Revista Ítalo-Española de Derecho Procesal
pp. 5-8
Madrid, 2024
DOI: 10.37417/rivitsproc/
Marcial Pons Ediciones Jurídicas y Sociales

ISSN: 2605-5244

EDITORIALE

Giulio illuminati

Stando ai dati riportati in un recente articolo di Filippo Spiezia, in Italia la prova digitale è rilevante in circa l'85% delle indagini penali, e nel 65% dei casi (vale a dire, il 55% del totale) per acquisirla occorre rivolgere una richiesta ad un *service provider* basato all'estero.

Ora, a prescindere da una precisa definizione del concetto di prova digitale — che in realtà abbraccia una grande varietà di dati informatici o informatizzati, anche piuttosto distanti fra loro quanto a caratteristiche — appare evidente che bisogna prendere atto di una progressiva mutazione della originaria struttura della prova e del processo penale. Infatti la prova per eccellenza ormai non è più la testimonianza, come sanno gli operatori pratici, e di conseguenza le nostre usuali categorie rischiano di sbandare, poiché ci troviamo di fronte ad una serie di elementi nuovi, particolarmente significativi, che sono anche difficili da inquadrare.

Per altro verso, la legge non riesce, come sempre accade, a tener dietro ai rapidi sviluppi della tecnologia: basti ricordare, nel nostro caso, che il codice di procedura penale italiano è entrato in vigore in un'epoca in cui le intercettazioni si eseguivano mediante una derivazione fisica dalla centrale telefonica, si ascoltavano in tempo reale, e il contenuto delle comunicazioni intercettate veniva riversato su nastro magnetico (che ancora molto di recente, prima delle ultime riforme, era menzionato appunto come tale nel codice).

Anche il concetto stesso di comunicazione oggi non è chiarissimo, tanto che assistiamo spesso a disorientamenti della giurisprudenza: c'è da domandarsi se non sia il caso di abbandonare l'idea di poter prendere in considerazione le sole comunicazioni in senso stretto. È vero che l'art. 15 Cost. parla testualmente di libertà e segretezza delle comunicazioni, però oggi il concetto si deve necessariamente ampliare, perché comunicazione non è soltanto il contenuto di una conversazione intercettata, ma anche ad esempio i metadati, attraverso i quali è possibile profilare un soggetto; mentre è irrilevante il

fatto che si tratti di comunicazioni captate in tempo reale o dati immagazzinati in un qualsiasi dispositivo. È inutile, in altre parole, continuare a porsi il problema se si tratti nel caso specifico di sequestro, perquisizione, o intercettazione, o addirittura di prova atipica. Forse si dovrebbe semplicemente cominciare a parlare, in termini generalissimi, di sorveglianza elettronica, in tutte le sue varie forme. Come accade, per esempio, in altri paesi: in Germania, lo sappiamo, il *Bundesverfassungsgericht* ha dedotto i limiti costituzionali alla possibilità di sorveglianza elettronica delle persone, assunta come categoria generale, dal principio della tutela della dignità umana e del libero sviluppo della personalità individuale. L'art. 8 Cedu include nel più ampio diritto al rispetto della vita privata e familiare la tutela della corrispondenza; analogamente si comporta, con l'art. 7, la Carta dei diritti fondamentali dell'UE, che inoltre aggiunge, all'art. 8, la previsione specifica del diritto alla protezione dei dati personali.

Anche la Corte costituzionale italiana, a suo tempo, ha avuto modo di pronunciarsi, sia pure in un *obiter dictum* (sentenza n. 173 del 2009), sul diritto alla riservatezza, ritenuto un diritto fondamentale «riguardante la vita privata dei cittadini nei suoi molteplici aspetti», che si basa sugli artt. 2 e 15 Cost. Si parla spesso, oggi, di "nuovi diritti", poiché secondo alcuni il testo della Costituzione non copre tutte le manifestazioni della personalità individuale; ma, come è stato evidenziato, quando si parla di nuovi diritti in realtà si fa riferimento a nuove manifestazioni di un diritto già riconosciuto dalla Costituzione, ovvero a diritti che risultano dalla combinazione di altri principi costituzionali preesistenti.

A questo proposito, può essere utile il rinvio — dando per nota la giurisprudenza europea in argomento — alla motivazione di una ormai antica sentenza della Corte costituzionale in tema di intercettazioni telefoniche, la n. 34 del 1973, che è sempre stato uno dei miei punti di riferimento primari. Una serie di principi enunciati da quella sentenza — di cinquanta anni fa — sono ancora oggi validi, nonostante siano stati dettati nella vigenza del codice abrogato, e vanno considerati applicabili a tutti i tipi di interferenza nella vita privata.

Anzitutto il bilanciamento tra diritto alla segretezza delle comunicazioni, ma si può a questo punto parlare anche di diritto alla riservatezza, e l'esigenza di prevenire e reprimere i reati, anch'essa oggetto, si afferma, di protezione costituzionale. Inoltre, la necessità di un'autorizzazione del giudice, con una motivazione che dia conto del bilanciamento effettuato; la previsione di limiti di durata dell'intercettazione. Soprattutto, poi, il principio di proporzionalità, oggi com'è noto diventato centrale: se ne parla di solito come di un'acquisizione derivante dalla giurisprudenza europea, e in parte è così, ma va sottolineato che già a quel tempo la Corte costituzionale ne aveva riconosciuto il valore. Infine, la necessità di garanzie di ordine tecnico, particolarmente importanti perché è indispensabile assicurare l'autenticità dei dati e l'integrità nella loro conservazione.

Dunque nella motivazione di quella storica sentenza viene detto già tutto: inclusa l'esigenza del controllo di rilevanza dei risultati; del controllo di legittimità dell'operazione; della tutela del segreto; e, in particolare, anche l'esigenza della tutela dei terzi. Va poi evidenziato che vi si parla per la prima volta di inutilizzabilità della prova illegittimamente acquisita — solo più tardi introdotta con la riforma del codice — con un passaggio celebre che vale comunque la pena citare, secondo cui dall'art. 15 comma 1 Cost. è possibile inferire «il principio secondo il quale attività compiute in dispregio dei fondamentali diritti del cittadino non possono essere assunte di per sé a giustificazione ed a fondamento di atti processuali a carico di chi quelle attività costituzionalmente illegittime abbia subito».

La verità è che le intercettazioni, come pure tutte le forme di sorveglianza elettronica, si collocano in un crocevia di interessi in conflitto: da un lato l'esigenza di svolgere le indagini e del segreto investigativo; dall'altro la tutela della segretezza delle comunicazioni e della riservatezza personale; per altro verso, il diritto di cronaca, del quale ha avuto più di una volta occasione di occuparsi la Corte europea, secondo cui la riservatezza non può essere invocata a fronte dell'art. 10 Cedu quando si tratta di un personaggio politico pubblico; infine, ma non per ultima, la tutela del diritto di difesa.

A questo punto appare chiaro che la garanzia costituzionale deve abbracciare tutte le possibili forme di interferenza nella vita privata. Al di là dell'intercettazione di comunicazioni in senso stretto, si può provare a fare un elenco delle possibili interferenze, probabilmente non esaustivo: l'intercettazione di flussi di dati; la conservazione dei dati esterni delle comunicazioni (*data retention*); la remotizzazione degli ascolti; l'instradamento delle comunicazioni internazionali; le ispezioni e perquisizioni informatiche; l'acquisizione della messaggistica istantanea, criptata o no; il sequestro della memoria del dispositivo; la geolocalizzazione; il *pen register*, che tiene traccia di tutte le chiamate in uscita; lo *stingray*, simulatore di telefono cellulare, sia attivo che passivo. Infine, il captatore informatico, un virus le cui potenzialità invasive sono enormi, che ha la possibilità di prendere possesso di qualunque dispositivo connesso ad internet con i privilegi di amministratore, con tutto ciò che ne consegue in termini di sorveglianza elettronica.

Per questo motivo non può essere condiviso quello che è diventato una sorta di luogo comune: si usa parlare di "neutralità tecnica" delle norme di garanzia, sarebbe cioè indifferente lo strumento che viene usato, purché sia tutelato il nucleo essenziale del diritto che deve essere riconosciuto. Ma in realtà c'è una enorme differenza, ad esempio, fra l'intercettazione di una comunicazione, la ripresa visiva, il virus informatico inserito nel cellulare, e così via. Il tipo di strumento condiziona gli effetti e i risultati, e le garanzie debbono essere tarate sulle modalità e sull'obiettivo. Al riguardo, ancora dalla Corte costituzionale tedesca, è stato affermato il cosiddetto "*purpose limitation principle*", vale a dire il principio secondo cui l'intervento deve essere limitato in funzione del legittimo scopo che viene perseguito.

Sulla circolazione dei dati così acquisiti da un procedimento all'altro occorre poi tener presente che ogni volta che si utilizza un dato di questo genere si realizza una nuova violazione della segretezza, che deve trovare giustificazione. Non basta l'esistenza a monte di un'autorizzazione di un giudice per concludere che il diritto è sufficientemente tutelato. L'utilizzazione in altra sede deve sempre restare un'eventualità eccezionale, perché l'autorizzazione originaria, emessa in un contesto differente, non può rappresentare un *passe-partout* mediante il quale la prova risulta una volta per tutte legittimata ed è possibile usarla dovunque e a qualunque fine. E l'osservazione diventa di particolare attualità se si pensa alla ben nota vicenda dei criptofonini (che aveva già visto intervenire la Corte di giustizia UE), concernente la trasmissione, richiesta con ordine europeo di indagine, del contenuto di comunicazioni già acquisite e decrittate dall'autorità giudiziaria estera in un procedimento penale pendente davanti ad essa.

Va infine ricordato che occorre anche evitare di cadere in quello che qualcuno ha acutamente definito "pregiudizio tecnologico", a causa del quale si tende a considerare i dati acquisiti con questo tipo di strumenti come dati oggettivi ed inconfutabili, validi ovunque. Non è così: si tratta infatti soltanto di indizi, e a volte nemmeno di indizi, ma di semplici notizie di reato. Il risultato delle intercettazioni spesso può essere ambiguo e persino fuorviante, spesso non è nemmeno correttamente conservato, spesso si basa su trascrizioni non fedeli e imprecise, su traduzioni e interpretazioni erronee, o pregiudicate dall'eventuale esclusione di brani di conversazione che potrebbero invece essere rilevanti.

In ogni caso le prove vanno cercate senza commisurarle all'obiettivo di prendere di mira una qualsiasi persona. Già negli anni sessanta del secolo scorso, erano espressamente vietate, negli Stati Uniti, quelle che venivano chiamate intercettazioni generali, dirette cioè a mettere sotto sorveglianza un sospettato in attesa di scoprire qualche elemento a suo carico: dal momento che è sempre necessario che esistano specifici motivi che giustifichino la restrizione del diritto fondamentale. In linea di principio, dunque, deve escludersi che le intercettazioni possano essere impiegate per andare alla ricerca di possibili reati. E la medesima logica va applicata anche, *mutatis mutandis*, all'utilizzazione dei dati ottenuti con la sorveglianza elettronica al di fuori del procedimento in cui sono state autorizzate. Altrimenti, come ha di recente riconosciuto anche la Corte costituzionale italiana, l'autorizzazione del giudice sarebbe un'autorizzazione in bianco, priva cioè del suo requisito essenziale, una motivazione pertinente e specifica.