L'ARCHIVIO DELLE INTERCETTAZIONI. LA CUSTODIA DEL MATERIALE E LA MARCIA VERSO LA DIGITALIZZAZIONE DELLE INFORMAZIONI

di Silvia Signorato
(*Ricercatore di diritto processuale penale, Università di Padova*)

SOMMARIO: 1. Tappe del percorso. – 2. Registro riservato delle intercettazioni ed archivio delle intercettazioni: due strumenti diversi. – 3. Le tre articolazioni dell'archivio delle intercettazioni: archivio riservato TIAP, archivio documentale ed archivio digitale. - 4. Captazione e registrazione, conferimento e deposito. – 5. I soggetti dell'archivio, tra chi lo dirige, lo sorveglia e chi vi accede. – 6. Misure di sicurezza a tutela del diritto alla riservatezza delle comunicazioni e alla protezione dei dati personali. - 7. La distruzione della documentazione a seguito di richiesta dell'interessato e la distruzione delle registrazioni per decorso del tempo. – 8. Conclusioni.

1. La disciplina prevista dall'art. 269 del codice di rito del 1988 si limitava a prevedere che i verbali e le registrazioni delle intercettazioni venissero conservati in forma integrale presso il pubblico ministero che aveva disposto l'intercettazione.

Tuttavia, lo scenario muta a partire dal 2017, con una disciplina peraltro soggetta a successive modifiche e plurimi differimenti applicativi, tanto da divenire applicabile ai soli procedimenti penali iscritti dopo il 31 agosto 2020[1].

Il percorso di riforma è quindi scandito in più tappe[2].

Il punto di partenza è rappresentato dal d.lgs. 29.12.2017 n. 216 (cd. riforma Orlando), che delinea un nuovo assetto[3] in materia di intercettazioni di conversazioni o di comunicazioni, disciplinando, tra l'altro, uno strumento dalla denominazione

[1] Come sottolineato da L. Giordano, *L'archivio delle intercettazioni*, in *Il Processo telematico*, 1° agosto 2020, § 2 è stato prevista «una sorta di "doppio binario" quanto alla disciplina del mezzo di ricerca della prova perché, per i procedimenti iscritti fino al 31 agosto 2020, continuerà ad essere applicabile la disciplina previgente».

[2] Il generale quadro di riferimento in tema di intercettazioni viene definito un «cantiere aperto» da M.L. Di Bitonto, *Lungo la strada per la riforma della disciplina delle intercettazioni*, in *CP* 2008, 8.

[3] Cfr. la *Relazione tecnica*, 2017, 3, visualizzabile in http://documenti.camera.it/apps/nuovosito/attigoverno/Schedalavori/getTesto.ashx?file=0472_F002.pdf&leg=XVII#pagemode=none

evocativa: l'«archivio riservato»[4] delle intercettazioni. Il rinnovato quadro sembra però determinare una sorta di «"reazione immunitaria" generalizzata»[5].

Di qui il d.l. 30.12.2019 n. 161, che apporta modifiche urgenti alla disciplina delle intercettazioni di conversazioni o comunicazioni. I cambiamenti involgono anche le previsioni in tema di archivio, che vengono rimodellate a partire dalla denominazione: non più «archivio *riservato*»[6], ma «archivio» *tout court* (nel codice di rito) e «archivio *digitale*» (nelle norme di attuazione).

La disciplina tocca però nervi sensibili e sembra non avere quiete. Ne deriva che il decreto legge viene convertito con significative modifiche dalla l. 28.2.2020 n. 7[7]. Ancora una volta viene rimodulata pure la disciplina dell'archivio delle intercettazioni.

Nel frattempo, in ragione del forte impatto applicativo dello strumento, si avverte la necessità di indicazioni anche marcatamente pratico-operative. Per soddisfare questa esigenza vengono emanati ulteriori atti: da un lato, il d.m. 20.4.2018 del Ministero della Giustizia in tema di accesso all'archivio [8]; dall'altro, il provvedimento del 5.12.2019 del Direttore generale dei servizi informativi automatizzati di adozione delle specifiche tecniche per il conferimento nell'archivio delle intercettazioni[9], le cui disposizioni hanno cessato di avere efficacia a seguito dell'ulteriore Provvedimento del Direttore Generale dei Servizi Informativi Automatizzati datato 1° luglio 2020[10].

Dal canto suo, la magistratura si attiva meritoriamente per fornire indicazioni in rapporto al d.l. 161/2019, così come convertito dalla l. 7/2020: in questa cornice si

---

[4] Come sottolineato da A. Camon, *Forme, destinazione e regime della documentazione*, in *Nuove norme in materia di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche,* a cura di G. Giostra - R. Orlandi, Torino 2018, 79 «è il fiore all'occhiello della riforma, un traguardo che veniva inseguito da almeno vent'anni. Il legislatore individua meticolosamente il materiale che vi viene custodito, staccandosi sia dai primi abbozzi di vecchi progetti sia dalla legge delega».

[5] In questi termini, cfr. M. Gialuz, *Premessa,* in *Dinternet* 2020 (3, supplemento), 3, il quale precisa come tale reazione si sia realizzata «ben al di là degli effettivi demeriti».

[6] Reputa che «l'espulsione del termine» «riservato» sia «*sine causa*» A. Scalfati, *Intercettazioni: spirito autoritario, propaganda e norme inutili*, in *www.archiviopenale.it* 2020, 3.

[7] Critica il risultato normativo F. Caprioli, *La procedura di filtro delle comunicazioni nella legge di riforma della disciplina delle intercettazioni*, in *CP* 2020, 1385, secondo il quale l'attuale assetto sarebbe «di gran lunga peggiore del precedente: un picassiano *collage* di vecchie e nuove regole (l'originaria screditatissima disciplina codicistica e la "circolare Spataro") il cui risultato è comprimere bruscamente gli spazi di tutela riservati alle vittime dell'intercettazione».

[8] Nello specifico, il decreto reca disposizioni di attuazione per le intercettazioni mediante inserimento del captatore informatico e per l'accesso all'archivio informatico a norma dell'art. 7 co. 1 e 3 d.lgs. 29.12.2017 n. 216.

[9] Cfr. Ministero della Giustizia, Dipartimento dell'Organizzazione Giudiziaria del Personale e dei Servizi, Direzione Generale per i Sistemi Informativi Automatizzati, provvedimento 5.12.2019, prot. m.: DoG07.05/12/2019.0015228.ID

[10] V. Ministero della Giustizia, Dipartimento dell'Organizzazione Giudiziaria del Personale e dei Servizi, Direzione Generale per i Sistemi Informativi Automatizzati, provvedimento 1° luglio 2020, art. 4 (Efficacia), m_dg.DOG07.01/07/2020.0007327.ID

collocano, ad esempio, la «Relazione su novità normative» della Corte Suprema di Cassazione[11], le direttive fornite in materia di intercettazioni dalle Procure della Repubblica[12], nonché guide pratiche come quella curata dall'Ufficio per l'innovazione del distretto di Napoli[13].

Ne esce un quadro composito ed articolato in cui fonti di vario livello si compendiano con la prassi, in una dinamica di «accentuato pluralismo e policentrismo giuridico»[14].

2. Il processo civile telematico (PCT) e il processo tributario telematico (PTT) sono da tempo una realtà.

Nel delicatissimo ambito del processo penale si è invece assistito a una maggiore resistenza all'ingresso della tecnologia, comunque penetrata, ad esempio, in riferimento alle notifiche e ai sistemi informatici utilizzati dagli uffici.

Aperta la strada verso la digitalizzazione, il legislatore la percorre. Le disposizioni in materia di archivio intendono infatti attuare un'anticipazione del

[11] Ufficio del Massimario e del ruolo, Sevizio Penale, Rel. 35/20, 23.3.2020.

[12] Al riguardo cfr., *ex multis*, Procura della Repubblica presso il Tribunale ordinario di Milano, *Direttiva in materia di intercettazioni (d.l. 30.12.2019)*, 6.7.2020, prot. n. 163/20; Procura della Repubblica, Direzione distrettuale antimafia, Reggio Calabria, 27.7.2020, provv. n. 37/2020; Procura della Repubblica presso il Tribunale di Torino, *Direttiva in tema di nuova disciplina delle intercettazioni,* 31.7.2020, prot. 3144/20/S.P (al riguardo, cfr. C. Parodi, *La nuova disciplina delle intercettazioni: le indicazioni operative della Procura della Repubblica di Torino*, in *ilProcessoTelematico*, 7.9.2020); Procura della Repubblica presso il Tribunale di Avellino, 23.7.2020, O.d.S. nr. 96/U/2020; Procura Generale della Corte di Cassazione, *Primi orientamenti in tema di applicazione della nuova disciplina delle intercettazioni di conversazioni o comunicazioni,* 31.7.2020, prot. 16926/20/uai/int-spart; Tribunale ordinario di Benevento, 3.8.2020, decreto n. 114; Procura della Repubblica presso il Tribunale di Campobasso, 7.8.2020, prot. n. 3016/2020/U; Procura della Repubblica presso il Tribunale di Livorno, 20.8.2020, prot. n. 3385/2020; Procura della Repubblica presso il Tribunale di Bologna, 24.8.2020, prot. 25.8.2020 n. int. 356; Procura della Repubblica presso il Tribunale di Enna, 25.8.2020, prot. 3445/2020; Procura della Repubblica presso il Tribunale di Tivoli, 27.8.2020, prot. n. 1324/2020; Procura della Repubblica presso il Tribunale di Reggio Emilia, ordine di servizio n. 32/2020; Procura della Repubblica presso il Tribunale di Cuneo, 28.8.2020, prot. 2446/2020 e 31.8.2020, prot. 2445/2020; Procura della Repubblica presso il Tribunale di Mantova, 31/8/2020, direttiva n.2/2020; Procura della Repubblica presso il Tribunale di Foggia, 1.9.2020, provv. 110/202; Procura distrettuale della Repubblica di Brescia, 1.9.2020, direttiva prot. n. 1590/2020; Procura della Repubblica presso il Tribunale ordinario di Venezia, linee guida 1.9.2020; Procura della Repubblica presso il Tribunale per i minorenni di Catania, 11.9.2020, prot. 863/2020; Procura della Repubblica presso il Tribunale di Perugia, 30.9.2020, prot. n. 4592/2020.

[13] Il riferimento è alla *Guida pratica ad una prima lettura tecnologica e normativa della legge 28 febbraio 2020, n. 7 e del decreto legge 30 aprile 2020, n. 28 (Modifiche alla disciplina delle intercettazioni di conversazioni o comunicazioni) alla luce della circolare n. 9/2020 del Procuratore della Repubblica di Napoli*, a cura dell'Ufficio per l'innovazione del distretto di Napoli (R. Patscot-Rid requirente; R. Marro-Rid giudicante), Struttura permanente di riferimento del CSM per l'innovazione, 6.8.2020.

[14] Così, R.E. Kostoris, *Manuale di procedura penale europea*[4], Milano 2019, 70 che peraltro impiega la locuzione in rapporto allo scenario europeo, caratterizzato «da un assetto delle fonti ben lontano dal tradizionale modello gerarchico-piramidale di matrice kelseniana».

processo di digitalizzazione della giustizia penale[15], a cui è stato dato un significativo impulso nell'ambito delle misure urgenti di contrasto a *covid*-19[16].

Per comprendere che cosa sia l'archivio, sembra opportuno sgombrare preliminarmente il campo da un equivoco di fondo che talora aleggia in materia. Il riferimento è alla indebita sovrapposizione dei concetti di archivio delle intercettazioni e di registro riservato delle intercettazioni *ex* art. 267 co. 5 Cpp. Si tratta infatti di due nozioni distinte, espressive di strumenti dalle funzioni diverse.

Sin dalla sua originaria formulazione codicistica, l'art. 267 co. 5 Cpp prevedeva che nell'ufficio del pubblico ministero fosse tenuto un apposito registro riservato (cd. modello 37)[17] in cui annotare[18], secondo un ordine cronologico, i decreti che

[15] In questo senso, cfr. Senato della Repubblica, XVIII Legislatura, 1.2.2 Testo correlato 1659 (*errata corrige*), p. 30.

[16] L'art. 83 co. 12 *quater*.1 d.l. 17.3.2020 n. 18, recante misure di potenziamento del servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da *COVID*-19, ha infatti previsto che «con uno o più decreti del Ministro della giustizia non aventi natura regolamentare, presso ciascun ufficio del pubblico ministero che ne faccia richiesta a norma del terzo periodo, è autorizzato il deposito con modalità telematica di memorie, documenti, richieste e istanze indicate dall'art. 415-*bis* co. 3 Cpp, secondo le disposizioni stabilite con provvedimento del Direttore generale dei sistemi informativi e automatizzati del Ministero della giustizia, anche in deroga alle previsioni del decreto emanato ai sensi dell'art. 4 co. 1 d.l. 29.12.2009, n. 193, convertito, con modificazioni, dalla l. 22.2.2010 n. 24. Il deposito degli atti si intende eseguito al momento del rilascio della ricevuta di accettazione da parte dei sistemi ministeriali, secondo le modalità stabilite dal provvedimento direttoriale di cui al primo periodo. I decreti di cui al primo periodo sono adottati su richiesta degli uffici del pubblico ministero, previo accertamento da parte del Direttore generale dei sistemi informativi e automatizzati del Ministero della giustizia della funzionalità dei servizi di comunicazione dei documenti informatici». A tale previsione hanno fatto seguito il Provvedimento 11.5.2020 n. 5477 del Direttore Generale dei sistemi Informativi Automatizzati del Ministero della Giustizia e il d.m. 9.6.2020 per la Procura della Repubblica presso il Tribunale di Napoli; il d.m. 17.6.2020 per la Procura della Repubblica presso il Tribunale di Perugia; il d.m. 17.6.2020 per la Procura della Repubblica presso il Tribunale di Catania; il d.m. 30.9.2020 per la Procura della Repubblica presso il Tribunale di Brescia; il d.m. 14.10.2020 per la Procura della Repubblica presso il Tribunale di Firenze; il d.m. 14.10.2020 per la Procura della Repubblica presso il Tribunale di Bari; il d.m. 14.10.2020 per la Procura della Repubblica presso il Tribunale di Ancona; il d.m. 14.10.2020 per la Procura della Repubblica presso il Tribunale di Salerno. Da ultimo, si veda inoltre l'art. 24 d.l. 28.10. 2020 n. 137 (Disposizioni per la semplificazione delle attività di deposito di atti, documenti e istanze nella vigenza dell'emergenza epidemiologica da COVID-19). In tema, cfr. Pubblicazione informativa a cura dell'ufficio per l'innovazione del Distretto di Napoli Struttura permanente di riferimento del CSM per l'innovazione (R. Patscot-Rid requirente; R. Marro-Rid giudicante), *Guida al Portale di Deposito atti penali (PDP)*, 31.10.2020.

[17] Tale registro denominato modello 37 è tenuto in tutti gli Uffici di Procura della Repubblica, nonché presso le Procure generali. Dal canto suo, il d.m. 23.3.2000 n. 264 (regolamento recante norme per la tenuta dei registri presso gli uffici giudiziari) ha previsto che il registro, prima dell'uso, venga numerato e vidimato in ogni mezzo foglio dal dirigente della cancelleria o della segreteria dell'ufficio o da persona da lui delegata. In aggiunta, è stato precisato che l'eventuale tenuta del registro in modalità informatica deve avvenire secondo regole tecniche e procedurali volte ad assicurare l'integrità, la disponibilità e la riservatezza dei dati, prevedendo anche l'identificazione del soggetto che accede ad essi (art. 4 co. 1).

[18] In tema di conseguenze processuali della ritardata registrazione nel modello 37 del provvedimento autorizzativo delle intercettazioni, cfr. Cass. 24.9.2003 n. 44518 in *GD* 2004 (8), 82 secondo la quale, in una simile ipotesi, non sarebbe ravvisabile alcuna invalidità *ex* art. 177 Cpp in ragione del principio di tassatività delle nullità.

dispongono, autorizzano, convalidano o prorogano le intercettazioni e, per ciascuna intercettazione, l'inizio e il termine delle operazioni. Un simile registro è spesso tenuto in forma cartacea. Essendo rimasto invariato nel tempo, esso risulta in parte anacronistico, ad esempio, in rapporto alle voci da compilare, che non tengono conto della mutata realtà tecnologica e delle attuali necessità. Per questo motivo, previa autorizzazione ministeriale, vari uffici sono ricorsi a registri telematici[19]. Dal canto suo, il d.l. 161/2019, da un lato, ha specificamente precisato che tale registro è gestito «anche con modalità informatica»; dall'altro, ha stabilito che la gestione e la tenuta del registro riservato avvenga sotto la direzione e la sorveglianza del Procuratore della Repubblica.

Uno strumento diverso dal registro riservato è invece l'archivio delle intercettazioni, la cui disciplina non sembra corredata da alcuna sanzione di inutilizzabilità per l'ipotesi di sua violazione[20].

L'archivio delle intercettazioni è stato istituito per dare attuazione al provvedimento datato 18.7.2013 del Garante per la protezione dei dati personali[21]. Quest'ultimo provvedimento era stato emesso a seguito di riscontri del Garante, i quali avevano mostrato come le Procure adottassero delle misure variegate in rapporto alla protezione dei dati personali e dei sistemi di gestione di tali dati. La profonda incidenza sul piano dei diritti fondamentali che può derivare dal trattamento di dati nell'ambito delle intercettazioni, il mutato contesto tecnologico che aggrava i rischi connessi a tale trattamento, nonché l'esigenza di adottare misure in materia di protezione dei dati personali tendenzialmente uniformi tra le Procure aveva indotto il Garante a prescrivere l'adozione di una serie di misure ed accorgimenti finalizzati a rafforzare il controllo preventivo e la sicurezza nel trattamento dei dati personali e dei sistemi nell'attività di intercettazione di conversazioni o comunicazioni elettroniche, anche informatiche o telematiche.

3. Tendenzialmente, il dibattito dottrinale sull'archivio si incentra sullo strumento in generale, sulla sua disciplina, sulle problematiche che ne derivano anche in rapporto alla tutela dei diritti fondamentali, senza addentrarsi nell'analisi della struttura concreta. Quest'ultimo profilo sembra invece importante perché la sua conoscenza rende più agevole la comprensione e l'interpretazione delle norme,

[19] T. De Giovanni, *Il registro delle intercettazioni: evoluzione storica e ritardi dell'informatizzazione*, in *Sicurezza Giustizia*, II, MMXVII, 27 ss. precisa come simili registri vengano concessi in comodato d'uso gratuito dalle società private che forniscono i sistemi informatici relativi alle intercettazioni.

[20] Per questa impostazione, cfr. Corte Suprema di Cassazione, Ufficio del Massimario e del ruolo, Sevizio Penale, cit., 53 ove si precisa che la disciplina *de qua* non afferisce all'ambito di utilizzabilità delle intercettazioni, ma a quello della tutela dei dati, in tutte le sue declinazioni.

[21] Cfr. Garante per la protezione dei dati personali, *Provvedimento in materia di misure di sicurezza nelle attività di intercettazione da parte delle Procure della Repubblica*, 18.7.2013 n. 356.

aiutando a cogliere aspetti che rischiano altrimenti di rimanere in ombra, pur potendo determinare ricadute di carattere anche sistematico.

Per questo motivo, pare opportuno ricordare come, da un punto di vista pratico, l'archivio delle intercettazioni si declini in tre componenti: archivio riservato TIAP, archivio documentale, archivio digitale delle intercettazioni[22]. Occorre soffermarsi distintamente su ciascuna articolazione.

a) Iniziando dall'archivio riservato TIAP[23] si può precisare come l'acronimo TIAP significhi Trattamento Informatico Atti Processuali. Nello specifico, TIAP è un applicativo informatico[24], che è stato sviluppato dal Ministero della Giustizia con l'obiettivo di pervenire ad una gestione digitale dei fascicoli, idonea ad implementarne il contenuto in rapporto alle varie fasi processuali, mediante atti, documenti e supporti multimediali, al fine di semplificare la classificazione, la codifica, l'indicizzazione dei fascicoli e le attività sugli stessi, come la ricerca o la consultazione.

TIAP è attivo da anni in molte realtà. All'interno di esso è stato creato l'archivio riservato TIAP[25], che rappresenta lo spazio digitale in cui conservare la documentazione inerente alle intercettazioni.

Va sottolineato che la documentazione inserita in TIAP non è, allo stato, una documentazione nativa digitale. In altre parole, i documenti in esso inseriti esistono dapprima in forma cartacea e, poi, vengono scannerizzati ed inseriti in TIAP.

Con l'attuazione del processo penale telematico lo scenario è però destinato a mutare in quanto anche la formazione dei verbali e degli atti avverrà *ab origine* in modalità telematica. In prospettiva, le stesse richieste del pubblico ministero e le autorizzazioni del giudice per le indagini preliminari saranno effettuate digitalmente e sottoscritte con firma digitale[26]. Al riguardo, si sottolinea fin d'ora un aspetto che

[22] L'art. 2 lett. *b* del provvedimento datato 5.12.2019 del Direttore Generale dei servizi informativi automatizzati di adozione delle specifiche tecniche per il conferimento nell'archivio riservato delle intercettazioni di cui all'art. 269 co. 1 Cpp definisce l'«archivio riservato informatico» come «sistema informatico (*hardware e software*) che consente di conservare tutte le conversazioni e comunicazioni disposte nell'ambito del procedimento, nonché di classificarle, in conformità alla relativa disciplina procedimentale; il sistema rende altresì disponibili le funzioni di accesso e di ascolto delle conversazioni o comunicazioni registrate». Da ultimo, la denominazione «archivio riservato informatico» è stata sostituita con quella di «archivio digitale informatico» (cfr. art. 2 lett. *b* del provvedimento del Ministero della Giustizia, Dipartimento dell'Organizzazione Giudiziaria del Personale e dei Servizi, Direzione Generale per i Sistemi Informativi Automatizzati, 1° luglio 2020).

[23] Si può rilevare come nell' «archivio *riservato* TIAP» permanga l'aggettivo «riservato», che è stato invece eliminato dalla l. 28.2.2020 n. 7, nonostante apparisse efficace.

[24] In base alla circolare della Direzione generale per i sistemi informativi automatizzati (DGSIA) del 26.1.2016 TIAP rappresenta il gestore documentale unico nazionale.

[25] Nello specifico, l'archivio riservato si trova in TIAP-DOCUMENT@.

[26] Ai sensi dell'art. 1 lett. *s* Codice dell'amministrazione digitale, la firma digitale consiste in «un particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento

non dovrà essere sottovalutato e che andrà specificamente ed attentamente regolamentato. A differenza della firma tradizionale che, una volta apposta, permane sul documento, la firma digitale scade, con tutti i riverberi che una simile circostanza può determinare anche sul piano della validità degli atti.

b) Proprio perché, allo stato, la documentazione cartacea continua a sussistere è necessario che esista anche il cd. archivio documentale, che non è un archivio digitale, ma un tradizionale archivio in cui conservare il materiale cartaceo che riguarda le intercettazioni.

c) Infine, l'archivio digitale delle intercettazioni (ADI) coincide con i *server*[27] che custodiscono, dopo che il pubblico ministero li ha inseriti in esso (cd. conferimento), le registrazioni disposte nell'ambito del procedimento ed i verbali[28], i quali ultimi si caratterizzano per la pluralità delle informazioni che riportano[29]. In essi si rinvengono infatti la trascrizione, anche sommaria, del contenuto delle comunicazioni intercettate; gli estremi del decreto che ha disposto l'intercettazione; il giorno e l'ora

informatico o di un insieme di documenti informatici». Per un approfondimento del concetto di documento informatico si rinvia ad A. Vele, *Documento informatico (profili processuali penali)*, in *DigDPen*, Agg. X 2018, 139-148.

[27] Per condivisibili ragioni di sicurezza, le specifiche tecniche relative alla conservazione dei dati nell'archivio digitale delle intercettazioni sono documenti a circolazione limitata e pubblicati in un apposito sito riservato. Non è quindi noto se il legislatore abbia ammesso la possibilità che i dati vengano conservati all'interno di un *Cloud*. Si tratta di una questione delicatissima. Come evidenziato dal Garante per la protezione dei dati personali, *Segnalazione al Parlamento e al Governo sulla disciplina delle intercettazioni mediante captatore informatico*, 30.4.2019 [*doc-web* 9107773], 3, la «delocalizzazione dei *server* in territori non soggetti alla giurisdizione nazionale costituisce (…) un evidente *vulnus* non soltanto per la tutela dei diritti degli interessati, ma anche per la stessa efficacia e segretezza dell'azione investigativa». Ne consegue che se, per ipotesi, i dati dell'archivio fossero conservati in un *Cloud*, esigenze di tutela dei diritti fondamentali renderebbero del tutto auspicabile l'impiego di *Cloud* italiani con *server* ubicati in Italia. Non bisogna infatti dimenticare come Corte cost. 6.4.1973 n. 34 abbia chiarito che in tema di captazione delle conversazioni e delle comunicazioni occorre offrire «garanzie che attengono alla predisposizione anche materiale dei servizi tecnici necessari per le intercettazioni telefoniche, in modo che l'autorità giudiziaria possa esercitare anche di fatto il controllo necessario ad assicurare che si proceda alle intercettazioni autorizzate, solo a queste e solo nei limiti dell'autorizzazione». Appare quindi assai opportuno l'ancoraggio al territorio italiano contenuto nel d.l. 16.7.2020 n. 76 recante misure urgenti per la semplificazione e l'innovazione digitale. L'art. 35 di tale decreto sottolinea infatti come la Presidenza del Consiglio dei ministri «promuove lo sviluppo di un'infrastruttura ad alta affidabilità *localizzata sul territorio nazionale* per la razionalizzazione e il consolidamento dei Centri per l'elaborazione delle informazioni (CED) definiti al co. 2, destinata a *tutte* le pubbliche amministrazioni». L'auspicio è che la localizzazione sul territorio italiano venga attuata anche per i dati conservati nell'archivio.

[28] Cfr. art. 2 lett. *d* Provvedimento del Direttore Generale dei servizi informativi automatizzati di adozione delle specifiche tecniche per il conferimento nell'archivio riservato delle intercettazioni di cui all'art. 269 co. 1 Cpp, 5 dicembre 2019 (tale provvedimento ha perso efficacia a partire dal giorno della pubblicazione sul portale servizi telematici del Ministero della Giustizia e sul sito *web* del Ministero della Giustizia del Provvedimento del Ministero della Giustizia, Dipartimento dell'organizzazione giudiziaria del personale e dei servizi, Direzione generale per i sistemi informativi automatizzati, 1° luglio 2020).

[29] Cfr. art. 268 co. 2 Cpp e art. 89 co. 1 e 4 NAttCpp.

di inizio e di cessazione delle intercettazioni; la descrizione delle modalità con cui è stata effettuata la registrazione; i nominativi delle persone che hanno partecipato alle operazioni. In aggiunta, nel caso in cui non sia possibile il contestuale trasferimento dei dati intercettati, il verbale deve indicare le ragioni impeditive, la successione cronologica degli accadimenti captati e delle conversazioni intercettate. Ancora, nell'ipotesi di intercettazioni delle comunicazioni e conversazioni tra presenti effettuate mediante *trojan* inoculato in un dispositivo elettronico mobile, nel verbale sarà indicato anche il tipo di programma impiegato e, laddove possibile, anche i luoghi di svolgimento delle comunicazioni o conversazioni.

4. Come noto, le comunicazioni intercettate sono registrate [30]. Poiché nell'archivio sono custodite le registrazioni delle intercettazioni, di primo acchito, si potrebbe forse pensare che tali registrazioni siano in esso custodite sin dal momento della captazione. Non è così.

Le operazioni di captazione e registrazione vengono effettuate «esclusivamente»[31] mediante impianti installati presso la Procura della Repubblica. Tuttavia, tale regola è stata in parte sopraffatta dall'eccezione prevista dall'art. 268 co. 3 Cpp. Infatti, nel caso di insufficienza o inidoneità degli impianti e se esistono eccezionali ragioni di urgenza, con provvedimento motivato il pubblico ministero può disporre il compimento delle operazioni tramite impianti di pubblico servizio o in dotazione alla polizia giudiziaria. Le maglie si allargano ulteriormente per le intercettazioni di comunicazioni informatiche o telematiche, dato che il pubblico ministero può disporre che le operazioni avvengano anche mediante impianti appartenenti a privati[32].

Ne consegue che, inizialmente, le registrazioni non si trovano nell'archivio, ma devono essere successivamente riversate in esso. Tale attività si traduce nel cd. conferimento delle intercettazioni, che consiste nell'inserimento nell'archivio digitale delle registrazioni e dei verbali [33]. Il conferimento deve essere effettuato

[30] In rapporto alle problematiche che si possono ricollegare alla registrazione, cfr. Cass. S.U. 26.6.2008 n. 36359.

[31] Cfr. art. 268 co. 3 Cpp.

[32] Secondo G. Di Paolo, *Prova informatica (diritto processuale penale)*, in *ED, Annali VI,* 2013, 747, l'art. 268 co. 3-*bis* Cpp non rappresenta una deroga, ma integra una sorta di prosecuzione del comma precedente, con la conseguenza che «le eventuali omissioni di motivazione in ordine all'inadeguatezza degli impianti presso gli uffici della pubblica accusa non potranno che tradursi nell'inutilizzabilità dei risultati investigativi conseguiti». Sotto altro profilo, occorre ricordare come le intercettazioni comportino dei costi. Per una disamina sulle spese e sulla relativa normativa si rinvia a Camera dei Deputati, Servizio Studi, XVIII legislatura, *La riforma della disciplina delle intercettazioni*, 7.5.2020, 5. In tema, si può segnalare come tra le voci di spesa dei dati attinenti alle comunicazioni captate vengano annoverate quelle relative alla remunerazione degli operatori, al noleggio dei macchinari ed all'acquisizione dei tabulati telefonici (i quali ultimi, trattando dati esterni alle comunicazioni, non sono però soggetti alla disciplina delle intercettazioni, ma alla distinta previsione *ex* art. 132 codice *privacy*).

[33] In argomento, cfr. Procura della Repubblica presso il Tribunale ordinario di Milano, cit., 2. Come ricordato da

immediatamente[34], una volta che l'attività di intercettazione, di ascolto, di trascrizione e di redazione dei verbali riguardanti le comunicazioni rilevanti è terminata. Il legislatore tiene però conto della realtà e considera anche l'ipotesi in cui non sia possibile effettuare immediatamente il trasferimento dei dati intercettati. In tal caso, il verbale dovrà indicare le ragioni che hanno impedito una simile immediata trasmissione, oltre alla successione cronologica degli accadimenti captati e delle conversazioni intercettate.

Quanto ai difensori, essi non vengono avvertiti del conferimento. Il procedimento da ultimo delineato dall'art. 268 co. 4 Cpp è infatti bifasico: si scinde la fase della trasmissione (o conferimento), non conosciuta dai difensori, da quella successiva del deposito, di cui deve essere invece dato avviso ai difensori. Previsto dall'art. 268 co. 4, secondo periodo, Cpp, il deposito deve avvenire entro cinque giorni dalla chiusura delle operazioni, «da intendersi come chiusura dei singoli R.I.T.[35]» e non dell'attività di intercettazione[36]. È a partire dal momento del deposito che registrazioni, verbali, decreti di disposizione, autorizzazione, convalida o proroga delle intercettazioni sono messi a disposizione dei difensori.

Si potrebbero però verificare dei casi in cui il deposito determini un grave pregiudizio per le indagini. In simili ipotesi, sussiste la possibilità di ritardare il deposito, peraltro non oltre la chiusura delle indagini preliminari e previa autorizzazione del giudice.

Dal canto suo, la disciplina prevista dall'art. 92 co. 2 NAttCpp stabilisce che, contestualmente alla trasmissione dell'ordinanza che dispone una misura cautelare, vengano restituiti al pubblico ministero tutti gli atti che contengono le comunicazioni e le conversazioni intercettate, che siano ritenute dal giudice irrilevanti o

---

Procura della Repubblica presso il Tribunale di Torino, *Direttiva in tema di nuova disciplina delle intercettazioni,* cit., 1, a partire dal momento del conferimento nell'archivio, la polizia giudiziaria non ha più la disponibilità delle intercettazioni. Ne consegue che potrà riascoltare le intercettazioni solo presso le sale collegate in rete all'archivio digitale.

[34] Nella prassi l'avverbio «immediatamente» sembra ricevere interpretazioni differenti. Infatti, in alcuni casi esso viene riferito all'intera attività di intercettazione; in altri, al momento in cui termina ciascuna operazione di intercettazione disposta; in altri ancora, al singolo R.I.T. ed ai conferimenti singoli.

[35] Così, Procura della Repubblica presso il Tribunale ordinario di Milano, cit., 2. Si può ricordare che R.I.T. è l'acronimo di Registro delle Intercettazioni. In tema, a livello operativo, si riscontrano prassi difformi. Infatti, alcuni uffici riconducono ad unico R.I.T. tutte le intercettazioni che riguardino la stessa persona, a prescindere dal numero dei dispositivi che vengono in rilievo. Diversamente, altri uffici hanno un R.I.T diverso per ogni apparecchio cd. bersaglio. Al riguardo, Procura generale della Corte di Cassazione, *Primi orientamenti in tema di applicazione della nuova disciplina delle intercettazioni di conversazioni o comunicazioni*, 31 luglio 2020, p. 2, precisa che, alla luce della nuova normativa, l'opzione operativa da scegliere coincida con quella che attribuisce un numero di R.I.T diverso per ogni numero di telefono/dispositivo su cui transitano le conversazioni o comunicazioni intercettate.

[36] In questo senso, anche W. Nocerino, *Prime riflessioni in margine del nuovo decreto legge in materia di intercettazioni*, in *SP* 2020, 70.

inutilizzabili[37]. Tale restituzione al pubblico ministero è finalizzata alla conservazione nell'archivio.

5. La riforma Orlando aveva previsto la tenuta dell'archivio presso l'ufficio del pubblico ministero che aveva richiesto ed eseguito le intercettazioni.

Il d.l. 161/2019 focalizza invece l'attenzione sul Procuratore della Repubblica[38] dell'ufficio che ha richiesto ed eseguito le intercettazioni, al quale affida la gestione e la tenuta dell'archivio oltre alla direzione e alla sorveglianza dello stesso (artt. 269 co. 1 e 268 co. 5 Cpp). Tuttavia, non viene specificato come, in concreto, dovrà svolgersi una simile attività di direzione e di vigilanza. È verosimile ipotizzare che ogni Procura elabori dei criteri generali, ferma restando la possibilità di impartire direttive *ad hoc* in relazione a casi specifici. L'auspicio è che ci sia un'omogeneità di previsioni tra le Procure per evitare quelle varianti che, in altri ambiti, rappresentano un aggravio per le parti ed i soggetti del processo, costretti a verificare di volta in volta prassi locali, talora anche assai differenti tra loro.

Occorre però rilevare come il dovere di vigilanza e sorveglianza del Procuratore non debba in alcun modo essere interpretato come monitoraggio tecnico della integrità dei dati. Il Procuratore dovrà predisporre delle misure per regolamentare gli accessi ed approntare tutta una serie di misure organizzative che garantiscano la sicurezza dei dati, ma non dovrà essere gravato di una sorta di vigilanza e sorveglianza tecnico-informatica di naturale competenza di ingegneri, informatici o esperti di ICT.

Attesa la delicatezza del materiale custodito nell'archivio, gli art. 269 co. 1 Cpp e 89-*bis* co. 3 NAttCpp si occupano di disciplinarne gli accessi, che andranno annotati in un registro, denominato modello 37-*bis*, «gestito con modalità informatiche». In particolare, dovrà essere cristallizzata la data, l'ora di accesso e l'ora di termine dell'accesso, nonché gli atti specificamente consultati.

L'accesso e l'ascolto delle conversazioni o comunicazioni registrate sono previsti per il giudice per le indagini preliminari e per i suoi ausiliari, nonché per il pubblico ministero ed i suoi ausiliari i quali, per espressa indicazione[39], ricomprendono anche gli ufficiali di polizia giudiziaria delegati all'ascolto. Possono inoltre accedere ed ascoltare le registrazioni i difensori delle parti, se necessario anche assistiti da un'interprete.

Si può precisare come sia il testo originario della norma sia quello risultante dal decreto all'art. 269 co. 1 Cpp facessero riferimento ai soli «difensori *dell'imputato*»,

[37] Sulle problematiche che si ricollegano al tema del diritto del difensore all'ascolto e alla copia delle registrazioni di intercettazioni utilizzate in sede cautelare, cfr. C. Bortolin, *sub* art. 116, in *Commentario Conso-Illuminati*[2], Milano 2015, 445, nonché A. Boldrin, *sub* art. 116, in *Commentario Illuminati-Giuliani*[3], Milano 2020, 405.

[38] Di conseguenza, non sul singolo sostituto Procuratore che conduce le indagini.

[39] Cfr. art. 89-*bis* co. 3 NAttCpp.

mentre l'art. 89-*bis* co. 3 NAttCpp richiamava anche i «difensori *delle parti*». Si trattava di un evidente difetto di coordinamento, a cui ha posto rimedio la legge di conversione, ammettendo in via generale l'accesso dei difensori delle parti che, ai sensi dell'art. 89-*bis* co. 4 NAttCpp, possono procedere all'ascolto delle registrazioni mediante un apparecchio a disposizione dell'archivio.

Ammesso l'accesso dei difensori, occorre però rendere effettiva tale possibilità. Come ribadito più volte anche dalla Corte europea dei diritti dell'uomo, il principio del contraddittorio implica anche che sia l'accusa sia la difesa possano effettivamente conoscere le prove. Inoltre, l'art. 6.3 lett. *b* Cedu prevede il diritto per l'accusato di disporre del tempo e delle facilitazioni necessarie a preparare la sua difesa[40]. Dal che sembra discendere il diritto a poter disporre di strutture adeguate e, quindi, di locali per l'ascolto delle intercettazioni idonei, dotati di strumentazione soddisfacente anche da un punto di vista numerico e con orari di ingresso compatibili con le esigenze della difesa.

In tema di accesso da parte dei difensori delle parti, la disciplina pare presentare un duplice profilo di criticità.

Da un lato, sembra rimanere escluso il difensore della persona offesa, la quale ultima, come noto, non è una parte[41]. Un simile assetto si pone però in tensione sistematica rispetto all'esercizio dei diritti e delle facoltà riconosciuti alla persona offesa *ex* art. 90 co. 1 Cpp, dato che l'ascolto delle intercettazioni può essere determinante per la presentazione di memorie o per l'indicazione di elementi di prova.

Dall'altro lato, la disciplina è polarizzata sui difensori[42]. Per questo motivo, ci si può chiedere se l'accesso sia consentito anche all'indagato, dato che l'art. 415 *bis* co. 2 Cpp prevede che lo stesso venga avvisato del deposito della documentazione relativa alle indagini e della facoltà sua e del proprio difensore di prenderne visione e di estrarne copia. Al riguardo, un aspetto problematico è rappresentato dal fatto che l'avviso ai sensi dell'art. 415 *bis* co. 2 Cpp riguarda il deposito della documentazione

[40] Cfr. Cedu, Case of Oao Neftyanaya Kompaniya v. Russia (Application no. 14902/04), 20 settembre 2011, §§ 527-551.

[41] Se nel codice previgente la persona offesa era una sorta di «postulante senza diritti» (così, F. Cordero, *Procedura penale*[8], Milano 2006, 276), nel nuovo codice ad essa vengono riconosciuti diritti e facoltà. Per un approfondimento al riguardo si rinvia a P.P. Paulesu, *La persona offesa dal reato,* in *ED*, Annali II (t. I) 2008, 593-617. In riferimento alla vittima si può poi ricordare come questo «slogan può sintetizzare una tendenza, ormai aperta e confermata, a dare importanza alla presenza e alla volontà dell'offeso, nel corso dell'accertamento penale, riconoscendogli diritti di intervento e di partecipazione attiva. Le esigenze espresse dal soggetto leso dal reato hanno guadagnato sempre maggiore considerazione» (Così L. Parlato, *La parola alla vittima. Una voce in cerca di identità e di "ascolto effettivo" nel procedimento penale*, in *Cass. pen*., 2013, 3294). Per un approfondimento su vittime di reato e processo penale cfr., inoltre, L. Luparia (a cura di), *Lo statuto europeo delle vittime di reato, Modelli di tutela tra diritto dell'Unione e buone pratiche nazionali,* Padova 2015).

[42] Come evidenziato da L. Giordano, *L'archivio delle intercettazioni*, cit., § 7 non sembra ad esempio prevista la possibilità dei difensori di farsi assistere da ausiliari, «la cui presenza potrebbe essere necessaria nel caso, per esempio, in cui si trattasse del flusso di dati telematici».

«*presso la segreteria del pubblico ministero*», mentre nel caso delle intercettazioni il deposito avviene *presso l'archivio*. Il dato testuale pare superabile solo attraverso una forzatura, peraltro in linea con i canoni del giusto processo e, in particolare, con l'art. 6.3 lett. *b* Cedu e 111 co. 3 Cost., che prevedono il diritto per l'accusato di disporre delle facilitazioni necessarie a preparare la sua difesa.

Sembrano invece rimanere escluse dall'accesso le parti (che potrebbero infatti accedere solo mediante i loro difensori) e le persone offese. Si potrebbe ritenere che ragioni di sicurezza inducano a restringere il più possibile il numero di soggetti che possono accedere ai locali e che, almeno le parti, potranno pur sempre ascoltare la registrazione rilasciata in copia al difensore. Ciò comporta però un aggravio di costi in capo alle parti, dato che il d.m. 4.7.2018[43] del Ministero della Giustizia prevede per ogni *compact disc* un diritto di copia forfetizzato pari ad euro 323,04.

Quanto alla possibilità di copia della registrazione e degli atti custoditi, si può poi ricordare come una simile eventualità fosse stata esclusa dalla formulazione originaria della norma,

nell'ottica di garantire al massimo grado la riservatezza. Nonostante il pregevole intento di protezione di tale diritto, tutelato sia all'art. 8 Cedu sia all'art. 2 Cost., la previsione sollevava però dei dubbi sul piano della compatibilità convenzionale e costituzionale. Ancora una volta veniva in rilievo il diritto a un equo processo *ex* art. 6.3 lett. *e* Cedu e 111 co. 3 Cost. laddove prevede il diritto per l'accusato di disporre delle facilitazioni necessarie a preparare la sua difesa. L'impossibilità di ottenere copia sembrava infatti appesantire ed ostacolare lo svolgimento delle attività difensive.

Da ultimo, il legislatore ha quindi effettuato un diverso bilanciamento tra i diritti in gioco. Ne è derivata una modifica della disciplina, in forza della quale è stato espressamente ammesso che i difensori possano estrarre copia delle registrazioni e degli atti acquisiti ai sensi degli artt. 268, 415-*bis* e 454 Cpp[44]. Il rilascio di ogni copia è annotato in un registro di cui è prevista la sola gestione in modalità informatica e nel quale viene tenuta traccia degli atti rilasciati e della data e dell'ora della consegna.

Se il rilascio delle copie è funzionale all'esercizio del diritto di difesa, non sfugge come lo stesso esponga a rischio la riservatezza, potendo oltretutto neutralizzare la garanzia della distruzione ai sensi dell'art. 269 Cpp, la quale può dispiegare appieno il suo effetto soltanto se non vi sono duplicazioni dei dati[45].

---

[43] Decreto di adeguamento degli importi del diritto di copia e di certificato ai sensi dell'articolo 274 d.p.r. 30.5.2002 n. 115.

[44] Per la precisazione che il diritto di ottenere copia può essere esercitato soltanto dopo il provvedimento di formale acquisizione delle intercettazioni, cfr. G. Amato, *Avviso di deposito esteso ai difensori di tutte le parti,* in *GD* 2020 (13), 53.

[45] Un parziale contrappeso può comunque essere ravvisato nell'illiceità della diffusione delle copie. Al riguardo, si veda S. Renzetti, *Una riforma (radicale?) per tornare allo spirito originario della legge: la nuova disciplina*

6. In ambito processuale penale l'incremento della digitalizzazione e della connettività, se correttamente governato, schiude nuovi scenari, potendo contribuire significativamente ad una maggiore efficienza del sistema. Tuttavia, non bisogna dimenticare i rischi connessi alla sicurezza informatica (cd. *cybersecurity*)[46]. Si tratta di un profilo rilevantissimo che involge sistemi informativi, reti di comunicazione, prodotti digitali, servizi, dispositivi utilizzati e uffici[47]. La *cybersecurity* non si ricollega soltanto ad aspetti tecnici, ma è strettamente connessa anche ai comportamenti adottati.

I dati conservati negli archivi digitali sono dati digitali. Ne consegue che sono caratterizzati da intrinseca predisposizione alla vulnerabilità, essendo facilmente modificabili ed eliminabili[48].

A ciò si aggiunge che gli stessi sistemi che trasmettono o custodiscono i dati possono avere delle falle derivanti da azioni criminose o da errori di programmazione o, ancora, da malfunzionamento, con il conseguente rischio di diffusione dei dati.

Eventuali fughe di dati rischiano di tradursi, però, in gravissime violazioni se non altro del diritto alla protezione dei dati personali, con conseguenze anche sul piano dell'efficacia investigativa. La direttiva 2016/680/UE si è occupata specificamente di prevedere delle norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento, perseguimento di reati e esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione dalle minacce alla sicurezza pubblica.

Consapevole che sicurezza e *privacy* si intrecciano in un rapporto simbiotico[49],

---

acquisitiva delle intercettazioni tra legalità, diritto vivente e soft law, in *LP*, 4.4.2018, 54 che sottolinea come «anche in questa fase, il miglior bilanciamento sarebbe stato, probabilmente, quello di puntare sui presidi sanzionatori del segreto, magari anche attraverso la previsione di pene più rigide o di una specifica aggravante per la diffusione di colloqui già distrutti».

[46] Cfr. regolamento 881/2019/UE, 17.4.2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»).

[47] Per un'analisi dei problemi legati alla sicurezza informatica in conseguenza dei mutati comportamenti derivanti dalla diffusione di *covid*-19 si veda il *report* di Interpol dal titolo "Cybercrime: COVID-19 Impact", 2020.

[48] Come indicato in Ministero della Giustizia, *Relazione del Ministro sull'amministrazione della giustizia anno 2019, inaugurazione dell'anno giudiziario 2020, Dipartimento dell'organizzazione giudiziaria del personale e dei suoi servizi*, 2020, p. 17, nel 2019 è «stato promosso un piano di intervento per la messa in sicurezza di sistemi relativi alle intercettazioni in modo tale che i fornitori dei servizi di intercettazione eseguano ogni intervento di amministrazione e manutenzione dei propri sistemi utilizzando le tecnologie di gestione degli accessi privilegiati installate dal Ministero della giustizia. Dette piattaforme consentono il *logging* e la "videoregistrazione" di tutte le operazioni svolte durante le sessioni di lavoro».

[49] Il medesimo rapporto sussiste con la segretezza, che si ricollega infatti strettamente alla predisposizione di adeguate misure di sicurezza tecniche e strutturali, unite al severo controllo non solo di chi accede all'archivio, ma anche del che cosa fa durante l'accesso all'archivio. Dal canto suo, la disciplina prevista dall'art. 89-*bis* co. 2

la direttiva 2016/680/UE chiarisce che la tutela della *privacy* si declina in due profili[50]: da un lato, quello della predisposizione di adeguate misure di sicurezza nella fase di programmazione dei mezzi di trattamento (cd. *privacy by design*)[51]; dall'altro, quello dell'adozione di adeguate misure tecniche ed organizzative nella fase del trattamento delle informazioni (cd. *privacy by default*).

Sul piano interno, il legislatore si rende conto della serietà e gravità dei rischi per i diritti fondamentali che possono derivare dall'impiego dell'archivio e mira a garantirne il più possibile la sicurezza[52], sia da un punto di vista di *privacy by design* che di *privacy by default*.

Di entrambi i profili paiono essersi occupati gli allegati A dei provvedimenti del Direttore generale dei servizi informativi automatizzati datati 5.12.2019 e 1° luglio 2020 relativi alle specifiche tecniche per il conferimento nell'archivio delle intercettazioni. Come precisato in entrambi i provvedimenti, le specifiche tecniche sono state elaborate tenendo conto delle indicazioni del Garante per la protezione dei dati personali in materia di intercettazioni di conversazioni e comunicazioni, con

---

NAttCpp stabilisce che l'archivio sia gestito impiegando delle modalità che assicurino la segretezza in rapporto alle intercettazioni non necessarie per il procedimento, irrilevanti, di cui sia vietata l'utilizzazione o che riguardino categorie particolari di dati personali. Tale previsione deve essere coordinata con l'art. 329 co. 1 Cpp in tema di atti di indagini, con la conseguenza che tutta la documentazione contenuta nell'archivio delle intercettazioni può essere coperta da segreto (in questo senso, cfr. Corte Suprema di Cassazione, Ufficio del Massimario e del ruolo, Sevizio Penale, cit., 53). Inoltre, *ex* art. 114 co. 2-*bis* Cpp, è sempre vietata la pubblicazione, anche parziale, del contenuto delle intercettazioni non acquisite ai sensi degli articoli 268, 415-*bis* o 454 Cpp. La *ratio* va individuata nella volontà del legislatore di applicare il divieto di pubblicazione a tutte le intercettazioni non acquisite al procedimento (in tema, cfr. M. Bolognari, *sub* art. 114 c.p.p., in *Commentario Illuminati-Giuliani*[3], cit., 390, nonché S. Renzetti, *sub* artt. 266-272, in *Commentario Illuminati-Giuliani*[3], cit., 1157). Ne consegue che può sussistere la segretezza anche quando termina il segreto investigativo (cfr. *Guida pratica ad una prima lettura tecnologica e normativa della legge 28 febbraio 2020, n. 7 e del decreto legge 30 aprile 2020, n. 28*, cit., 5). Più in generale, per un approfondimento critico delle norme che regolano la segretezza e i limiti di pubblicazione degli atti processuali penali cfr. R. Orlandi, *La giustizia penale nel gioco di specchi dell'informazione*, in *Dir. pen. cont. Trim.* 2017, n. 3, 37-46. Si può rilevare che il testo originario dell'art. 269 co. 1-*bis* Cpp stabiliva che «non sono coperti da segreto i verbali e le registrazioni delle comunicazioni e conversazioni acquisite al fascicolo di cui all'art. 373 comma 5». Tale norma è stata però abrogata dal decreto legge, per essere poi riesumata dalla legge di conversione che l'ha riproposta con qualche minimo adattamento, prevedendo che «non sono coperti da segreto *solo* i verbali e le registrazioni delle comunicazioni e conversazioni acquisite di cui all'art. 373 co. 5 *o comunque utilizzati nel corso delle indagini preliminari*».

[50] Cfr. art. 20 (Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita), direttiva 2016/680/UE.

[51] Cfr. D. Klitou, Privacy-Invading Technologies and Privacy by Design. Safeguarding Privacy, Liberty and Security, in the 21st Century, Berlino 2014, nonchè J. Van Den Hoven, *La* Privacy by Design*: il caso della videosorveglianza,* in Aa.Vv., *Cittadini, città e videosorveglianza*, Montreuil 2010, 61 ss.

[52] L'archivio intende «rendere tracciabile l'accesso a informazioni relative ai risultati delle intercettazioni innalzando gli *standard* di sicurezza indispensabili per la tutela della riservatezza di terzi non coinvolti nella vicenda processuale o delle parti stesse rispetto alla diffusione di dati non utilizzati o non rilevanti a fini investigativi o processuali». In questi termini, Senato della Repubblica, XVIII Legislatura, cit., p. 7.

particolare riguardo al provvedimento del 18.7.2013. Nell'ottica di una maggiore tutela della sicurezza, le specifiche tecniche sono state opportunamente pubblicate soltanto in un sito riservato a cui possono accedere le mere società fornitrici, peraltro a seguito di apposita richiesta.

Dal canto suo, anche la disciplina del codice di procedura penale e delle relative norme di attuazione presta una costante attenzione al tema della sicurezza. In tale prospettiva, infatti, si prevede (art. 89 co. 2 NAttCpp) che i programmi impiegati per l'installazione e la captazione mediante *trojan* debbano essere conformi ai requisiti tecnici previsti dal Decreto del Ministero della Giustizia. Inoltre, le intercettazioni così eseguite possono essere conferite soltanto in impianti della Procura della Repubblica e solo dopo che siano state acquisite informazioni circa le condizioni tecniche relative alla sicurezza e alla affidabilità della rete di trasmissione. Ancora, durante il trasferimento dei dati va effettuato un costante monitoraggio dell'integrità in modo tale che sia garantita l'esatta corrispondenza tra quanto intercettato, registrato e trasmesso (art. 89 co. 3 NAttCpp).

Ma la sicurezza dei dati deve essere garantita non solo sotto il profilo digitale, ma anche in rapporto alla adeguatezza degli ambienti[53] in cui sono conservati i dati, senza contare che è necessario tenere traccia di tutti coloro che effettuano l'accesso, identificandoli e assegnando loro un codice di volta in volta diverso. Assai opportunamente, quindi, l'art. 3 d.m. 20.4.2018 del Ministero della Giustizia stabilisce che debbano essere adottate misure organizzative di vigilanza dei locali ove può essere esercitato il diritto di accesso. Inoltre, si prevede il divieto di introdurre dispositivi idonei alla comunicazione, alla duplicazione, alla diffusione esterna degli atti e delle registrazioni. Di conseguenza, è vietato l'ingresso anche di telefoni.

I problemi si collocano però sul fronte dei controlli. Certamente, la videoripresa dei locali potrà fornire un valido ausilio, ma non basta. Non si può infatti dimenticare come esistano registratori o *device,* idonei a videoriprendere, dalle dimensioni talmente ridotte da essere facilmente occultabili. Si tratta di un fenomeno che, forse, potrebbe essere in parte arginato impiegando strumentazione atta a rilevare l'esistenza di dispositivi occultati.

7. In tema di conservazione delle informazioni captate si contrappongono esigenze diverse tra cui, da un lato, quella di conservare i dati per il più ampio arco temporale e in maggior numero possibile per finalità di accertamento dei reati;

[53] A tale fine il Garante per la protezione dei dati personali, *Provvedimento in materia di misure di sicurezza nelle attività di intercettazione da parte delle Procure della Repubblica*, cit., 3 ha espressamente previsto l'adozione di misure di sicurezza fisica quali, ad esempio, impianti per il rilevamento e l'estinzione di incendi o idonee misure di protezione e serrature di sicurezza alle finestre.

dall'altro, quella di protezione del diritto alla riservatezza delle comunicazioni[54] che, come noto, la Corte costituzionale ha ricondotto all'area dei diritti inviolabili *ex* art. 2 Cost., ammettendone la limitazione «soltanto nella misura strettamente necessaria alle esigenze di indagini[55]».

Una adeguata tutela della riservatezza delle comunicazioni e, più in generale, del diritto alla protezione dei dati personali implica che, almeno in certi casi, l'interessato possa richiedere l'eliminazione dall'archivio di dati che lo riguardano[56].

In effetti, gli interessati [57] possono formulare richiesta di distruzione della documentazione al giudice che ha autorizzato o convalidato l'intercettazione[58]. Dal canto suo, il giudice può pronunciarsi nel senso della distruzione della documentazione soltanto se quest'ultima non è necessaria per il procedimento[59].

---

[54] Naturalmente, a tali esigenze si possono ad esempio aggiungere quella della tutela dell'esercizio del diritto di difesa o della segretezza della documentazione. Sottolinea G. Illuminati, *La disciplina processuale delle intercettazioni,* Milano 1983, 4 come all'interno «della cosiddetta sfera della riservatezza occorre però distinguere il vero e proprio diritto al segreto che, pur essendo della medesima natura – poiché ha sempre ad oggetto il controllo sulla circolazione delle informazioni attinenti alla vita privata – riceve una tutela più specifica e più rigorosa». Quanto alla distinzione tra segreto e segretezza, secondo F. Caprioli, *Colloqui riservati e prova penale,* Torino 2000, 11-12 il primo tutelerebbe l'esigenza che, ad eccezione del destinatario, nessuna persona percepisca la comunicazione; la segretezza proteggerebbe invece l'interesse che nessun altro oltre al destinatario della comunicazione «apprenda i fatti e le comunicazioni che costituiscono l'oggetto della comunicazione stessa».

[55] In questi termini, *ex multis,* Corte cost. 13 febbraio 1995 n. 37.

[56] Altro discorso è che, *ex* art. 271 co. 3 Cpp, in ogni stato e grado del processo, il giudice possa disporre la distruzione della documentazione delle intercettazioni non utilizzabili salvo che la stessa documentazione costituisca corpo del reato. Come evidenziato da A. Camon, *Le intercettazioni nel processo penale*, Milano 1996, 259 la norma non pare riferibile ai casi di nullità. Infatti, «in materia di captazioni foniche, questa sanzione colpisce anomalie del procedimento acquisitivo ed in tali casi il rimedio è meno drammatico: basta rinnovare *secundum legem* l'acquisizione». La previsione *ex* art. 271 co.3 Cpp mira a neutralizzare da subito i possibili sviluppi di una prova vietata (cfr. A. Camon, *sub* art. 271 c.p.p., in *Commentario Illuminati-Giuliani*[3], cit., 1137), ma garantisce anche la riservatezza delle comunicazioni.

[57] Si può ricordare come nella categoria dei soggetti interessati possa essere ricompreso anche il pubblico ministero. In questo senso, cfr. Cass., 20.10.2016 n. 48595. A seguito della richiesta degli interessati, il giudice decide in camera di consiglio *ex* art. 127 Cpp. Rileva A. Camon, *Forme, destinazione e regime della documentazione*, cit., 91: «Spiace invece che sia andata perduta un'intuizione del disegno Mastella, dov'era previsto che, alla fine dell'indagine, i soggetti titolari delle utenze sotto controllo venissero informati dell'intercettazione subita. Era un'idea ancora grezza, che aveva bisogno di qualche messa a punto (…); ma avrebbe potuto rivitalizzare l'art. 269 c.p.p., che continuerà invece a scontare un grave difetto: attribuisce un diritto a soggetti che, nella maggioranza dei casi, non sanno d'averlo e non potranno quindi esercitarlo». Sicché il terzo estraneo al processo appare una sorta di «convitato di pietra» (così S. Renzetti, *Una riforma (radicale?) per tornare allo spirito originario della legge: la nuova disciplina acquisitiva delle intercettazioni tra legalità, diritto vivente e* soft law, cit., 67). A fronte di un simile assetto, secondo C. Conti, *La riservatezza delle intercettazioni nella "delega Orlando",* in *DPC* 2017, 92 la tutela dei terzi estranei finisce per essere rimessa alla valutazione del pubblico ministero e, almeno sul piano fattuale, al previo vaglio della polizia giudiziaria.

[58] Per un approfondimento sui profili differenziali della disciplina in tema di distruzione *ex* art. 269 co. 2 e 271 co. 3 Cpp si rinvia a Procura della Repubblica presso il Tribunale di Napoli, *Criteri direttivi in tema di intercettazioni inutilizzabili o irrilevanti nonché in tema di conversazioni del difensore*, direttiva 1/2016, 16.2.2016.

[59] Cfr. art. 269 co. 2 Cpp.

Al riguardo, occorre chiedersi se il giudizio di necessarietà debba riguardare il solo procedimento in cui sono state disposte le intercettazioni o possa essere riferito anche agli altri procedimenti in cui le medesime intercettazioni sono utilizzabili[60] *ex* art. 270 Cpp[61].

Appare di tutta evidenza che pure soggetti di procedimenti diversi, ma in cui le intercettazioni siano utilizzabili[62], possano essere interessati a una simile distruzione. Non bisogna dimenticare che suoni e voci captate rappresentano dati personali, qualora permettano di indentificare un soggetto anche in via indiretta[63]. Il che rende applicabile la direttiva 2016/680/UE[64] e il relativo decreto attuativo[65], i quali non mancano di riconoscere agli interessati il diritto alla cancellazione dei dati personali[66].

Tuttavia, ciò non significa che il giudice debba valutare la non necessarietà per il procedimento tenendo conto anche degli altri procedimenti in cui le medesime intercettazioni sono utilizzabili. A parte il fatto che tale giudice potrebbe non conoscere nemmeno l'esistenza degli altri procedimenti, sono le stesse regole in tema di competenza ad imporre che il giudice effettui la sua valutazione soltanto in ordine al procedimento soggetto al suo vaglio.

In definitiva, ogni interessato potrà chiedere la distruzione delle registrazioni in tutti i procedimenti in cui esse siano utilizzabili, ma il giudice potrà valutare la non necessarietà soltanto in rapporto ai procedimenti rispetto ai quali è competente e non

---

[60] La riforma Orlando ha infatti previsto l'utilizzabilità delle intercettazioni anche al di là del procedimento in cui le stesse sono state eseguite. Una simile eventualità è però subordinata alla circostanza che gli esiti siano rilevanti e indispensabili per l'accertamento dei delitti per i quali è obbligatorio l'arresto in flagranza, nonché per i reati ricompresi nel catalogo *ex* art. 266 co. 2-*bis* Cpp. In aggiunta, da ultimo, il d.l. 161/2019 ha allargato ulteriormente il regime di utilizzabilità. Nello specifico, nel caso in cui la captazione sia avvenuta mediante *trojan* gli esiti potranno essere utilizzati anche per procedimenti diversi, qualora essi risultino indispensabili per l'accertamento dei reati *ex* art. 51 commi 3-*bis* e 3-*quater* Cpp, nonché per i delitti dei pubblici ufficiali e degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni.

[61] Sottolinea come non sembri coerente ancorare il vaglio sulla presenza delle condizioni per distruggere la documentazione alla sola necessità del procedimento nell'ambito del quale le intercettazioni sono state effettuate, CSM, *Parere sul Disegno di Legge n. 1659 AS di conversione del Decreto Legge n. 161/2019 recante modifiche urgenti alla disciplina delle intercettazioni di conversazioni o comunicazioni*, delibera 13.2.2020, 9.

[62] Ai sensi dell'art. 270 co. 2 Cpp, nel caso di utilizzabilità in altri procedimenti, i «verbali e le registrazioni» delle intercettazioni sono depositati presso l'autorità competente per il diverso procedimento.

[63] In questo senso, cfr. Garante 17 dicembre 1997, in *Bollettino* n. 2, 1997, 57 [doc. web n. 39849].

[64] Cfr. art. 14 lett. *e* direttiva 2016/680/UE, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

[65] Il riferimento è al d. lvo 18.5.2018, n. 51 e, in particolare, all'art. 10 lett. *e* dello stesso.

[66] Dal canto suo, la C.G.UE ha rimarcato l'esistenza del diritto all'oblio anche in rapporto alla rete. Al riguardo, cfr. C.G.UE, 13.5.2014, C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*.

anche in riferimento ai diversi procedimenti in cui le intercettazioni sono utilizzabili.

Poiché ogni giudice è autonomo in ordine alla valutazione potrebbero verificarsi casi in cui determinate intercettazioni, distrutte[67] su richiesta degli interessati in rapporto ad un procedimento, vengano invece considerate necessarie in un diverso procedimento.

Quanto alla decisione sul requisito della necessarietà per il procedimento, si tratta di un giudizio prognostico assai difficile, perché ciò che può apparire non necessario o necessario al momento di tale decisione potrebbe rivelarsi l'opposto in un momento successivo. Si pensi solo ai casi in cui gli indagati utilizzino linguaggi in codice non ancora decodificati. Frasi che ad un primo ascolto potrebbero apparire non necessarie per il procedimento potrebbero invece rivestire un'importanza strategica, anche *pro reo*, in un momento successivo[68]. Senza contare che la distruzione decontestualizza ciò che resta, con il rischio che venga poi misinterpretato.

Un diverso caso di distruzione delle registrazioni si verifica in conseguenza dello scorrere del tempo. In tema, occorre ricordare che, ai sensi dell'art. 269 co. 2 Cpp, le registrazioni sono conservate sino alla sentenza non più impugnabile[69], salvo che il giudice non abbia disposto *ex* art. 271 co. 3 Cpp la distruzione della documentazione delle intercettazioni.

Il legislatore ricollega quindi il termine di conservazione delle registrazioni all'irrevocabilità della sentenza[70]. Almeno in rapporto ai reati associativi, sarebbe parso però più opportuno adottare un approccio incentrato sul numero di anni trascorsi dal momento del passaggio in giudicato, come avviene in tema di trattamento di dati per finalità di polizia[71] ove, ad esempio, i dati confluiti in un procedimento penale, e

[67] Nel caso in cui il giudice opti per la distruzione, quest'ultima dovrà essere eseguita con il controllo del giudice, «nei casi in cui è prevista».

[68] Analogamente, in riferimento alla valutazione di rilevanza, cfr. G. Giostra, *Prima lezione sulla giustizia penale*, Bari-Roma 2020, 167. Di diversa opinione M. Gialuz, *Segreto e tutela della riservatezza e divieto speciale di pubblicazione delle intercettazioni*, in *Dinternet* 2020 (3, supplemento), 69 che pone in evidenza il rischio che la mancata distruzione del materiale captato si traduca in un bacino informativo dal quale l'accusa attinga le intercettazioni «ripescandole nell'ambito di nuovi filoni di indagine aperti magari a distanza di anni. Uno scenario evidentemente inaccettabile in una democrazia liberale come la nostra».

[69] La nozione di conservazione sino alla sentenza irrevocabile è concetto diverso da quello di periodo di accessibilità alle registrazioni da parte dei difensori. Sotto quest'ultimo profilo, *ex* art. 268 co. 4 Cpp è il pubblico ministero a stabilire le tempistiche. Viene però fatta salva la possibilità per il giudice di reputare necessaria una proroga. Critica il meccanismo, ritenendo che sarebbe stato più opportuno rimettere al giudice per le indagini preliminari la determinazione della durata del deposito per i difensori dell'indagato L. Filippi, *D.L. intercettazioni: abrogata la riforma Orlando, si torna all'antico*, in *www.quotidianogiuridico.it*.

[70] Ricorda come la previsione *ex* art. 269 co. 2 Cpp, secondo la quale le intercettazioni devono essere distrutte dopo la sentenza irrevocabile, sia sostanzialmente disapplicata e sottolinea come la norma andrebbe abrogata N. Gratteri, *Memorie depositate dagli auditi*, in *Audizioni informali nell'ambito dell'esame del disegno di legge n. 1659 (d.l. 161/2019 - intercettazioni)*, Sed. n. 109, 4.2.2020, https://www.senato.it/3649.

[71] Effettuato da organi, uffici e comandi di polizia.

raccolti mediante una videoripresa che documenti l'attività operativa, vengono conservati per vent'anni dal passaggio in giudicato in caso di provvedimento di archiviazione e di sentenza di assoluzione o di non doversi procedere, mentre vengono conservati per venticinque anni dal passaggio in giudicato nel caso di sentenza di condanna[72].

8. La digitalizzazione è un fenomeno inarrestabile che permea ormai di sé ogni settore, compreso quello della giustizia. Tuttavia, in ragione della particolare delicatezza dei diritti in gioco, in materia penale si è assistito ad un atteggiamento di tendenziale prudenza, con punte di resistenza, nei confronti dell'ingresso della tecnologia. Vari ambiti hanno però ceduto all'assedio. Ad esempio, l'esigenza di contrastare una criminalità sempre più tecnologica, unita alla circostanza che, di frequente, le prove sono digitali, ha portato ad individuare una nuova declinazione delle indagini rappresentata dalle indagini digitali[73]. Dal canto suo, la necessità, tra l'altro, di limitare i contatti degli imputati con le associazioni criminose e di ridurre i costi dei trasferimenti dei detenuti è stata determinante nell'individuare l'istituto della partecipazione a distanza mediante collegamento video[74].

Nonostante il processo civile telematico ed il processo tributario telematico fossero divenuti realtà, il processo penale ha cercato di resistere alla sua rimodulazione in processo penale telematico, anche se aveva iniziato a subire una progressiva digitalizzazione, ad esempio in rapporto all'impiego dei sistemi informatici ed alle notifiche telematiche. Da ultimo si è però assistito ad una sorta di marcia verso la digitalizzazione, come dimostrano le misure adottate in conseguenza di *covid*-19 e la previsione dell'archivio delle intercettazioni.

Inizia a delinearsi una giustizia penale tecnologica, secondo un assetto idoneo a determinare significativi effetti sistematici sul processo penale. Tracciata la via verso la digitalizzazione occorre percorrerla, nella consapevolezza che si tratta di un percorso in divenire, soggetto a continue modifiche per adeguare la realtà tecnologica a quella giuridica. Si tratta di un cammino che richiede tempo e tempismo, costanza, pazienza, risorse e apporto collaborativo da parte di tutti i soggetti coinvolti.

---

[72] Cfr. art. 10 co. 3 d.p.r. 15.1.2018 n. 15 (regolamento a norma dell'art. 57 del d. lgs. 30.6.2003 n. 196 recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia). Al riguardo, esprime «iniziale "smarrimento"» per il fatto che una materia così delicata sia stata disciplinata da un provvedimento di rango non legislativo, B. Galgani, *Giudizio penale,* habeas data *e garanzie fondamentali,* in *www.archiviopenale.it* 2019, 9.

[73] Sull'impatto sistematico determinato da simili indagini cfr., volendo, S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino 2018.

[74] Per un approfondimento del tema si rinvia a M. Daniele, *La formazione digitale delle prove dichiarative. L'esame a distanza tra regole interne e diritto sovranazionale*, Torino 2012.

Anche in riferimento all'archivio, non sfuggono gli ostacoli che si ricollegano a più ampie problematiche di fondo relative alle risorse umane, alle strutture e ai sistemi informatici, alla semplificazione.

a) Quanto al profilo delle risorse umane, occorre rilevare come la gestione ed il funzionamento dell'archivio difficilmente potrà avvenire a personale tendenzialmente invariato da un punto di vista numerico. Come si è già ricordato, all'interno di TIAP viene conservata la documentazione digitale inerente alle intercettazioni. Allo stato, però, la documentazione è analogica, in quanto cartacea. Ciò significa che dovrà esserne effettuata una copia digitale al fine di poterla inserire in TIAP. L'art. 1 d.m. 20.4.2018 del Ministero della Giustizia assegna tale compito al pubblico ministero, che non potrà far altro che delegarlo.

Sotto questo profilo, vi sono però Procure che evidenziano come il proprio utilizzo di TIAP possa essere solo parziale, ad esempio in rapporto alla mera fase del deposito degli atti *ex* art. 415-*bis* c.p.p., essendo impossibile estenderne l'utilizzo a causa della mancanza di risorse di personale[75].

In ogni caso, a personale invariato, ne deriverà un sovraccarico di lavoro per il delegato alle scansioni ed all'inserimento della documentazione in TIAP. Il che può determinare un suo sviamento dalle mansioni a cui solitamente attende, con conseguente inevitabile ritardo nello svolgimento delle stesse.

Dal canto loro, al fine di una corretta fruizione di TIAP, gli incaricati alla scansione dovranno avere cura di verificare, da un lato, che nella copia digitale non vi siano omissioni di pagine; dall'altro, che quanto scansionato sia chiaramente visualizzabile, che non vi siano tagli di pagine e che, possibilmente, il documento digitale mostri pagine scansionate in corretta successione e non storte. Occorre mettersi nei panni di chi dovrà leggere quelle pagine ed adoperarsi perché il risultato della scansione sia il migliore possibile.

b) Venendo al secondo aspetto, esso è relativo all'inadeguatezza strutturale e informatica che connota ancora talune realtà.

Sul piano strutturale, non si può ignorare come talune Procure si siano trovate dinanzi alla difficoltà di individuare dei locali idonei a custodire l'archivio delle intercettazioni.

Inoltre, in tema di inadeguatezza informatica, il panorama appare diversificato. Salve le virtuose eccezioni, in linea tendenziale gli Uffici giudicanti sembrano caratterizzati da un minor grado di informatizzazione rispetto alle Procure della Repubblica. Ma anche queste ultime si connotano per livelli di informatizzazione differenziati. Va poi rilevato che alcune Procure lamentano la mancanza

[75] Al riguardo, cfr. Procura della Repubblica presso il Tribunale di Torino, *Direttiva in tema di nuova disciplina delle intercettazioni,* cit., p. 2, nota 1.

dell'applicativo informatico per il registro modello 37 (registro R.I.T.). Si tratta di un profilo problematico perché, ad eccezione delle Procure che utilizzano sistemi in grado di ricomprendere l'intero *iter* delle intercettazioni, nelle altre Procure «i R.I.T. continueranno ad essere annotati su registro cartaceo, con tutti i conseguenti inconvenienti tecnici»[76]. Appare quindi necessaria una tempestiva informatizzazione dei R.I.T.

Va inoltre ricordato come non sia raro che la magistratura onoraria risulti sprovvista di una postazione informatica[77]. Criticità ancora maggiori si delineano in rapporto ai tirocinanti.

Inoltre, come si diceva, uno dei fattori del corretto funzionamento dell'archivio è rappresentato da TIAP, la cui efficacia è strettamente correlata all'esattezza ed alla qualità delle scansioni dei documenti in esso immessi. Il che discende anche da aspetti marcatamente pratico operativi, legati alla strumentazione a disposizione. Ne consegue l'urgenza di verificare che gli uffici abbiano a disposizione *scanner* adeguati[78], rispetto ai quali esista un servizio di assistenza in grado di intervenire tempestivamente e risolutivamente in caso di guasti o anomalie quali, ad esempio, macchine che si inceppano, fogli immessi nei fascicolatori che scompaiono tra gli ingranaggi, pagine prelevate insieme anziché una alla volta.

Più in generale, significative problematiche si delineano in rapporto al servizio di assistenza dei sistemi informatici, dato che tale servizio si trova a fronteggiare contemporaneamente le esigenze di più uffici giudiziari, con possibili riverberi sul piano della mancanza di tempestività dell'intervento[79].

c) Una terza linea di fondo si ricollega ad uno dei principi della delega legislativa[80] all'emanazione del vigente codice di procedura penale, secondo il quale il codice avrebbe dovuto attuare la «massima semplificazione nello svolgimento del processo con eliminazione di ogni atto o attività non essenziale».

Al di là dell'aura che la circonda, l'informatizzazione non è di per sé sufficiente al raggiungimento di questo obiettivo. Sistemi non adeguati possono infatti provocare

---

[76] Così, M. de Lucia, *Memorie depositate dagli auditi,* in *Audizioni informali nell'ambito dell'esame del disegno di legge n. 1659 (d.l. 161/2019 - intercettazioni)*, Sed. n. 109, 4.2.2020, 1, https://www.senato.it/3649.

[77] Come riportato nella Relazione 2019 del CSM sullo stato della giustizia penale telematica in riferimento al 2018, solo 29 Procure ordinarie su 133 erano in grado di assegnare in via esclusiva una postazione di lavoro con dotazioni informatiche collegate alla rete a tutti i V.P.O. in servizio.

[78] Va dato atto che, da ultimo, si è proceduto all'acquisto di 5000 *scanner* (apparecchiature con funzionalità di copia e stampa). Al riguardo, cfr. Ministero della Giustizia, *Relazione del Ministro sull'amministrazione della giustizia anno 2019, inaugurazione dell'anno giudiziario 2020, Dipartimento dell'organizzazione giudiziaria del personale e dei suoi servizi*, 2020, p. 15.

[79] Come emerge da Consiglio Superiore della Magistratura, *Relazione sullo stato della giustizia penale telematica 2018,* cit., p. 2, sul versante dell'assistenza, viene avvertita l'esigenza di poter disporre di una maggiore presenza di personale tecnico presso le sedi giudiziarie.

[80] Cfr. art. 2 n. 1 l. 16.2.1987 n. 81.

complicazioni, rallentamenti, se non la paralisi. Occorrono quindi sistemi informatici inerenti all'archivio che combinino facilità di utilizzo, efficacia e capacità di tenere il passo con le evoluzioni normative e tecnologiche.

Servono sistemi che semplifichino e che non aggravino il lavoro del magistrato. In definitiva, occorre una digitalizzazione al servizio del magistrato e non un magistrato al servizio della digitalizzazione. Solo nel primo caso, infatti, l'informatizzazione avrà contribuito a realizzare il principio espresso dalla legge delega relativo alla «massima semplificazione».

Semplificazione non significa però semplicismo. Al riguardo, si può evidenziare un aspetto apparentemente marginale, ma larvatamente destrutturante, che caratterizza i sistemi informatici. Il riferimento è allo scadimento del linguaggio in rapporto ai vocaboli impiegati nell'ambito degli applicativi informatici. Chiunque usi TIAP o altri applicativi informatici è costretto a visualizzare di continuo termini come «cruscotto» o «vaschetta». Si potrebbe obiettare che, nella maggior parte dei casi, l'involuzione lessicale si ricollega al fatto che i vocaboli sono il frutto di una infelice traduzione dall'inglese. Il che è senz'altro vero, ma il fenomeno va monitorato perché non è scevro da effetti.

Basti ricordare quanto asserivano, ad esempio, Heidegger o Wittgenstein. Il primo riteneva che il linguaggio fosse la casa dell'essere e che non fosse l'uomo a forgiare il linguaggio, ma il linguaggio a forgiare l'uomo. Ne deriverebbe che lo svilimento del linguaggio avrebbe come ricaduta diretta l'impoverimento del pensiero del giurista. Se, poi, si accede all'idea di Wittgenstein, secondo la quale «i confini del mio linguaggio sono i confini del mio mondo»[81], occorre interrogarsi sul fatto di essere limitati da un «cruscotto» o da una «vaschetta». Per questo motivo, sarebbe opportuno avere cura anche del lessico impiegato nei sistemi informatici.

Se, allo stato, l'operatività dell'archivio delle intercettazioni è in parte contornata di talune (superabili) problematiche applicative, va rilevato come si sia assistito ad un lodevole sforzo volto a dare attuazione alla nuova disciplina. Il riferimento è anzitutto all'enorme lavoro svolto dalla Direzione generale per i sistemi informativi automatizzati che, oltretutto in tempi di pandemia, si è trovata a dover tracciare nuove vie a fronte della complessità tecnologica. Non si può poi dimenticare l'importante lavoro svolto dalle procure della Repubblica, dalla polizia giudiziaria, dalle cancellerie e da tutti i soggetti a vario titolo coinvolti per rendere operativo l'archivio.

In conclusione, l'archivio delle intercettazioni appare ancora uno strumento *in fieri*, il cui funzionamento è subordinato alla disponibilità di adeguate risorse umane ed informatiche. Intanto, ne è stata delineata l'architettura. Occorre proseguire sulla

[81] Cfr. L. Wittgenstein, *Tractatus Logico-Philosophicus,* 1921, § 5.6.

via della sua edificazione ancorandola ai seguenti pilastri: sicurezza dei dati, efficacia ed efficienza, finalizzate alla tutela dei diritti fondamentali e alla massima semplificazione.