GIUSTIZIA INSIEME

Processo Penale

Audizione al Senato del Procuratore Nazionale Antimafia Giovanni Melillo sul tema delle intercettazioni del 31 gennaio 2023

di Giovanni Melillo

3 febbraio 2023

I fattori di criticità della materia delle intercettazioni appaiono, ad un'osservazione obiettiva, tali e tanti da mettere in crisi ogni ambizione di poter realizzare altro che progressive tappe di una faticosa ricerca di equilibri resi continuamente precari dalle evoluzioni tecnologiche e degli stessi fenomeni criminali.

Siamo di fronte a tensioni che attraversano i sistemi giuridici di tutte le società democratiche e che continuamente si trasformano e impongono nuove sfide.

Naturalmente, molto può farsi. A condizione di sottrarsi alla tentazione di rendere una materia così delicata oggetto di continue contrapposizioni polemiche e grossolane o strumentali semplificazioni, anziché di uno sforzo condiviso e responsabile di avvicinamento ad una dimensione problematica di straordinaria complessità, che, per di più, nello scenario italiano soffre l'effetto della perdurante azione di ulteriori fattori di criticità.

Proverò ad indicare alcuni di tali fattori, nei quali, a mio avviso, possono scorgersi i tratti di evidenti ritardi istituzionali, legislativi e degli assetti organizzativi del sistema giudiziario, che definiscono altrettanti profili di responsabilità.

Ma, confidando nell'interesse di codesta Commissione a conoscere le valutazioni del Procuratore nazionale antimafia e antiterrorismo, proverò anche ad indicare anche alcune possibilità, da tempo mature, per realizzare una manovra di deciso rafforzamento del quadro delle garanzie difensive, senza detrimento delle istanze di efficace contrasto di gravi fenomeni criminali.

Una manovra possibile soltanto avendo avuto cura di sgombrare il capo da grottesche e miopi visioni di una realtà oltremodo complessa, che esige analisi realistiche e rigorose, anche se non sempre confortanti, derivandone da esse, infatti, non già le illusorie ricette che ordinariamente discendono dall'insofferenza per la complessità dei problemi da considerare, ma la responsabilità di un impegno gravosissimo per le istituzioni politiche, amministrative e giudiziarie.

Procederò ad una rassegna tanto dei fattori di criticità quanto di alcune possibili vie d'uscita con criteri descrittivi ai limiti della brutalità delle necessarie sintesi.

- *La trasformazione del rapporto fra giurisdizione e tecnologie conseguente al passaggio nell'era digitale*: da tempo fanno ingresso nel processo penale gigantesche masse informative ed enormi flussi di dati personali, ciò che acuisce e finanche drammatizza, da un lato, il tema della tutela dei diritti individuali trascinati nelle indagini e nel processo e, dall'altro, il ritardo del sistema giudiziario a dotarsi di tecnologie e saperi, ma vorrei dire anche di una cultura delle nuove tecnologie, di cui vi è necessità impellente per governare i rischi di collisione fra le ragioni di giustizia e i beni e gli interessi, privati e istituzionali, complessivamente coinvolti;

- *L'ingresso del digitale nella vita di organizzazioni e reti criminali*: quando si valuta l'aggressività delle tecniche investigative, occorre tener conto anche della straordinaria vitalità delle tecniche di elusione di ogni controllo collegata alla capacità, non solo del crimine organizzato mafioso, di dotarsi di tecnologie in grado di preservarne l'impenetrabilità: piattaforme criptate e ricorso al *dark web* per le ordinarie comunicazioni telematiche, sofisticati sistemi di sorveglianza elettronica delle aree di interesse, ossessiva cura della segretezza di movimenti e comunicazioni dei vertici dei gruppi criminali. Giovanni Falcone, ricorderete, diceva "*i mafiosi saranno avranno sempre una lunghezza di vantaggio su di noi*". Un modo semplice, ma acuto, per indicare una caratteristica costante della criminalità mafiosa: la sua capacità di agire avvalendosi di straordinarie capacità di adattamento, ma anche di conoscenza della modernità e delle sue tecnologie. La lungimiranza di quel giudizio è visibile nei dati dell'ordinaria esperienza investigativa, attraverso la visione di vere e proprie nuove componenti dei gruppi criminali, costituite da complesse funzioni di *security*, ossessivamente protese a prevenire ogni controllo, a controllare ogni potenziale rischio d'indagine, a proteggere e bonificare ogni luogo e dispositivo

utilizzato a fini criminosi, a dotarsi di dispositivi di *storage* dei dati di gestione degli affari criminali e delle collegate attività di reinvestimento speculativo e riciclaggio assolutamente impenetrabili. Questa dimensione funzionale del crimine organizzato è in parte tutta interna alle organizzazioni criminali, generando nuove figure direttive e nuove leadership, e in parte si intreccia invece con l'ordinario sistema d'impresa del mondo *cyber* e con le stesse funzioni investigative, l'uno e le altre essendo continuamente esposte a pesante pressione corruttiva e collusiva: non vi è indagine di mafia nella quale non si registrino tracce di evidenti di ciò, ciò che in controluce rivela che la diretta penetrazione di presenze e interessi mafiosi nel concreto agire di *cyber security* è un rischio sempre più concreto e reale.

- *La continua modificazione del panorama investigativo che si realizza quando entrano in gioco, ed è ormai regola nelle indagini appena rilevanti, le tecniche investigative impiegate in altre giurisdizioni*: le piattaforme telematiche criptate: non è possibile entrare nei dettagli di questa ormai nota frontiera investigativa, ma certo i confini dei relativi campi problematici non possono essere tracciati prescindendo da ciò che avviene nei sistemi ancorati rigidamente al *rule of law*, a meno di optare per un impossibile isolamento internazionale e di pagare il prezzo di un arretramento della nostra capacità di contrasto dei più gravi fenomeni criminali: un tema assai delicato, dove è in gioco persino il tradizionale primato di professionalità ed efficacia dei nostri apparati di polizia, di fatto pressoché esclusi da ambiti di cooperazione che esigono la condivisione di eccezionali risorse tecnologiche e di nuovi strumenti operativi, come l'impiego a fini investigativi, pur rigidamente controllato attraverso la fissazione di rigorosi presupposti e limiti, di nuove tecniche intrusive e di quei medesimi *hackers etici* che anche lo Stato ha per fortuna, sia pure solo in tempi recentissimi, imparato ad utilizzare per sottoporre i propri sistemi informati a *stress test* necessari per saggiarne la resistenza ad attacchi interni ed esterni; oggi le indagini più importanti in materia di narcotraffico e di riciclaggio si nutrono di acquisizioni probatorie rese possibili da quadri normativi e strumenti investigativi più avanzati di quelli disponibili per la magistratura e le forze di polizia italiane. Basterebbe pensare, per apprezzare i divari normativi delle condizioni del lavoro investigativo, alle previsioni del codice di rito francese che consentono l'istallazione di un dispositivo tecnico per accedere, archiviare e trasmettere dati informatici memorizzati in un dispositivo anche attraverso il ricorso a risorse dello Stato soggette al segreto di difesa nazionale ai sensi dell'art. 706-102-1**[1]** e ss. del codice di procedura penale. Ma analoghe possibilità si rinvengono nelle legislazioni tedesche, olandesi e belghe, consentendo attività, ormai giunte alla violazione *live* di quelle piattaforme criptate, impossibili nello scenario italiano, ma essenziali per l'efficacia delle indagini in materia di criminalità organizzata e terrorismo. La necessità di avanzamento delle frontiere normative e

delle capacità investigative è ancor più visibile considerando gli effetti e l'impatto complessivo di uno scenario globale segnato da conflitti armati ed ibridi, nei quali è diffuso l'impiego anche sperimentale di tecnologie aggressive dei sistemi informativi, che inevitabilmente si trasferiranno nel mercato dell'impresa, a disposizione anche delle reti criminali mafiose e terroristiche. Può sembrare una prospettiva di rischio lontana, ma così non è, se soltanto si guarda al ruolo che tipicamente quelle reti criminali da sempre giocano nelle aree segnate da profondi processi di destabilizzazione.

- *Una lunga stagione di pratica subalternità cognitiva della macchina giudiziaria, ma anche degli apparati di polizia nell'impiego a fini di giustizia delle tecnologie digitali*: a quelli appena accennati è collegato intimamente un ulteriore fattore di criticità, che da tempo io individuo nel determinarsi – a valle di una prolungata stagione di tacita rinuncia dello Stato ad esercitare la responsabilità di investire in tecnologie digitali e, quel che più conta, di impegnarsi nell'organizzazione e nel controllo gestionale dell'impiego a fini di giustizia di quelle sempre più raffinate tecnologie – nel determinarsi e nel persistere di una condizione, culturale prima ancora che pratico-operativa, di grave subalternità, innanzitutto cognitiva, dell'amministrazione della giustizia e, dunque, della giurisdizione e delle nostre pur straordinarie forze di polizia, rispetto alle tecnologie impiegate nelle indagini, totalmente in mani private e di regola impiegabili soltanto attraverso la mediazione tecnica di soggetti privati. Altro che le "risorse dello Stato soggette al segreto di difesa nazionale" previste dalle leggi francesi: in Italia, l'uso investigativo delle tecnologie, soprattutto di quelle più sofisticate e invasive, richiederebbe più incisive e mature *policies* di sicurezza effettivamente riconducibili alla responsabilità dello Stato (uso da anni, per indicare una via d'uscita, una metafora ferroviaria: i vagoni possono essere privati, ma i binari devono essere tracciati e presidiati da agenti pubblici). Il tema riguarda, volendo, anche le funzioni di *intelligence* e, dunque, di preservazione della sicurezza della Repubblica, dal momento che le garanzie funzionali in questo ambito delle agenzie si realizzano con le stesse tecnologie e mediante l'impiego dei medesimi fornitori utilizzati dalla giustizia penale, ai quali ultimo è dovuto affidamento, che non può essere tuttavia assoluto, come dimostrano casi emblematici, quale quello rivelato dalle indagini della Procura di Napoli sul programma *Exodus*, che forse già dal nome avrebbe dovuto suscitare apprensione in chi scelse di dotarsi di un *software* per intercettazioni telematiche con captatore informatico che operava trasferendo in chiaro su un server in Colorado del sistema di *cloud* di *Amazon* i dati captati, come tali visibili da chiunque sul *web*.

Dunque, il sistema esige una profonda e complessiva opera di razionalizzazione e securizzazione, che modifichi sensibilmente prassi, abitudini e comportamenti, ingenerati da

una lunga stagione di pauperismo e subalternità tecnologica dell'amministrazione della giustizia e degli apparati di polizia, in grado di incidere negativamente, oltre che sull'efficacia delle indagini, anche sulla correttezza del trattamento dei dati personali e, dunque, sulla tutela della riservatezza delle persone coinvolte a vario titolo nelle indagini e nei processi.

Il Garante della protezione dei dati personali, del resto, di ciò ebbe modo di accorgersi, allorquando, nell'estate del 2013, adottò una delibera che improvvisamente aprì uno squarcio nell'allora debolissimo tessuto protettivo dei dati personali delle intercettazioni.

I Procuratori della Repubblica furono per la prima volta indicati come responsabili del trattamento dei dati personali e chiamati ad assumere iniziative rigorosamente ispirate dalla necessità di alzare, praticamente da terra, gli standard di sicurezza delle sale e delle procedure organizzative funzionali alle intercettazioni.

Fortunatamente, molto tempo è passato. Molte cose sono cambiate.

Poco dopo quella delibera, infatti, fu avviata una significativa azione di potenziamento delle misure di sicurezza dei sistemi di gestione delle intercettazioni.

Anche su tale scia, molti uffici requirenti hanno sviluppato una più avanzata cultura della sicurezza dei dati delle intercettazioni, ricercando e applicando soluzioni persino più avanzate di quelle richieste dalla legge per la corretta e sicura gestione dei dati delle intercettazioni, nella consapevolezza del ruolo di garanzia della legalità processuale nella fase delle indagini preliminari che il p.m. deve conservare e che appare francamente preoccupante che sia considerato con sufficienza e approssimazione concettuale.

Oggi questi temi sono al centro del confronto permanente che la DNA ha avviato con tutti i Procuratori distrettuali: un confronto necessario per ancorare il coordinamento investigativo a modelli organizzativi e metodologie di lavoro razionali e uniformi.

Ma molte cose devono essere ancora fatte, soprattutto per estendere le prassi virtuose a tutti gli uffici e, in particolare, anche alle Procure ordinarie dalle più piccole dimensioni, ove si concentrano maggiormente le debolezze infrastrutturali e il correlato rischio di introduzione di prassi improprie e inadeguate.

È una strada lunga quella che occorre percorrere, senza interrompere il cammino sia pure faticosamente fatto sin qui, del quale sono parte essenziale:

> il principio posto alla base della riforma del 2017, secondo il quale, quali che siano presupposti e limiti di utilizzabilità delle intercettazioni, occorre preservare dalla conoscenza di persone diverse dai soggetti processuali la conoscenza delle intercettazioni

irrilevanti a fini di giustizia e, a maggior ragione, di quelle inutilizzabili; le une e le altre devono essere definitivamente segregate e protette da ogni pubblicità;
per questa ragione viene introdotto uno strumento nuovo: l'Archivio riservato delle intercettazioni: come preciserò, tale strumento è, per scelta normativa, soltanto parzialmente utilizzato, ma ha grandi potenzialità, poiché consente ulteriori, grandi implementazioni delle funzioni di segregazione e controllo della corretta gestione dei dati, attraverso l'auspicabile estensione dell'obbligo del suo impiego per la gestione di attività d'indagine, che non sono *stricto iure* captazioni, ma che determinano l'acquisizione di masse di dati personali persino più grandi e delicate (dalle funzioni di *on line search* dei captatori telematici, vale a dire di ricerca file nella memoria dei dispositivi e di *keylogger* sino alle copie forensi dei dispositivi di comunicazione oggetto di ispezione e sequestro); ciò comporterebbe la conseguenza di estendere anche a queste attività le regole del codice che impongono una rigorosa e controllata dal giudice selezione dei dati rilevanti e utilizzabili e la definitiva segregazione di quanto il giudice ritenga irrilevante ed inutilizzabile);
il decreto ministeriale 20 aprile 2018, che ha introdotto disposizioni per definire i requisiti tecnici dei programmi informatici funzionali all'esecuzione delle intercettazioni mediante captatore, a partire dalla regola fondamentale che tali programmi siano elaborati ed utilizzati assicurando l'integrità, la sicurezza e l'autenticità dei dati captati su tutti i canali di trasmissione riferibili al captatore; un ambito problematico delicatissimo, ma che esige chiarezza e la preservazione del dibattito dal rischio di enfatizzazione di allarmi infondati e suscettivi di uso strumentale: è ben vero che tecnicamente è possibile elaborare e impiegare *malware* in grado di manipolare i dati, distruggendoli o creandoli, ma si tratterebbe (oggi come ieri, per le analoghe attività abusive astrattamente possibili nell'epoca dell'analogico e dei verbali cartacei) di attività illegali, sanzionate penalmente in modo severo, potendo di volta in volta integrare, a seconda dei casi, i delitti di depistaggio, di intercettazione illegale, di accesso abusivo a sistemi informatici e telematici, di frode in pubbliche forniture, di calunnia, di falso materiale o ideologico in atti pubblici, di favoreggiamento. Il richiamo a queste gravi ipotesi delittuose vale a rendere chiaro che gli abusi in questo campo non sono senza prezzo: la vicenda *Exodus*, già richiamata nelle audizioni che hanno preceduto la mia, sta lì a dimostrarlo, se, dopo aver segnalato le relative pratiche abusive, si tiene a mente che si tratta di abusi individuati dalla magistratura, che ha proceduto immediatamente nei confronti dei responsabili della società che gestiva quel *software* illegale per le intercettazioni mediante captatore informatico, che peraltro è risultato nella disponibilità anche delle agenzie di *intelligence*. Un dato che segnalo soltanto per indicare che i rischi collegati alla dipendenza cognitiva dello Stato dalle tecnologie private hanno dimensione più ampia di quella data dalla visione delle intercettazioni giudiziarie, ma anche per sottolineare che lo Stato e la magistratura non assistono inermi alla consumazione di abusi e delitti in danno dell'amministrazione della giustizia e delle libertà dei cittadini. Come è avvenuto anche quando è stata denunciata, a margine di una famosa vicenda processuale, tutt'ora in corso, la possibilità che ci fosse stato un illecito uso dei dispositivi di memorizzazione dei dati trasmessi da un

captatore informatico: in questo caso, escludendosi, allo stato delle mie conoscenze, la fondatezza di quelle allarmanti ipotesi, sulla base di immediati e approfonditi accertamenti, svolti in contraddittorio con le parti private, affidati congiuntamente da tre procure della Repubblica agli specialisti del C.N.A.I.P.I.C. della Polizia postale e delle comunicazioni.

Al decreto del 2018 avrebbe dovuto accompagnarsi un altro, volto all'istituzione di un Tavolo tecnico presso il Ministero della giustizia per il monitoraggio del sistema delle prestazioni obbligatorie, intervenuto soltanto pochi giorni fa; il Tavolo tecnico è uno strumento essenziale per presidiare le funzioni di controllo pubblico sui rischi correlati all'impiego di tecnologie sempre più invasive; per di più uno strumento flessibile, che consente anche la partecipazione di rappresentanti di culture e interessi diversi, dall'accademia al mondo dell'impresa; un altro passo importante che potrà dare frutti importanti, attraverso un lavoro collegiale al quale sono chiamati a partecipare anche il Procuratore generale della Cassazione e il Procuratore nazionale antimafia e antiterrorismo, ma al quale è prevista e auspicabile la partecipazione anche di altri Uffici giudiziari.

Come si accennava, il nuovo decreto sulle tariffe delle prestazioni funzionali all'esecuzione delle intercettazioni, per quanto adottato faticosamente e con non poche traversie del suo cammino, è infine giunto al traguardo, ponendosi come importante strumento di garanzia: non solo dell'uniformità e dell'economicità delle relative spese, ma dell'interesse generale a definire e a rendere uniforme un profilo identitario dei fornitori e delle tecnologie impiegate, secondo principi di trasparenza, affidabilità tecnologica e organizzativa, correttezza del trattamento dei dati personali, integrità e sicurezza dei dati e tracciabilità di ogni attività che li riguardi; anche in questo caso, l'esperienza delle Procure che si erano già dotate di standard di sicurezza assai elevati ha molto contribuito a definire i contenuti del decreto, come può agevolmente rilevarsi, confrontando le misure organizzative che il decreto oggi rende obbligatorie per tutti ai provvedimenti organizzativi già adottati, fra le altre, dalle Procure di Napoli, Torino e Milano.

Nella sua premessa, il decreto 18.10.2022 reca finalmente la prima, pur debolissima, traccia normativa di un altro, essenziale passaggio evolutivo dei sistemi di intercettazione: " *occorre proseguire nella razionalizzazione tecnica ed organizzativa dei sistemi di intercettazione, avente quale obiettivo finale la realizzazione di cinque data center nazionali, e che tale processo deve essere accompagnato da una revisione sistematica dei metodi di programmazione delle spesa relativa*": a questo obiettivo si lega la responsabilità, anche politica, di realizzare urgentemente il consolidamento delle attuali 140 sale server (attraverso la creazione di poche sale interdistrettuali, governate da architetture digitali e logiche di gestione direttamente definite e controllate dal Ministero, ovviamente nella cornice data dal perimetro nazionale della cybersicurezza): si tratta di un progetto a lungo rimandato, benché ricompreso sin dal 4 aprile 2017, dal Piano decennale di finanziamenti per gli investimenti nel settore delle infrastrutture digitali dell'amministrazione giudiziaria che nasceva dallo sforzo di ripensare l'intera architettura dei sistemi di intercettazione alla luce delle indicazioni date dal Garante nazionale della privacy nel 2013; è del tutto

evidente, infatti, che 140 sale server, per di più gestite secondo modelli differenziati, offrivano e tuttora offrono garanzie solo apparenti ai temi della sicurezza, essendo costituite da macchine e algoritmi gestiti da privati, la conoscenza e l'uso dei quali avviene soltanto attraverso la mediazione dell'impresa privata. Il consolidamento delle infrastrutture è un passaggio essenziale e una scelta non più eludibile o rinviabile, sulla quale da tempo convergono le sensibilità maturate fra le procure distrettuali. Da questo passaggio, apparentemente pratico, dipende invece l'equilibrio complessivo del sistema e nessuna scelta normativa, anche oggi, potrebbe vantare credibilità prescindendo dalla sua realizzazione. Non solo: la mancata realizzazione di quel progetto consentirebbe di chiudere agevolmente la procedura di infrazione, per violazione delle regole sull'evidenza pubblica europea nelle procedure di affidamento dei servizi funzionali alle intercettazioni, da tempo pendente nei confronti dell'Italia. Io credo che il Parlamento possa far molto anche vigilando sulla tempestività dei processi organizzativi necessari alla coerente attuazione delle leggi adottate e dettando per essi direttive e cadenze rigorose.

Lo stato dei processi di digitalizzazione e la gestione dell'Archivio delle Intercettazioni: questo fondamentale strumento di segregazione delle intercettazioni inutilizzabili o non rilevanti a fini di giustizia ha dimostrato di funzionare: anzi, come già detto, deve estendersene l'impiego al complesso dei dati personali afferenti alle comunicazioni che cadono nell'orbita delle investigazioni (da quelli acquisiti con il captatore con funzioni *on line search* alle copie forensi di dispositivi oggetto di ispezione, perquisizione e sequestro, sino ai servizi di videosorveglianza o di localizzazione con GPS, talvolta non meno invasivi delle intercettazioni), che invece oggi, di regola, con l'esercizio dell'azione penale sono assoggettati al regime di pubblicità proprio della fase del giudizio. Ma già attualmente il sistema, da tutti apprezzato, rivela criticità: di capienza, per insufficienza delle architetture di *storage*, di sicurezza, per la perdurante assenza di sistemi di monitoraggio degli accessi, delle operazioni e degli interventi sui server delle imprese fornitrici dei servizi (il *software* sperimentato a Milano e Napoli dal Ministero, il cd. *Bomgar*, sembra essere stato accantonato, per ragioni non chiare: forse, perché lento e inadeguato, ma, forse, anche per la resistenza opposta dalle società del settore all'introduzione di controlli sulle fonti e le tecniche di inserimento dei dati), ma soprattutto pensato solo per la gestione del procedimento in corso, mancando ancora una regola temporale per la conservazione dei dati, di fatto imponendosi quella del *sine die*. Sono criticità che dovrebbero costituire oggetto di prioritaria considerazione politica e gestionale, salvo a voler rendere ancora una volta omaggio alla tradizionale indifferenza delle politiche della giustizia ai temi posti dalle tecnologie e dalla loro gestione, che hanno invece grande e silenzioso impatto sulla sorte dei diritti delle persone.

Soprattutto, molto può il Parlamento fare per l'avanzamento degli equilibri del rapporto fra esigenze delle indagini e diritti della persona: perché vi è bisogno di un deciso avanzamento di quegli equilibri, attraverso la previsione di nuove e più elevate garanzie individuali e della funzione difensiva.

Ma non vi è bisogno alcuno di indebolire senza ragione la capacità di risposta repressiva di gravi fenomeni criminali, perché ciò determinerebbe prezzi elevati da pagare e inevitabili, nuove e inconcludenti oscillazioni del pendolo legislativo.

Vi sono, dunque *rilevanti e anche gravi deficit normativi che aggravano le tensioni sul complesso rapporto fra segretezza delle indagini* (e dei contenuti e della stessa esistenza delle intercettazioni, in particolare) *ed effettività del diritto di difesa e della libertà di informazione*: sono profili bisognevoli di urgente intervento, possibile senza indebolire l'efficacia delle indagini.

Alcuni di tali profili sono da sempre sulla sfondo, ma vanno comunque indicati, per non sottacere i pericoli che si profilano quando se ne oscura il rilievo:

- l'ipocrita distinzione fra atto segreto e atto non più segreto, ma non pubblicabile: un tema che la dottrina liberale più autorevole addita da sempre come primo fattore di credibilità del sistema (basta rimandare agli scritti di Glauco Giostra e Francesco Palazzo e di tanti altri eminenti studiosi): un sistema razionale esigerebbe che ciò che sia segreto sia effettivamente tutelato e preservato come tale e ciò che segreto più non è possa essere pubblicato; la riforma del 2017 va in questa direzione, prevedendo, da un lato, la definitiva segregazione di ciò che non è utilizzabile e rilevanti a fini di giustizia e, dall'altro, la pubblicabilità delle ordinanze cautelari, salvo che nella parte riferita ai contenuti delle intercettazioni: una strada giusta, ma non interamente percorsa; peraltro, la disciplina transitoria, pur ragionevole, di fatto ha rallentato e persino ostacolato la stessa visione dell'importanza degli effetti pratici conseguenti alla riforma;
- la mancanza di una formale ed espressa previsione normativa sull'accesso degli organi di informazione agli atti non segreti esclusivamente mediante la procedura formale dell'art. 116 c.p.p.: non è la panacea di ogni male, ma l'esperienza dimostra che, dove si applica quella procedura, si sopiscono le tensioni e si annullano quasi i rischi propri del sistema di *scambi immorali* denunciato da anni dal giornalismo più attento e colto; sancire espressamente la legittimità di quell'interpretazione, che fortunatamente va estendendosi, varrebbe a consolidare e diffondere modelli più avanzati, in linea con l'idea fondamentale che vuole le democrazie fondate sui principi di indipendenza della funzione giudiziaria e di libertà di informazione.

Ma altre questioni sembrano estranee al dibattito pubblico e sono a mio avviso, invece, straordinariamente rilevanti nella prospettiva del potenziamento delle garanzie difensive e del contenimento del rischio di abusi.

Ed è di questi ultimi profili che, a mio sommesso avviso, occorre la più urgente valutazione del legislatore.

Li indico assai sommariamente, ma spero con sufficiente chiarezza, atteso il rilievo cruciale dei relativi passaggi normativi.

Vi è un evidente ritardo normativo nel prendere atto della profonda necessità di innalzamento delle garanzie legali collegate alla tutela dei dati personali che confluiscono nei sistemi digitali: un ritardo evidente, direttamente collegato al da tempo sopravvenuto rilievo eccezionale dei dati personali diversi da quelli oggetto della tradizionale captazione delle comunicazioni: ma tale da imporre, come è stato detto, "*la formulazione di un nuovo apparato normativo dagli orizzonti più vasti*" (Marafioti, 2023). La stessa nozione codicistica di "intercettazione", intesa quale captazione clandestina dei flussi di comunicazione in atto fra due soggetti, entra in crisi nell'era digitale, non valendo ad abbracciare e disciplinare unitariamente fenomeni diversi, ma caratterizzati comunemente dalla sottrazione alla sfera di privatezza delle persone di dati di straordinario rilievo giuridico e sociale. È questo un punto cruciale per cogliere la radice di tensioni che la giurisprudenza mostra di non saper risolvere e che probabilmente non può risolvere, come dimostra la sofferenza visibile nell'impiego delle tradizionali categorie del *documento* e della *corrispondenza* per individuare la cornice normativa di attività invasive per le quali si rivela la necessità di rafforzamento delle garanzie individuali. Una sofferenza ancor più grande, perché palesemente sostenuta dalla consapevolezza che soltanto il legislatore può definire il punto di equilibrio fra efficienza delle indagini e tutela della riservatezza e delle altre libertà fondamentali; è forse giunto il momento di riconoscere che vi è un deficit di effettività del principio di legalità processuale e delle correlate garanzie difensive che può essere colmato senza pregiudizio per le esigenze di accertamento dei reati più gravi e in coerenza con l'intervento legislativo del 2017; mi riferisco alle possibilità di acquisizione occulta di *chat* pregresse e comunque di contenuti dei dispositivi di comunicazione telematica mediante captatore in funzione *on line search* o alle possibilità di ispezione, perquisizione e sequestro di archivi informatici, quali quelli contenuti anche in un semplice *smartphone*, derivanti dall'inquadramento giurisprudenziale di queste attività come attività "atipiche" di ricerca della prova: è giunto il momento, di "*valorizzare, nel settore delle indagini digitali, il principio di proporzionalità quale parametro di legittimità per le attività investigative*" (Marafioti, 2023), ciò che oggi non è, se, come sovente accade, è dato sequestrare uno *smartphone* o altro dispositivo analogo con provvedimento adottabile procedendo per qualsivoglia reato: in ipotesi, anche per semplici contravvenzioni ovvero comunque per delitti di scarsa gravità. In pratica, si tratta di innalzare il valore del principio di libertà di comunicazione prevedendo l'intervento del Giudice e l'introduzione di rigorose condizioni di proporzionalità ed adeguatezza dell'agire investigativo, così legando l'esercizio del potere di acquisizione dei dati personali a rigidi presupposti, definiti da adeguati limiti edittali e da altre tassative specificazioni e, non ultimo, a più rigorosi e perciò controllabili

oneri motivazionali; soprattutto, è necessario prevedere che i dati siano trattati come quelli delle intercettazioni, confluendo nell'Archivio delle Intercettazioni: soltanto così i dati irrilevanti a fini di giustizia potranno restare segregati e sfuggire ad ogni diffusione sterminatrice della reputazione, dell'onore e della vita delle persone.

Vi sono altri temi di complessità e delicatezza tali da imporre *la necessità d un intervento immediato del legislatore e per tale via limitare la discrezionalità giudiziaria correlata a clausole generali che abbisognano di essere sostituite da rigorose e tassative prescrizioni legali*: in generale, è istituzionalmente pericoloso che tali temi siano affidati al giudice al di fuori di una rigorosamente delimitata griglia normativa: non solo per la precarietà e la possibile difformità delle pronunce, ma perché, valendo ogni *revirement* o comunque nuovo indirizzo interpretativo a creare instabilità e pratica crisi della prevedibilità e della stessa comprensibilità della giurisdizione, si introduce ogni volta il rischio di travolgimento di esiti processuali non definitivi, ma legittimamente formati su indirizzi della giurisprudenza di legittimità tanto consolidati da costituire diritto vivente: i rischi più alti li vedo per le stesse indagini di mafia e di terrorismo in relazione alle oscillazioni giurisprudenziali che ormai segnano, nonostante plurimi interventi delle Sezioni Unite della Cassazione, l'interpretazione del concetto di "criminalità organizzata" di cui all'art. 13 del d.l. 152/1991, sul quale posano i pilastri di un regime differenziato delle intercettazioni per i delitti di mafia e terrorismo che mi pare che nessuno possa contestare nella sua perdurante necessità e nella sua stessa giustificazione razionale; bene, dinanzi a pronunce, per quanto isolate, che, stravolgendo gli indirizzi dati dalle Sezioni Unite, affermano che sarebbero delitti di criminalità organizzata soltanto quelli associativi, così giungendo alla conclusione, contraria persino al senso comune, che un omicidio di mafia non sarebbe un delitto di criminalità organizzata; si staglia così tutta la responsabilità politica del legislatore di definire esattamente i contorni e i limiti di tale nozione: al vantaggio della chiarezza delle scelte politiche si assocerà quello della salvaguardia delle vicende processuali in corso; è questo un tema che attualmente agisce come fattore di destabilizzazione di tutte le indagini e di tutti i processi di mafia non ancora giunti alla definitiva conclusione, anche con riferimento all'analoga clausola legale che definisce l'ambito di applicazione della disciplina della sospensione feriale dei termini processuali: al momento, tale tema ha formato oggetto di una mia preoccupata missiva diretta al Procuratore generale della Corte di Cassazione, nella quale ho potuto esprimere soltanto, in uno all'allarme condiviso dai Procuratori distrettuali, l'auspicio di un urgente, nuovo intervento delle Sezioni Unite. Ma, intanto, ancora nei giorni scorsi, cadono nel nulla processi costruiti pazientemente sulla base di orientamenti dalla giurisprudenza di legittimità della stabilità dei quali sembrava potersi confidare.

Naturalmente, al piano dell'innalzamento delle garanzie attiene anche la questione della ulteriore delimitazione dell'impiego di alcune delle tecniche di indagine più invasive, come

quelle legate all'impiego a fini di captazione del cd. *trojan*, vale a dire le *intercettazioni telematiche mediante captatore informatico*; si tratta di un tema sul quale il mio Ufficio è pronto ad offrire ogni doveroso e opportuno contributo informativo, ma che di per sé è oggetto di una responsabilità tipicamente politica, come tale esclusiva del legislatore e delle forze politiche che concorrono a determinarne l'esercizio. Quale Procuratore nazionale antimafia e antiterrorismo, tuttavia, avverto la responsabilità di porre a disposizione delle valutazioni del Parlamento i dati di una ormai vasta e consolidata esperienza, i quali dimostrano, senza tema di smentita, che l'efficacia reale dell'azione di contrasto della criminalità mafiosa dipende largamente dalla capacità di proiettare le indagini sui versanti nei quali operano le sue componenti più sofisticate e pericolose, perché deputate ai processi di reinvestimento speculativo, di condizionamento delle pubbliche amministrazioni (basta al riguardo riferirsi alle valutazioni governative che sono state alla base dello scioglimento degli organi elettivi di amministrazioni anche di grande importanza sociale) e di penetrazione profonda dei mercati d'impresa, a partire da quelli sui quali si riversano i maggiori flussi della spesa pubblica. Tali processi sono affidati non a uomini con la coppola sul capo e la lupara in spalla, ma al linguaggio, largamente praticato dal mercato e nel mercato, della frode fiscale e, soprattutto, della corruzione. Molte ed anche importanti indagini di mafia, soprattutto, ma non solo, nelle regioni centro-settentrionali, sono originate da indagini avviate sul fronte del contrasto della corruzione e delle frodi fiscali; escluderle dal novero di quelle per le quali quelle tecniche investigative sono consentite sarebbe dunque scelta legittima, ma destinata ad avere conseguenze pesantissime, non solo sul versante del contrasto della corruzione, ma anche sul terreno delle indagini di mafia. Come pure appartiene alla responsabilità esclusiva del legislatore la scelta del tempo di tale eventuale scelta, coincidente con l'attuazione di processi di spesa pubblica finanziati con risorse euro-unitarie, generate, almeno in parte, dalla tassazione di cittadini ed imprese di altri Paesi dell'Unione Europa, per presidiare l'uso delle quali l'Unione agisce anche in ambito investigativo e giudiziario attraverso l'Ufficio del Procuratore Europeo. Non spetta ad un magistrato pronunciarsi al riguardo, ma vorrei, anche in questa autorevolissima sede, ricordare le parole pronunciate dal Presidente Draghi nella sala dedicata a Giovanni Falcone della DNA nel settembre scorso, invitandoci a considerare quale disastroso effetto avrebbe sulla credibilità dell'Italia la mera diffusione della percezione che una significativa parte di quelle risorse possano finire nelle mani delle mafie e nei mille rivoli di fenomeni corruttivi che certo non sono estranei alla spiegazione del dato statistico che rivela che il 70 per cento delle opere pubbliche incompiute si trovano nelle regioni meridionali. In ogni caso, vale forse la pena di sottolineare che nel 2019 non si realizzò l'introduzione dell'uso del *trojan* per i delitti contro la p.a., già consentito dalla riforma del 2017 per tutti i delitti che consentono il ricorso alle intercettazioni, ma soltanto l'equiparazione dei delitti di corruzione *et similia* ai delitti di criminalità organizzata e terrorismo ai limitati fini, oltre

che dell'estensione degli ambiti di privata dimora considerati prescindendo dal loro utilizzo a fini criminosi, dell'esclusione dell'obbligo del Giudice di indicare, all'atto dell'autorizzazione, non soltanto le ragioni che rendono necessaria quella invasiva modalità di captazione, ma anche "i luoghi e il tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono" (art. 267, comma 1, c.p.p.): una clausola che nell'esperienza pratica si risolve nella pretesa di esercizi di chiromanzia che contrastano con la realtà delle investigazioni e la stessa possibilità di predisporre dettagliati piani previsionali e nella conseguente generazione di controversie e polemiche intorno ai limiti di quelle predizioni, tanto più considerando che, dopo tutto, quando si ricorre al captatore, lo si fa partendo dal dimostrato presupposto che non sia dato individuare preventivamente i luoghi e i tempi di una determinata condotta. Ma conviene ricordare, poiché nel dibattito pubblico sembra affacciarsi l'idea che le intercettazioni siano disposte ad ogni passo di un qualsiasi pubblico ufficiale, che per i delitti di criminalità organizzata soltanto la soglia di accesso a queste tecniche di intercettazione è data dalla sussistenza di *sufficienti indizi*, per tutti gli altri casi, compresi quelli in tema di corruzione, essendo invece necessaria la dimostrazione dell'esistenza di *gravi indizi* di reità.

Le ragioni di rivisitazione normativa non si esauriscono lungo quei pur fondamentali tracciati argomentativi: vi è una grave ed evidente carenza di garanzia legale di fondamentali istanze di rafforzata tutela della segretezza dei contenuti delle intercettazioni nelle prassi operative: in alcuni uffici esistono già disposizioni organizzative e direttive alla polizia giudiziaria che impongono, ad esempio, di attestare la distruzione di ogni copia di lavoro di file audio e trascrizioni una volta scaduto il termine dato dalla legge per procedere all'elaborazione investigativa del materiale raccolto ovvero anche il divieto di inserire nei *data base* delle forze di polizia i contenuti delle intercettazioni prima e indipendentemente dalla cristallizzazione del materiale utilizzabile e rilevante da quello che tale non è che si realizza al momento dell'esercizio dell'azione cautelare o della richiesta di giudizio, ovvero ancora il dovere di traduttori, interpreti e consulenti trascrittori di attestare di non conservare alcuna copia dei dati cui hanno avuto accesso per ragioni del loro ufficio di ausiliari; sono scelte rivelatesi importanti nella prevenzione degli abusi del passato, ma che sarebbe necessario elevare di rango precettivo, assicurandone l'uniforme applicazione. Va, in altri termini, sancita la necessità di ancoraggio a precisi canoni normativi del trattamento di informazioni e dati così delicati: ad esempio, prevedendo un divieto generale di conservazione da parte di chiunque vi abbia avuto accesso di dati diversi da quelli che possono legittimamente ritenersi rilevanti e utilizzabili; una materia delicata, che non consente però il trascinamento di prassi insensibili alle istanze di tracciabilità e controllo delle attività investigative che hanno a che fare con dati segreti, a cominciare dall'impiego di tecniche codificate di raccolta e conservazione di atti e documenti informatici; i dati segreti vanno trattati come tali, soprattutto se si prevede che

quelli non rilevanti a fini di giustizia, ma intanto acquisiti agli atti, sia destinati restare tali: il loro trattamento esige dunque precise garanzie di trattamento, conservazione e tracciabilità; si tratta di un aspetto importante, che vale a rimarcare con nettezza la distinzione fra la libertà di informazione, che può giungere persino oltre il confine del segreto, e il dovere dei pubblici ufficiali di preservare il segreto, osservando regole e protocolli assai più rigidi di quelli oggi praticati.

È parimenti necessario, al medesimo fine, che una norma legale imponga all'amministrazione della giustizia di assicurare la tracciabilità di tutti gli interventi, anche di mero accesso, ai dati delle intercettazioni conservati nell'Archivio delle intercettazioni: scelta tanto più necessaria fino a quando le infrastrutture fondamentali – le sale *server* - non saranno consolidate e trasferite nella sfera di controllo dello Stato: le tecnologie consentono già ora di farlo, con riferimento ai server privati dei fornitori collegati all'A.D.I., ma, in mancanza di una prescrizione legislativa che ne faccia una priorità, il dispiegamento dei *software* a ciò necessari finisce inevitabilmente in coda alla lista delle cose da fare delle strutture ministeriali; ma è cosa che non tollera approssimazioni e ritardi, come quelli già sopra indicati; tocca al Ministero colmare al più presto il vuoto di iniziative su questo decisivo terreno, ma il Parlamento può aiutare il Ministro e il Ministero a realizzare questo passaggio, prescrivendone la doverosità e dettandone i tempi.

La tensione sui profili di sicurezza collettiva e della stessa funzione di sicurezza della Repubblica, che pure si avvale dei medesimi servizi, conseguente alla continua tensione dei nuovi prodotti e delle nuove strategie commerciali con i principi alla base della definizione normativa di prestazioni obbligatorie da assicurare a fini di giustizia e di sicurezza: materia delicatissima, come ovvio. Ma segnata da due distinte e fra loro concorrenti urgenze di regolazione legislativa:

la prima è generata dalla decisione della Grande Sezione della Corte UE del 20 settembre 2022, in materia di presupposti e condizioni di conservazione dei dati di traffico telefonico e telematico. L'interpretazione della Corte integra la disciplina data dalla Direttiva 58/2002, relativa alla vita privata e alle comunicazioni elettroniche, distinguendo le possibilità di conservazione dei dati che nei sistemi nazionali possono essere introdotte con provvedimenti normativi, a seconda della natura e del diverso valore degli obiettivi delle misure legislative. La Corte costruisce quindi una gerarchia delle esigenze che possono giustificare una conservazione ampia dei metadati delle comunicazioni (quelli cioè destinati a confluire nei cd. tabulati, che altra decisione della Corte UE ha imposto di riservare al Giudice), a seconda che si tratti di "*salvaguardia della sicurezza nazionale*" ovvero di esigenze di "*prevenzione, ricerca, accertamento e perseguimento dei reati e... della sicurezza pubblica*": nel primo caso soltanto, in forza di un necessario principio di proporzionalità, sarebbe possibile introdurre o conservare un obbligo di conservazione generalizzato e indiscriminato di

quei metadati. Questa la decisione, ma l'adattamento normativo nel sistema italiano non può non tener conto del fatto che criminalità mafiosa e terroristica partecipano a pieno titolo alla definizione di minacce alla sicurezza nazionale; lo comprova, oltre alla constatazione della realtà derivante dalla storia recente del nostro Paese, la circostanza che criminalità organizzata e terrorismo sono anche, secondo la legge italiana (e sin dal d.l. 345/1991), minacce alla sicurezza della Repubblica, come tali corrispondenti a specifiche finalità preventiva delle agenzie di *intelligence*; appare cruciale, dunque, nel valutare l'impatto della giurisprudenza della Corte di Lussemburgo, tenere al riparo il contrasto della criminalità organizzata e del terrorismo, da una ridefinizione degli obblighi di conservazione che varrebbe a minare la sicurezza nazionale, tanto più nel momento nel quale la pericolosità del crimine organizzato mafioso e del terrorismo si salda alle spinte minacciose che su questi versanti muovono dai teatri di guerra e di destabilizzazione;

secondo punto: ogni giorno entrano in gioco *software* e tecniche commerciali che rischiano di vanificare o ostacolare seriamente quella finalità di prevenzione, tanto della sicurezza nazionale che della sicurezza pubblica e della correlata esigenza di prevenzione e perseguimento dei reati: la riservatezza è giustamente un *atout* commerciale ed anche dunque un fattore di concorrenza, ma gli obblighi in tema di prestazioni obbligatorie valgono a costruire una cornice di compatibilità con i valori della sicurezza: ogni volta si produce la necessità di una verifica tecnica attenta: un settore questo nel quale la DNA, con l'essenziale partecipazione dei servizi centrali di polizia, agisce come interlocutore naturale tanto delle imprese quanto dei ministeri interessati, ma del quale sarebbe necessario un coordinamento costante e unitario, che non può che essere della Presidenza del Consiglio dei Ministri, le attribuzioni della quale sono peraltro direttamente coinvolte, sia dal punto di vista del ruolo della nuova Agenzia per la cybersicurezza sia da quello delle prerogative del sistema di *intelligence* che per le sue attività ricorre alle medesime tecnologie: un tema urgente anche questo, non solo nella prospettiva della riscrittura già in corso di molte delle norme del codice delle telecomunicazioni, ma anche e soprattutto in quella del raccordo operativo di funzioni statuali di amministrazione attiva che ancora sfuggono alla logica propria soltanto di una visione unitaria ed organica di una così delicata materia.

---

[1] L'articolo 706-102-1 del codice di procedura penale, nella sua formulazione risultante dalla legge 23 marzo 2019, dispone: "*Si può ricorrere all'attuazione di un dispositivo tecnico il cui scopo, senza il consenso degli interessati, è quello di accedere, ovunque, a dati informatici, di registrarli,*

archiviarli e trasmetterli, in quanto conservati in un sistema informatico, come vengono visualizzati su uno schermo dall'utente di un sistema automatizzato di elaborazione dati, poiché li introduce inserendo dei caratteri o mentre vengono ricevuti e inviati dalle periferiche.

"Il pubblico ministero o il giudice istruttore può designare qualsiasi persona fisica o giuridica autorizzata ed iscritta in uno degli elenchi previsti dall'articolo 157, al fine di compiere le operazioni tecniche che consentano la realizzazione del dispositivo tecnico di cui al primo comma di questo articolo. Il Pubblico Ministero o il Giudice Istruttore possono altresì prescrivere l'utilizzo di risorse dello Stato soggette al segreto di difesa nazionale nelle forme previste dal Capo I del Titolo IV del Libro I".