Revista Ítalo-Española de Derecho Procesal
Vol. 1 | 2019 4 pp.
Madrid, 2019
Marcial Pons Ediciones Jurídicas y Sociales

ISSN: 2605-5244

EDITORIALE

Il progresso scientifico e tecnologico, lo sappiamo, è sempre più veloce della risposta legale alle nuove sfide che ne derivano. La tecnologia fornisce oggi strumenti, di uso comune, ancora impensabili solo una decina di anni fa. Ciò si riflette in maniera diretta e significativa anche nella sfera processuale.

L'informatica mette a disposizione, soprattutto nel processo penale, possibilità inedite di svolgere indagini e di accertare i fatti rilevanti in maniera efficace. Si tratta anche di una necessaria risposta allo sviluppo ed alla evoluzione delle organizzazioni criminali moderne, a livello nazionale e transnazionale. Ma la sorveglianza elettronica e il controllo dei dati personali e dei comportamenti privati, anche se sono spesso in grado di produrre effetti positivi nel contrasto alla criminalità, trovano attuazione in maniera sempre più sofisticata ed invasiva nei confronti dei diritti fondamentali.

Dal punto di vista pratico, inoltre, il ruolo centrale che questo genere di accertamenti va assumendo –anche per la loro presunta maggiore attendibilità– rende sempre meno rilevanti i mezzi di prova tradizionali, come le prove dichiarative, e finisce col relegare ai margini anche il diritto al contraddittorio inteso come diritto al confronto con i testimoni, consacrato nelle carte internazionali dei diritti quale requisito del *fair trial.* Non di rado il dibattito processuale si svolge solo sull'interpretazione del prodotto di un'intercettazione, di una videoripresa o dell'analisi di dati; e la stessa attività di indagine punta principalmente sulla tecnologia, che rappresenta spesso una facile e rapida alternativa alla faticosa ricerca di informazioni e di indizi materiali utili alla ricostruzione dei fatti.

Un'altra conseguenza è il progressivo appannamento della distinzione fra prevenzione e accertamento dei reati. L'uso degli strumenti informatici per fini preventivi non è soggetto alle garanzie del processo penale, anche se può incidere sui diritti individuali e costruire le basi per l'azione penale. La legge dovrebbe dunque delimitare con la massima precisione questi interventi, rispettando anche il principio di proporzionalità ripetutamente affermato dalle corti costituzionali e dalle corti europee.

Ma forse è il momento di prendere atto che non è più sufficiente che siano assicurate le garanzie tradizionali di tipo liberale, finalizzate alle espressioni fisiche della personalità individuale, come la libertà personale, domiciliare, di circolazione, di comunicazione, di manifestazione del pensiero. Sempre più importanti, nella società attuale, sono i diritti connessi con la libertà morale, la dignità della persona, l'autodeterminazione, e specialmente la disponibilità dei dati e delle informazioni personali. Com'è noto, già nel 2008 il *Bundesverfassungsgericht* tedesco ha elaborato la definizione di "domicilio informatico", al fine estendere la tutela costituzionale a quella espansione della vita dell'individuo rappresentata dalla utilizzazione quotidiana dei mezzi di comunicazione elettronici. Forse è anche necessario abbandonare l'approccio esclusivamente personalistico delle carte dei diritti e chiedersi se non sia piuttosto necessario riconoscere l'esistenza di un interesse collettivo alla sicurezza dei dati e delle comunicazioni elettroniche.

Si parla in questi casi dell'emersione di "nuovi diritti", ma è forse più corretto parlare di nuove manifestazioni dei diritti inviolabili già riconosciuti, o di contenuti impliciti nella tutela dei diritti espressamente nominati, se non addirittura di diritti preesistenti e coessenziali allo stesso ordinamento costituzionale. E non è estranea a questa nuova dimensione la loro affermazione nelle fonti internazionali, che compongono insieme alle costituzioni nazionali un quadro di garanzie ormai indissolubile.

L'art. 8 della Convenzione europea dei diritti dell'uomo prevede il rispetto della vita privata e familiare, del domicilio e della corrispondenza, e l'art. 10 include nella libertà di espressione la libertà di ricevere e comunicare informazioni. La Carta dei diritti fondamentali dell'Unione europea ribadisce queste garanzie nei corrispondenti artt. 7 e 11, aggiornandone la formulazione (si parla di "comunicazione" anziché di corrispondenza) e menzionando specificamente, all'art. 8, il diritto alla protezione dei dati personali, che peraltro si può ritenere già incluso nella generale tutela della *privacy*. In ogni caso, le clausole di salvaguardia contenute rispettivamente nell'art. 53 CEDU e nell'art. 52 comma 3 CDFUE consentono l'allineamento dei diritti riconosciuti nelle diverse sedi.

La necessità della tutela legale aumenta con l'ampliarsi delle informazioni reperibili nella moderna società della comunicazione. Si pensi ai numerosi *data bases* pubblici e privati, di dimensioni enormi, e alla possibilità di condivisione e di scambio delle notizie in essi contenute; alle informazioni biometriche, che possono includere anche dati particolarmente sensibili come le cartelle cliniche elettroniche; agli elementi contenuti negli spazi virtuali (*cloud based data)*; ed anche – ormai non è più un semplice futuribile - al cosiddetto internet delle cose. A ciò si aggiungono, specie a livello di indagini preventive, le tecniche di elaborazione dei dati: estrazione (*data mining*), confronto (*data matching*), profilazione (*data profiling*). Le corti europee si sono ripetutamente occupate della conservazione dei dati personali (*data retention*), imponendo limiti precisi, con riferimento fra l'altro all'esigenza di previsioni legislative chiare ed accessibili, alla durata e allo scopo della conservazione, alla loro circolazione, alle garanzie contro gli abusi e l'accesso illegale. Non tutte le legislazioni nazionali, anche quelle più recenti, sembrano tuttavia aver recepito in maniera adeguata tali indicazioni.

Il controllo è reso inoltre difficile dallo scambio automatico di dati tra le diverse fonti e dalla possibilità di una elaborazione automatica. L'ultima frontiera, nel momento attuale, è rappresentata dalla cosiddetta prova digitale, generata automaticamente da un algoritmo che elabora i dati raccolti, superando così o almeno ridimensionando fortemente anche la valutazione critica ad opera delle parti e dello stesso giudice. Di questo argomento e delle connesse problematiche, soprattutto con riferimento al diritto di difesa, si occupa Serena Quattrocolo nel documentato e approfondito saggio contenuto in questo numero. Ma il tema è ancora più ampio, poiché com'è noto si stanno sperimentando oltreoceano algoritmi predittivi, come quelli studiati nel suo recente libro da Jordi Nieva Fenoll, che pretenderebbero di fornire al giudice strumenti di conoscenza basati su calcoli probabilistici, svolti mediante i dati immessi nel sistema (salvo poi scoprire che il risultato dipende dalla scelta dei dati ritenuti rilevanti). Si sta andando verso la fantomatica "macchina sillogizzante" destinata a sostituire il giudice?

Tornando alle forme di interferenza diretta nella vita privata, è facile constatare come oggi l'intercettazione delle comunicazioni telefoniche è solo un aspetto, e forse neanche più il principale, delle tecniche di sorveglianza elettronica: che comprendono, fra l'altro, l'ascolto delle conversazioni di persone presenti, le riprese visive, le intercettazioni della posta elettronica e dei *social networks*, le perquisizioni informatiche, il controllo degli accessi ad internet e, più in generale, la presa di possesso del terminale informatico, fisso o mobile, mediante il cosiddetto *trojan virus*.

Si comprende allora che è necessaria una normativa più articolata, corrispondente alle diverse forme che il controllo occulto può assumere: non è più sufficiente una generica riserva di legge e di giurisdizione, ma occorre differenziare presupposti, limiti e modalità a seconda del grado di intrusività della singola misura restrittiva.

Ma come va misurato il grado di intrusività? Se è vero, come ha ribadito il *Bundesverfassungsgericht* nel 2016 - pur ammettendo in linea di principio la sorveglianza elettronica – che va sempre rispettato il nucleo fondamentale della vita privata, occorre determinare il livello della interferenza: in relazione alla natura dei dati (per esempio, se si tratta del contenuto di una comunicazione o dei suoi dati esterni), alla loro quantità, anche in dipendenza dalla durata della misura, alle potenzialità dello strumento tecnico utilizzato. Si usa parlare al riguardo di neutralità tecnica delle norme di garanzia, poiché non conterebbero le modalità dell'intervento ma il diritto di volta in volta tutelato: però questo non sembra necessariamente vero, dato che nel rispettare i principi di idoneità, necessità e proporzionalità della misura, come affermati dalla giurisprudenza europea e costituzionale, occorre tener conto anche delle violazioni strumentali e collaterali all'impiego di un determinato espediente, indipendenti dall'obiettivo legittimamente perseguito, e dovrebbe quanto meno essere specificato quali sono le tecniche ammissibili.

In conclusione, anche se ciò lascia inevitabilmente spazio a valutazioni discrezionali, il parametro di riferimento fondamentale dovrebbe essere costituito da quella che viene definita "ragionevole aspettativa di *privacy*": dipendente dal grado di segretezza, soggettivo ed oggettivo, del dato ricercato, così come dalle finalità del suo impiego, con la necessità di una tutela maggiore in vista dell'eventuale acquisizione a fini probatori.

Come si accennava all'inizio, l'aggiornamento della risposta del diritto è appena cominciata.

Giulio ILLUMINATI