INTERCETTAZIONI LEGALI SOLO SE "CERTIFICATE"

Dott. Giovanni RUSSO, Procuratore nazionale antimafia e antiterrorismo aggiunto.

1. Introduzione

E' ben nota la rilevanza investigativa e probatoria delle intercettazioni, un tempo prettamente telefoniche e, più recentemente, anche telematiche e ambientali.
Esse permettono l'acquisizione di elementi probatori (non solo conversazioni ed altri tipi di comunicazione, ma anche documenti, immagini, video ecc.) che sono il frutto della diretta (e inconsapevole) produzione dei soggetti intercettati. Forniscono, cioè, informazioni "di prima mano", di grande interesse giudiziario, perché caratterizzate, il più delle volte, da spontaneità e veridicità e perché correlate a manifestazioni comunicative private, idonee a rivelare le reali motivazioni e finalità dell'agire umano.

Con la rivoluzione digitale, le relazioni comunicative hanno assunto un ruolo centrale, potremmo dire "essenziale" in tutti gli ambiti della vita quotidiana e, quindi, anche nei contesti criminali.
Se nel 2017 The Economist, con qualche ritardo, poteva affermare che "*The world's most valuable resource is no longer oil, but data*", risulta evidente che al giorno d'oggi le informazioni rappresentano certamente l'oggetto del desiderio dei moderni delinquenti, che hanno sostituito grimaldelli, piedi di porco e ordigni esplosivi con nuovi e sofisticati strumenti digitali (virus, worm, trojan malware, adware, ransomware) oppure, più semplicemente, hanno imparato ad approfittare di password deboli o di siti internet non sicuri.
Ma la ricerca informativa è anche il "terreno di caccia" degli apparati investigativi e giudiziari, il cui compito è prevenire la commissione dei reati e sanzionare gli autori dei crimini.

L'inviolabilità della libertà e della segretezza delle comunicazioni, proclamata come principio dall'art. 15 della Costituzione, deve trovare oggi una sua declinazione anche digitale, realizzando quella che il mondo anglosassone definisce come "**cyber security**", assicurata dall'insieme degli strumenti, delle tecnologie e delle procedure atti a garantire disponibilità, confidenzialità e integrità ai dati e ai sistemi informatici.

Una "barriera" virtuale tra il mondo esterno e le informazioni in formato digitale che ognuno di noi produce, detiene, scambia. Cresce, dunque, di giorno in giorno, l'esigenza di individuare metodologie e competenze in grado di assicurare la sicurezza informatica dei sistemi, anche complessi, per fronteggiare forme sempre più dirompenti di compromissione di micro e macro ecosistemi digitali, ad esempio, con dati esfiltrati o criptati con richiesta di riscatto.
Ma si impone, parallelamente, la necessità di realizzare efficaci attività di indagine penale, nell'ambito dell'area legale autorizzata dal secondo comma del citato art. 15 Costit.

2. Le intercettazioni legali

Come il chirurgo, in condizioni di necessità e, se possibile, previo consenso della persona interessata, opera col bisturi una lesione nei tessuti del corpo umano, per tutelare il bene superiore della vita, il sistema giustizia dello Stato può intervenire, lacerando la sfera della privacy di un determinato soggetto, per ragioni di interesse investigativo. L'autorizzazione a ledere, momentaneamente e per le sole esigenze di giustizia, il diritto alla libertà e alla segretezza delle informazioni delle comunicazioni è fornita dalla Costituzione in presenza di due condizioni.

Innanzitutto deve sussistere una previsione legislativa che faccia da guida, da argine e che orienti la dimensione della "violazione" in quell'area di riservatezza, calibrandone gli effetti nell'ambito delle finalità costituzionalmente riconosciute e rilevanti. Nel caso di specie, le finalità rilevanti che consentono questa compressione della libertà di comunicare (senza che altri ascoltino) nascono dall'esigenza penalistica di garantire l'ordine sociale attraverso la punizione di chi commette dei reati.

La seconda condizione è costituita dall'esistenza di un provvedimento del magistrato, cioè una valutazione, caso per caso, della ricorrenza dei presupposti previsti dalla legge e della oggettiva pertinenza di questa compressione in relazione ai fini costituzionalmente garantiti che sono concorrenti. Il magistrato verifica la sussistenza dei presupposti, disciplinati nel codice di procedura penale dagli articoli 266 e seguenti, ivi compresa la necessità/indispensabilità di un così rilevante tipo di intromissione nella sfera personale tutelata rispetto alle finalità investigative.

La mutevolezza delle capacità comunicative e trasmissive che, come cittadini, sperimentiamo quotidianamente impone al legislatore di adeguare periodicamente le regole procedurali, affinché le descritte garanzie costituzionali siano assicurate anche in presenza di innovazioni tecnologiche.

In particolare, vengono in considerazione i recenti interventi legislativi (il Decreto Legislativo 29 dicembre 2017, n. 216 e il decreto-legge 30 dicembre 2019, n. 161 convertito con legge 28 febbraio 2020, n. 7): essi, **nel riconoscere il ruolo delle intercettazioni come strumento di indagine necessario**, si propongono di fissare il giusto equilibrio tra la segretezza della corrispondenza e di ogni altra forma di comunicazione e il diritto all'informazione.

Vengono introdotte alcune novità come quella che **vieta "sempre" la pubblicazione**, anche parziale, del contenuto delle intercettazioni non acquisite, quella che interviene nell'ambito dell'art. 266 c.p.p. e, in particolare, in relazione all'impiego del captatore nei luoghi qualificabili come domicilio, per il quale è richiesta adeguata motivazione in seno al decreto autorizzativo. Si assiste, altresì, al potenziamento del ruolo del Pubblico Ministero sul vaglio delle intercettazioni: egli dovrà anche vigilare affinché nei verbali non siano riportate espressioni lesive della reputazione delle persone. Viene previsto un archivio digitale, gestito e tenuto sotto la direzione e la sorveglianza del Procuratore della Repubblica dell'ufficio che ha richiesto ed eseguito le intercettazioni.

L'intervento legislativo, quindi, è chiamato a tenere conto delle novità nel campo delle attività tecniche di captazione, rese possibili dalla disponibilità non solo dei nuovi strumenti tecnologici in senso stretto ma anche dallo sviluppo di una nuova dimensione di espressione degli spazi comunicativi intra e inter relazionali. Ci si riferisce alle svariate piattaforme di comunicazione (ad es. i *social network*) in relazione alle quali assumono sempre maggiore importanza le intercettazioni telematiche che consentono di penetrare questi nuovi ambiti relazionali restituendo, anche a livello storico, una grande quantità di informazioni generate con le nostre attività, attraverso i computer e,

soprattutto, attraverso i *devices* portatili. Questi strumenti, peraltro, sono funzionali anche ad un'altra esigenza umana, cioè quella della memorizzazione, ovvero della custodia di documenti e attività in genere che l'utilizzatore compie o alle quali è interessato. L'accesso captativo a questi strumenti consente quindi non solo di registrare e ascoltare in tempo reale o differito le conversazioni, ma consente anche di ricostruire, a mesi o anni di distanza, una traccia storica delle attività svolte dal "bersaglio" (relazioni e contatti che il soggetto ha avuto, compresi i contenuti che sono lì depositati). Si tratta, a ben vedere, di una sorta di estensione digitale della personalità.
Proprio nella rilevanza di tale impatto sembra di poter invenire il fondamento della previsione dell'obbligo di distruzione del materiale costituito da verbali, registrazioni di comunicazioni intercettate etc., **non rilevanti**: non vengono dettate regole esclusivamente di tipo formale ma si cerca, in qualche modo, di affrontare, il più vicino possibile, il contenuto informativo, per differenziarlo in base alla concreta utilità che la sua conoscenza rivesta nell'ambito delle indagini (e del dibattimento), restituendo la parte irrilevante a quella sfera di riservatezza della persona che ne è titolare, tutelata per diritto ma violata per ragioni di giustizia.

Il tema denuncia tutta la sua delicatezza: il legislatore ha saputo individuare regole aggiornate che mettano in sicurezza, in chiave adeguatamente moderna, i valori che sono alla base del principio costituzionale sopra indicato? E l'applicazione pratica che di quelle regole fanno magistrati, polizia giudiziaria e tecnici addetti alle operazioni materiali di intercettazione garantisce effettivamente che la compressione del diritto di ognuno di noi ad una sfera di riservatezza (entro la quale liberamente atteggiarsi comunicativamente con gli altri e entro la quale manifestare, liberamente, la nostra personalità) sia la minima possibile?

3. Criticità vere e presunte

Da più parti sono stati sollevati rilievi e rimostranze circa l'impiego dello strumento intercettativo, sia con riferimento al ricorso in via generale a tale mezzo di indagine, sia con riguardo alle concrete modalità di esecuzione dello stesso.
Al netto delle posizioni meramente strumentali, finalizzate alla paralisi o alla delegittimazione di specifiche indagini, va osservato che **la enorme dimensione di dati che vengono sottratti, seppur per ragioni di giustizia, alla vita di migliaia di persone, assume valore certamente degno di attenzione**. Non possono, pertanto, essere tollerate sbavature.

Ebbene, taluni episodi assurti agli onori della cronaca, sia pure frammentariamente, hanno potuto ingenerare la convinzione che non tutti i meccanismi siano attuati in maniera soddisfacente. In attesa di conoscere i risultati degli approfondimenti svolti al riguardo, anche nell'ambito di procedimenti penali, vanno comunque rilevate alcune "zone d'ombra" che sarebbe necessario contrastare.

In primo luogo, mancano regole uniformi per la realizzazione delle operazioni di intercettazione. **Non esiste un mansionario né un catalogo delle prestazioni che disciplinino in dettaglio le azioni da porre in essere nelle fasi pre e post intercettazione** (oltre che, ovviamente, nell'esecuzione delle operazioni di captazione in senso stretto). Eppure sarebbe importante poter contare su di un "disciplinare", considerando che l'ufficio di Procura, per poter effettuare le attività tecniche di intercettazione, deve necessariamente rivolgersi alla **galassia** delle innumerevoli aziende, presenti sul mercato e che offrono servizi di questo tipo, ognuna delle quali segue proprie regole e prassi.
In secondo luogo, per ragioni prevalentemente "tecniche", possono verificarsi anomalie nella continuità dei flussi delle attività di captazione, che comunque non sono sempre sicure, fondandosi, anche se per necessità tecniche, su di un trasferimento del dato captato attraverso più punti.

Altri aspetti di opacità possono riguardare la modalità di custodia dei dati acquisiti, soprattutto con riferimento alla fase di smistamento dall'operatore telefonico all'azienda incaricata delle intercettazioni e, da questa, all'ufficio di Procura.
Alcune problematiche sono sorte anche con riguardo alle tecniche di inoculazione dei captatori informatici, dovendosi prevenire casi di "infezioni massive", nonché con riferimento alla effettiva rimozione del virus, una volta terminata l'intercettazione autorizzata (non è accettabile che il virus, ancorché "inattivato", venga lasciato all'interno del dispositivo *target*).

Sono ben evidenti, in tale scenario, le difficoltà, per i circa 140 Procuratori del nostro Paese, di esercitare una efficace azione di controllo sul sistema dei flussi sopra sommariamente descritti. Un groviglio abbastanza complicato, insomma, e tale da rappresentare, nel suo complesso, una struttura critica.

Nella migliore delle ipotesi, infatti, il Procuratore, attraverso la struttura dedicata alle intercettazioni (il "CIT"), potrà assicurare in maniera rigorosa la correttezza degli aspetti burocratici/procedurali (l'esattezza del bersaglio da attingere, la conformità all'autorizzazione del Gip delle attività da delegare, il rispetto delle scadenze, ecc.), ma **non potrà certamente espletare alcun effettivo controllo circa le risorse e le soluzioni tecnologiche di volta in volta adottate**. Neppure i pregevoli decaloghi, che qualche Procura con più spiccata sensibilità e più avanzate competenze in questo settore ha avuto cura di predisporre (e che sono stati diffusi a tutti gli uffici di Procura nell'ambito della condivisione delle *best practises*), possono ritenersi una soluzione appagante. Questo decalogo, che contiene una serie di condizioni che gli operatori incaricati delle intercettazioni devono assicurare prima di iniziare le attività, finisce per collocarsi - infatti - sul piano delle iniziative meramente formali per due motivi: la Procura non dispone di alcuno strumento efficace e completo per un controllo della veridicità dei titoli vantati dal contraente, né della effettività degli impegni assunti; **può agire soltanto *ex post*, ovvero quando emerge già la patologia**.

La seconda ragione è che oggettivamente un decalogo astratto, a fronte della velocità con la quale mutano i sistemi tecnologici (soprattutto in questo settore vengono ideati ogni settimana nuovi prodotti, nuovi software, nuove applicazioni ecc.), rischia di diventare obsoleto anche a pochi mesi dalla sua stesura o sottoscrizione.

4. Il valore dell'accreditamento o della certificazione

In realtà, basterebbe guardare ai modelli internazionali di valutazione della sicurezza informatica: esaminare i sistemi nel loro complesso, valutandoli rispetto ad altri fattori come, ad esempio, la tipologia di dato, la sua importanza sotto il profilo della sicurezza, il luogo di conservazione, la natura e le prerogative dei suoi fruitori. Non a caso uno degli elementi di maggiore novità introdotti dal Regolamento (UE) 2016/679 sulla protezione dei dati è stata la previsione di una valutazione di impatto, cioè una valutazione del rischio, con conseguente gestione, che dipendesse proprio dai suddetti fattori.
In tutti i settori in cui tali sistemi informatici lavorano, dal manufatturiero all'agroalimentare, dal chimico al meccanico, la scelta della migliore prassi o soluzione da applicare tiene conto delle esigenze di sicurezza: gli enti internazionali di standardizzazione come ISO, ITU, ETSI, ecc., con la loro documentazione tecnica, hanno infatti profilato le casistiche d'uso. L'aggregazione di tali standard internazionali, sulla base delle finalità da perseguire e del settore di pertinenza, è alla base dei c.d. accreditamenti o certificazioni condotte da enti terzi (in quanto diversi sia dall'utilizzatore che dal produttore), valorizzando di conseguenza l'intera filiera sotto i profili della qualità e dell'affidabilità.

In tutti i Paesi in cui l'accreditamento è stato introdotto è aumentata la competitività e l'intero sistema socio-economico ne ha beneficiato, dalle istituzioni alle imprese, ai consumatori, in termini di reputazione e di *performance*.
Nel dettaglio, come ricordato dal nostro ente di certificazione nazionale Accredia, diversi potrebbero essere i vantaggi: nel caso delle istituzioni, o della Pubblica Amministrazione più in generale, si possono ottenere benefici in termini di riduzione della legislazione nazionale aggiuntiva e di semplificazione dei controlli diretti nei confronti di organizzazioni pubbliche o private che possiedono la certificazione.

5. Le intercettazioni legali come servizi informatici da certificare

E' dunque paradossale rilevare che le intercettazioni, intese come servizi informatici noleggiati dalla Pubblica Amministrazione, non possono riferirsi ad alcuno standard internazionale, che comprenda le varie peculiarità, a differenza di quanto avviene in tanti altri settori.
Spesso si è portati a valutare erroneamente che tale forma di garanzia o certificazione sia già in qualche modo contemplata nella dichiarazione di aderenza ai requisiti elencati nei relativi bandi di gara e nei loro allegati tecnici. In realtà, l'elencazione di requisiti tecnici dei bandi non può essere mai così dettagliata da considerare tutti gli aspetti necessari, ad esempio come quello della sicurezza, del trattamento, degli standard ETSI per l'inoltro dei dati ai sistemi dell'autorità giudiziaria, ecc. **Nella maggior parte dei casi, quindi, si procede sulla base di una semplice autodichiarazione del fornitore**, che ha il solo scopo pratico di manlevare i pubblici uffici dalle verifiche preliminari, altamente specialistiche sotto il profilo tecnico, che questi ultimi non sarebbero in alcun modo in grado di svolgere.

Il principale vantaggio di una certificazione anche nel settore delle intercettazioni sarebbe quello di fornire una **preventiva garanzia** circa la legalità (intesa come rispondenza alle regole tecniche più avanzate) dell'intero sistema delle intercettazioni, **evitando di dover ricostruire ogni volta l'intera filiera di gestione del dato intercettato**, con benefici anche sotto il profilo della riduzione dei tempi processuali. Si avrebbero inoltre vantaggi nello snellimento delle procedure di gara: in moltissimi altri settori industriali la certificazione indipendente di prodotto costituisce già un requisito legale o contrattuale. Infine, si avrebbe finalmente la disponibilità di un'elencazione oggettiva di caratteristiche che permetterebbe ai pubblici uffici una più semplice scelta del prodotto più adeguato alle specifiche esigenze del momento.

In tal modo si raggiungerebbero tre obiettivi importanti.

1. Garantire al cittadino che le modalità tecniche delle captazioni, della trasmissione e della custodia delle sue comunicazioni rispettino elevati e costanti standard qualitativi, idonei ad assicurare l'effettività dei precetti delle norme di rango costituzionale e ordinario. In altri termini, dare a tutti la certezza che l'intero "processo" dell'attività intercettativa sia presidiato da meccanismi tecnici – validati *ab inizio* e costantemente monitorati – che garantiscano l'integrità, la continuità, la non manipolabilità, la non replicabilità, la confidenzialità delle comunicazioni.
2. Garantire ai Procuratori della Repubblica di poter disporre, già all'atto della scelta dell'azienda a cui affidare le attività intercettative, di elementi valutativi affidabili; attribuire ai predetti Procuratori – attraverso le competenze del soggetto certificatore – strumenti per verificare in maniera continuativa e attendibile le modalità attraverso le quali viene posto in esecuzione il mandato intercettativo che egli ha conferito, sulla base dell'autorizzazione del GIP, alla Polizia Giudiziaria. Attraverso la certificazione del "processo" intercettativo, in altri termini, il Procuratore ottiene la garanzia scientifica che ogni istante dell'attività invasiva avvenga senza intromissioni, interferenze, errori, dimenticanze, negligenze, trascuratezza ecc.
3. Garantire all'operatore incaricato di eseguire le intercettazioni, di avere un qualificato e competente interlocutore con il quale potersi permanentemente interfacciare, anche a fronte di ogni nuovo evento che si manifesti e che richieda una "decisione" di tipo tecnologico.

Lo strumento necessario per il raggiungimento dei tre obiettivi è la certificazione – a cura di soggetto terzo qualificato e accreditato – dell'intero processo di intercettazione e captazione delle informazioni: esso, fin dall'avvio dell'installazione, anzi fin dalla scelta degli strumenti tecnologici, da quelli hardware al software, deve essere validato dal punto di visto scientifico così che se ne certifichi la idoneità a realizzare un'attività conforme ai parametri di legge.
Dal punto di visto organizzativo la individuazione dei soggetti certificatori, da abilitare a tale funzione in materia di intercettazione, potrà essere compiuta dal Ministero della Giustizia, eventualmente per macro aree territoriali, oppure potrà essere rimessa alla **discrezionalità dei singoli Procuratori della Repubblica, attingendo tale figura nell'ambito di elenchi previamente validati dallo stesso Ministero**.©