprendere le vostre abitudini, ma diventa vostro amico su qualche social network ed in questo modo sarete voi stessi a fornirgli le informazioni che gli servono.
Mentre nuovi crimini, prima impensabili (si pensi per esempio al *social network bullying*) avvengono, nuove forme di indagine, anche molto sofisticate, sono possibili; al classico *criminal profiling* che cercava di individuare le caratteristiche del criminale si sta sostituendo un'analisi più o meno massiccia di profili e di dati inseriti spesso proprio da chi il crimine ha commesso, magari per mania di protagonismo. E' dunque necessario avere una visione unitaria di questa miniera di informazioni, seguire criteri rigorosi di analisi e, non ultimo provvedere ad una formazione specifica per gli organi di polizia, fra i quali la polizia municipale.

La **crescente disponibilità di dati consente oggigiorno di affrontare il problema della gestione della sicurezza urbana e nazionale con nuovi strumenti da affiancare alla insostituibile conoscenza del territorio da parte delle forze dell'ordine**[2]; fra questi gli strumenti di *crime mapping* che possono essere utili a condurre analisi che possono fornire un importante quantitativo, oltre che qualitativo, all'organizzazione dei servizi di controllo del territorio da parte degli organi di polizia. Certamente il rapido sviluppo dei *social media* supera il legame tra fatti sociali e spazio fisico e pone **questioni non banali sulla possibilità di analizzare i dati disponibili in *social network* e *blog* per la gestione della sicurezza** a tutti i livelli (locale, nazionale ed internazionale).

Il tema dei social media e del loro utilizzo ai fini della sicurezza urbana porta al tema **dell'utilizzazione dei dati dei *social network*, tramite tecniche di *social mining* e, a monte, l'analisi dei cosiddetti "*big data*" tramite il *data mining*[3].** Se è vero che vi è una grande disponibilità di informazione, è altrettanto vero che questa deve essere trasformata in vera e propria conoscenza al fine di essere utilizzabile da parte degli organi di polizia e delle agenzie di sicurezza a tutti i livelli; per far questo, così come vi sono vari filoni di estrazione dell'informazione, vi sono **varie prospettive di analisi, le abitudini delle persone, le opinioni, le**

[1] Intervento di **Sergio Bedessi**, Presidente di CEDUS - Centro Documentazione Sicurezza Urbana e Polizia Locale.

[2] Intervento di **Enrico Di Bella**, docente di Statistica Economica e Sociale presso l'Università degli Studi di Genova, esperto in *crime mapping* e *smart safety.*

[3] **Filomena Maggino**, Docente di Statistica Sociale e di Analisi Statistica Multivariata presso l'Università degli Studi di Firenze.

informazioni sulla mobilità, sui consumi, e tutte queste possono aver rilievo rispetto al tema della sicurezza.

Una delle difficoltà che si pongono a chi effettua queste operazioni è quella che molte informazioni sono di proprietà privata e quindi divengono utilizzabili solamente a pagamento; un altro problema è quello connesso al "rumore" che questi dati si portano dietro: in pratica i dati ottenuti non sempre sono perfetti e devono quindi prima essere "puliti".

Un altro problema connesso all'accesso e all'utilizzazione dei dati contenuti nei big data è quello della riservatezza degli stessi e dei limiti che questa riservatezza può incontrare nel caso sia in gioco la sicurezza.

Quanto è lecito infatti prelevare informazioni dai big data, oppure da Facebook, Twitter, Picasa, Instagram, su persone che non risultano ancora formalmente indagate?[4]

Vi è evidentemente il **problema dell'utilizzazione dei dati recuperabili sui *social media*** o sui big data **da parte degli organi di polizia ancor prima delle vere e proprie indagini di polizia giudiziaria**.

Vi sono infatti alcune fasi precedenti alle indagini vere e proprie che possono porre alcune problematiche; si tratta di quelle fasi di osservazione, che si potrebbero definire di "*intelligence*", e che in epoche passate venivano effettuate dagli organi di polizia nell'ambiente fisico, per le strade di una città, e che oggi invece devono essere effettuate in un ambiente virtuale.

La differenza è che mentre con l'osservazione dell'ambiente fisico non si entrava in contatto con dati oggi definiti "sensibili" dal punto di vista della disciplina della riservatezza dei dati, oggi l'accesso degli organi di polizia ai *social media* e, in genere, ai *big data*, implica necessariamente l'accesso a informazioni che spesso sono appunto "sensibili".

Se, per chi appartiene ad un organo di polizia, infiltrarsi nei *social network* arrivando a dissimulare la propria identità per meglio svolgere il proprio lavoro è sicuramente lecito nel caso di reati particolari, come la pedo-pornografia, meno lecito potrebbe esserlo nel caso di reati minori (prima della vera e propria attività di polizia giudiziaria) o addirittura di eventi che non è chiaro a priori se siano o meno illeciti penali.

Una sentenza della Corte Costituzionale tedesca del 27 febbraio 2008 si era già espressa negativamente **sull'uso generalizzato dei c.d. Bundestrojan (Trojan di Stato), programmi capaci di captare informazioni dai computer di chi è connesso a internet,** rilevando come tale attività comportasse rischi di un controllo pervasivo e una invasione della **sfera privata** e della **riservatezza.**

Infine il convegno ha mostrato come ormai i social media siano divenuti **importante strumento di comunicazione per gruppi terroristici** (grazie al fatto che le intercettazioni dei messaggi sono estremamente più difficoltose delle intercettazioni delle conversazioni telefoniche)**, nonché di proselitismo**[5]; da qui l'aumentato interesse non solo a livello internazionale e nazionale, ma anche a livello di sicurezza urbana per gli organi di polizia, anche locale.

Certamente non è semplice riuscire ad analizzare i flussi di comunicazione che le reti terroristiche mettono in piedi; la ricercatrice ha comunque mostrato come siano possibili tecniche di analisi che possono coadiuvare gli organi di polizia nelle indagini ed anche nelle fasi di *intelligence*.

---

[4] **Fabio Piccioni**, avvocato penalista, docente presso la Scuola di Specializzazione delle Professioni Legali

[5] **Gerta Zaimi**, collaboratrice del Centro Studi Strategici Internazionali e Imprenditoriali dell'Università di Firenze.

In definitiva il convegno ha dimostrato come, pur con varie difficoltà, i *social media* in generale e i *social network* in particolare possano essere una miniera di informazioni importantissima per tutti gli organi di polizia in generale.

Gli organi di polizia locale possono essere particolarmente interessati a questi strumenti di *intelligence* in un'ottica evolutiva di un controllo del territorio probabilmente sempre meno fisico, ma non per questo meno importante.