EDITORIALE

ALFREDO GAITO

Comunicazioni criptate ed esigenze difensive (da Blackberry a Sky-ECC)*

L'autore esamina l'evoluzione e l'involuzione delle problematiche riguardanti la materia delle intercettazioni telefoniche e telematiche analizzandone patologie, storture e nuovi approdi applicativi, suggerendo in conclusione un approccio europeisticamente orientato volto alla salvaguardia dei principi di eguaglianza, di proporzionalità e di legalità.

Encrypted communications and defensive needs (from Blackberry to Sky-ECC)

The author examines the evolution and involution of the problems concerning the subject of telephone and telematic interception, analyzing pathologies, distortions and new applications, suggesting in conclusion a European-oriented approach aimed at safeguarding the principles of equality, proportionality and legality.

1. *Evoluzione ed involuzione delle problematiche in tema di intercettazioni telefoniche e telematiche.* Pur se all'apparenza è datato e risalente, per una serie di ragioni disparate, diversamente recepite dai soggetti pubblici nei processi per gravi delitti di traffico internazionale di stupefacenti (esigenze di una politica criminale e processuale tanto rigorosa quanto incentivante la collaborazione) e dagli imputati sanzionati con condanne esemplari (dilatate opportunità di patteggiamento sulla pena in appello), nonché per il progressivo superamento di quella tecnologia, il tema di queste riflessioni sui modi della decriptazione dei flussi comunicativi non è mai stato affrontato in maniera appagante e risolto in modo persuasivo né dalla pur copiosa letteratura penale processuale né dalla giurisprudenza di legittimità. Si tratta di problematica pressoché inesplorata che, tuttavia, è divenuta di particolare attualità e rilevanza per effetto del Regolamento (UE) 2023/1543 e della Direttiva (UE) 2023/1544; fonti europee sopravvenute che, per essere "trasposte" in Decreto Legislativo di adeguamento e, rispettivamente, in Decreto Legislativo di attuazione, presuppongono (e impongono) la preventiva soluzione della questione di fondo della decriptazione nei modi, nei contenuti e negli effetti "interni" anche in funzione di paratie temporali predeterminate.

Oggi si discute soprattutto dei diversi problemi[1] della mancata tutela e del rischio di abusi a danno dei terzi non imputati oggetto di intercettazione[2] e dei limiti alla acquisizione dei dati elettronici trasmessi attraverso sistemi criptati come Sky-ECC, dei messaggi di testo *Whatsapp* e della loro trasmigrazione in procedimenti eterogenei[3], finanche in altri Paesi attraverso l'ordine europeo di indagine, nonché dei presupposti e dei limiti cronologici della perquisizione informatica alla luce non soltanto della oramai ben nota sentenza n. 170 del 2023 della Corte costituzionale[4] ma anche delle recentissime statuizioni della Corte Europea dei Diritti dell'Uomo di Strasburgo prima[5] e della Corte di Giustizia dell'Unione Europea del Lussemburgo poi[6]. Ma all'origine -e ne

---

* Contributo integrato e aggiornato in corso di stampa.

[1] Cfr. Cass., Sez. Un., c.c. 29 febbraio 20'24, ric. n. 3354/23, inf. provv. n. 3 del 2024; Id., Sez. Un., c.c. 29 febbraio 2024, ric. n. 31618/23, inf. provv. n. 4 del 2024; Id., Sez. I, c.c. 12 marzo 2024, dep. 3 aprile 2024, sent. n. 13535-24; Id., Sez. VI, 18 gennaio 2024, n. 2329 ord.; Id., Sez. III, c.c. 3 novembre 2023, dep. 30 novembre 20234, n. 47798 ord.

[2] Corte E.D.U., Sez. I, 24 maggio 2024, Contrada c. Italia: «...94. l'estraneo al procedimento penale, anche se si rende conto di essere stato oggetto di una misura di captazione, non dispone di alcuna via d'impugnazione che gli consenta di chiedere il controllo giurisdizionale delle intercettazioni disposte nei suoi confronti. Tuttavia, la Corte ha già affermato che privare una persona presa di mira da un'intercettazione della possibilità effettiva di impugnare retroattivamente tale provvedimento significa privarla di un'importante garanzia contro possibili abusi (*Roman Zakharov*, § 300) 95. La Corte conclude che il diritto italiano non fornisce garanzie adeguate ed effettive che tutelino dal rischio di abuso le persone oggetto di una misura di intercettazione che, non essendo sospettate di essere coinvolte in un reato né imputate, rimangono estranee al procedimento. In particolare, non è previsto che queste persone abbiano la possibilità di adire un'autorità giudiziaria per ottenere un controllo effettivo della legittimità e della necessità della misura e per ottenere, se del caso, un adeguato sollievo».

[3] Cfr. Cass., Sez. VI, c.c. 21 maggio 2024, Donnarumma, ancora non dep.; LA ROCCA, *Relazione* al Convegno su La complessità del sistema delle prove, Genova, 23 maggio 2024.

[4] Esemplarmente ROMEO, *L'insostenibile leggerezza del diritto e le nuove frontiere dell'etica dei magistrati*, in *Arch. Pen. Web*, 2024.

[5] V. Corte E.D.U., Sez. I, 15 febbraio 2024, Škoberne c. Slovenia, ove la Corte europea ha avuto cura di chiarire, tra l'altro, il profilo delle garanzie minime necessarie per evitare abusi e quello della c.d. interferenza necessaria (ed invero, al § 137 della decisione è stabilito che la legge deve indicare le garanzie di base che riguardano «...*la natura dei reati che possono dar luogo a un ordine di intercettazione; la definizione delle categorie di persone che possono essere sottoposte a intercettazione delle loro comunicazioni; un limite alla durata dell'intercettazione; la procedura da seguire per l'esame, l'uso e la conservazione dei dati ottenuti; le precauzioni da adottare per la comunicazione dei dati ad altre parti; le circostanze in cui i dati intercettati possono o devono essere cancellati o distrutti*»); cfr. anche Corte E.D.U., 9 marzo 2021, Eminağaoğlu c. Turchi.

[6] Oltre a Corte di Giustizia U.E., sent. 30 aprile 2024, nella causa C-670/22 (sulla quale v. *infra*), Il riferimento è alle sentenze 2 marzo 2021 nella causa C-746/18 (decisa in contraddittorio con i rappresentanti dei Governi estone, danese, irlandese, francese, lettone, ungherese, polacco, portoghese, finlandese e inglese ma senza la partecipazione di una rappresentanza per il governo italiano) e 7 settembre

parlavo con Giuseppe Riccio già nel 1996 allorché in un periodo di mia difficoltà personale accettò generosamente di affiancarmi a Perugia per supplenza sulla seconda Cattedra di Procedura penale- il problema di attualità era esclusivamente quello della messaggistica Blackberry.
Nella massima sintesi consentita dalla complessità dell'argomento.
Per una trentina d'anni, nella quasi totalità dei processi di criminalità organizzata e per traffico internazionale di stupefacenti, si è riproposta la questione decisiva dei modi di acquisizione e valutazione dei dati telematici relativi alle c.d. *chats pin-to-pin* che, pur intercettati dalle disparate A.G. attive nel nostro Paese, risultano criptati ed intellegibili se non con l'ausilio del sistema di decrittazione residente presso la casa-madre Blackberry (la RIM) in Canada (quello che in buona sostanza consente la trasposizione "in chiaro" di tali messaggi solo tra i due interlocutori in possesso dei rispettivi dispositivi Blackberry); in altri termini, i messaggi –criptati "all'origine"– raggiungono il *server* canadese e da questo vengono restituiti "in chiaro" al solo destinatario. Del tutto evidente come, senza il diretto intervento *a posteriori* da parte di chi detiene il sistema di decrittazione, l'intercettazione di tali messaggi scritti risulta del tutto inutile[7].
L'esperienza giudiziaria[8] ha dimostrato come il più delle volte la trascrizione "in chiaro" dei messaggi in discorso era stata acquisita (tramite una società italiana intermediaria) all'estero senza l'espletamento di attività rogatoriali, senza il rispetto di procedure che ne garantissero la genuinità e la immodificabilità, mentre la fase acquisitiva della prova deve rispettare la propria regolamentazione e il risultato probatorio deve essere controllabile e, prima ancora, tracciabile e ripercorribile (molto spesso le difese non hanno avuto neppure accesso ai *files* originali trasmessi dalla Blackberry alla società intermediaria e da questa alla A.G. ma fornendo sistemi e programmi differenti alle

---

2023 in causa C-162/22 (decisa in contraddittorio con i rappresentanti dei Governi lituano, ceco, estone, irlandese, francese, italiano, ungherese).

[7] Diffusamente COLACCHI, *Intercettazione delle comunicazioni <<pin to pin>> sugli apparecchi Blackberry: un'attività a limite dell'effettività del diritto di difesa*, in *Arch. Pen. web*, 2020; FURFARO., *Le intercettazioni "pin to pin" del sistema Blackberry, ovvero: quando il vizio di informazione tecnica porta a conclusioni equivoche*, *ivi*, 2016; ROMOLI, *Chat BlackBerry: una prima pronuncia in sede di riesame cautelare che forse ha sottovalutato alcuni profili di criticità del fenomeno*, *ivi*, 2015.

[8] Cfr. Cass., Sez. IV, 24 ottobre 2019, Solimando, n. 2246, in *ItalGiureweb*; Id., Sez. IV, 15 ottobre 2019, Brandimarte, n. 277949; Id., Sez. III, 9 maggio 2019, n. 36381, Z., *ivi*, n. 276701; Id., Sez. I, 16 novembre 2017, Mancuso, *ivi*, n. 271541; Id., Sez. IV, 8 aprile 2016, Fortugno, *ivi,* n 266983; Id., Sez. IV, 4 novembre 2015, Brandimarte*, ivi*, n. 267184.

Procure e alle difese). In altri termini e di fatto, i contenuti delle comunicazioni *pin-to-pin* criptate intercettate dall'A.G. italiana sono stati acquisiti per come decifrati (con un *ignoto* sistema di proprietà di una società straniera sul territorio straniero) ad opera di soggetti estranei alle indagini attraverso strumentazione non verificabile e non sempre usufruibile dalla difesa[9].

Se la fase di decrittazione fosse avvenuta con la stessa strumentazione, la difesa avrebbe dovuto rinvenire, con gli appositi codici funzionali alla comprensione del linguaggio informatico, le medesime funzionalità operative mentre nella realtà effettuale (tranne rare eccezioni) in alcun modo è stata posta nelle condizioni di poter interloquire nella prospettiva di una utile ripetizione e/o verifica dell'operazione di decifrazione: per l'effetto, l'opera di "trasmutazione" del dato informatico in dato "probatorio" è rimasto affidato a personale di P.G. che ha operato con ignote modalità su strumenti esclusivi alle quali – sostanzialmente– bisognerebbe approcciarsi con puro "atto di fede", nella misura in cui è rimasto inibito il controllo dell'esatta corrispondenza dell'interpretazione del dato nel passaggio da elemento grezzo a prova "in chiaro", e con ciò la verifica del processo di produzione del risultato, ovvero la "tracciabilità" della catena di conservazione del dato.

Ogni qualvolta la duplicazione, estrazione e trasmissione dei dati sia avvenuta senza alcun controllo, o comunque senza che questo controllo sia stato reso ostensibile, e dunque verificabile, per la difesa, mina qualsivoglia garanzia di intangibilità del dato telematico, in aperta violazione della normativa europea recepita in Italia con Legge 18 marzo 2008, n. 48, modificativa del codice di procedura penale, la cui *ratio legis* è quella di rendere verificabile e sempre ripetibile il procedimento di copia dei dati acquisiti. Senza il positivo accertamento delle concrete modalità di estrazione, duplicazione e conservazione dei dati, deve ritenersi interrotta e non garantita la "catena di custodia" che presuppone la conservazione dell'originale, la ripetibilità del procedimento di estrazione delle copie, la conformità delle copie all'originale mediante la cosiddetta "validazione giuridica", ovvero attraverso l'attribuzione alla copia del-

[9] Si suole ripetere acriticamente che né alla mancata messa a disposizione delle parti dell'algoritmo necessario per la messa in chiaro dei relativi dati informatici né all'attività di decriptazione di messaggi, scambiati mediante sistema Blackberry, compiuta in segreto nel corso delle indagini per mezzo della nomina di ausiliari tecnici di polizia giudiziaria e del ricorso alla spontanea collaborazione del produttore del sistema operativo, potrebbero mai non determinare alcuna lesione dei diritti di difesa: Cass., Sez. VI, 27 novembre 2018, Testa, Rv. n. 275534.

la medesima firma digitale (codice fisso contraddistinto dall'algoritmo di *hash*) generata dall'originale.
D'altra parte, una volta ammesso e pacificamente riconosciuto il diritto della difesa a ottenere i *files* integrali delle ordinarie intercettazioni telefoniche o ambientali, onde consentire il confronto di quanto captato e registrato col materiale trascritto[10], pare davvero incomprensibile negare il diritto al controllo di parte sull'operazione di decrittazione dei messaggi *pin-to-pin*, che parimenti si risolve in una (doverosa) verifica del risultato probatorio.
Pare dunque chiaro come la questione non riguardasse (e non riguardi) *soltanto* la fase di "recupero" dei dati delle *chats pin-to-pin* dal *server* straniero, con la correlata "questione rogatoria" bensì anche quella (fondamentale) della decrittazione dei messaggi, che nei casi limite finisce per essere acriticamente recepita al di fuori di ogni possibile verifica delle parti processuali, con tutte le conseguenze invalidanti a trarsene, sulla scia degli insegnamenti della Corte costituzionale[11]. Diverso, ovviamente, sarebbe il discorso nella misura in cui l'acquisizione dei dati in discorso fosse confinato nell'ambito delle intercettazioni preventivi, quelle consentite ai servizi di *intelligence* in funzione di prevenzione e contrasto dei fenomeni terroristici[12], mentre l'erosivo degrado delle garanzie è da contrastare con fermezza quando tutte le scorciatoie operative qui denunciate finiscono col refluire nel processo penale[13].

---

[10] La giurisprudenza è arroccata nel ribadire che:
a) l'acquisizione della messaggistica scambiata mediante sistema Blackberry, c.d. *pin-to-pin,* non necessita di rogatoria internazionale;
b) a nulla rileva che per "decriptare" i dati identificativi associati ai codici PIN occorra ricorrere alla collaborazione del produttore del sistema operativo avente sede all'estero;
c) la decriptazione del dato informatico contenuto nella messaggistica Blackberry è attività distinta dalla captazione e può essere svolta, ai sensi dell'art. 234-*bis* c.p.p. mediante la mera richiesta alla società produttrice del sistema operativo di trasformare, tramite apposito algoritmo, i dati informatici in contenuti intellegibili (Cass., Sez. VI, 20 aprile 2021, Civale, Rv. n. 281819);
[11] Il riferimento è a Corte cost., sent. n. 434 del 1990, che ha dichiarato l'illegittimità del secondo comma dell'art. 1 Legge n. 283 del 1962 nella parte in cui non prevedeva che –per i casi di analisi su campioni prelevati da sostanze alimentari deteriorabili– il laboratorio competente desse avviso dell'inizio delle operazioni alle persone interessate, affinché queste potessero presenziare ad esse, eventualmente con l'assistenza di un consulente.
[12] V. NOCERINO, *Le intercettazioni e i controlli preventivi. Riflessi sul procedimento probatorio*, Padova, 2019.
[13] Pare di non poco momento che nella già citata decisione Škoberne c. Slovenia la Corte sovranazionale abbia stabilito al § 136 come «*affinché un'ingerenza sia conforme al secondo paragrafo dell'articolo 8 non è sufficiente che sia capace o efficace nel perseguire lo scopo in questione, ma deve anche essere proporzionata, nel senso che stabilisce un giusto equilibrio tra gli interessi pubblici concorrenti e i diritti*

2. *Modi eterodossi di decriptazione di dati codificati e pretesa regolarità.*
Sia chiaro: ove ne sussistano le condizioni di legge, non si pone in dubbio la legittimità delle intercettazioni "a monte", cioè della captazione del dato criptato e cifrato, bensì quella della successiva acquisizione del dato "in chiaro". E in nessun modo "l'intermediazione" da parte della società italiana cambia i termini della questione: la stessa società, priva di un proprio *server*, si è sempre limitata a chiedere ed ottenere i *files* detenuti in Canada dalla "casa madre" e ad inoltrarli all'A.G italiana; sul punto è palese l'equivoco consistente nel ritenere che il sistema di cifratura adottato dalla Blackberry riguarda esclusivamente la fase della trasmissione del messaggio che, infatti, giunge al destinatario in forma decriptata, con la conseguenza che la rappresentante italiana ha correttamente trasmesso al *server* della Procura investigante i messaggi in chiaro così come essa stessa li ha recapitati al destinatario: nel sistema Blackberry la cifratura dei messaggi avviene all'origine (cioè in partenza); il messaggio non raggiunge direttamente il destinatario ma "passa" per il *server* canadese che provvede alla decrittazione e all'inoltro del messaggio "in chiaro" all'interlocutore.
Ma quel che comunque conta è che la trasmissione e decrittazione di tali messaggi sia stata posta in essere con modalità sconosciute e non verificabili, laddove la semplice trascrizione dei dialoghi ordinariamente intercettati si snoda attraverso una serie di passaggi codicistici improntati alla garanzia del (e possibilità di verifica il) risultato: dalla registrazione dei dati presso strutture giudiziarie (ovvero esterne ma debitamente "autorizzate"), all'ascolto di quanto intercettato (e redazione dei "brogliacci") da parte di personale di P.G., alla trascrizione finale dei colloqui ad opera di perito nominato dal giudice, mentre in caso di *chat pin-to-pin* dovrebbe insindacabilmente recepirsi quanto posto in essere senza alcuna possibilità di verifica da parte della difesa, sistematicamente private della copia dei dati originali.

---

sanciti dalla Convenzione (cfr. *Handyside c. Regno Unito*, 7 dicembre 1976, § 48, Serie A n. 24; *Breyer*, sopra citata, § 91; e *Szabó e Vissy c. Ungheria*, no. 37138/14, § 55, 12 gennaio 2016)». La Corte ha sottolineato la necessità che l'ingerenza sia fondata su un effettivo bisogno sociale e, in particolare, proporzionata rispetto allo scopo perseguito oltre che assistita da adeguate garanzie contro gli abusi. E allora, per dirla mutuando parole già da altri impiegate in modo efficace: «*"proporzionalità" e "controllo" sono, in estrema sintesi, i parametri dai quali si misura la "necessità democratica" che giustifica l'ingerenza nella comunicazione privata*»: FURFARO, *Un problema irrisolto: le intercettazioni telefoniche*, in *Procedura penale e garanzie europee*, a cura di Gaito, Torino, 2006, 127.

Il tema è stato affrontato nella elaborazione giurisprudenziale e superato con una certa disinvoltura in termini di nullità cedevoli in riferimento ai casi definiti con rito abbreviato[14]; di contro, non può non sottolinearsi che le sanatorie sono fenomeno che fa eccezione alla regola generale, e costituiscono un numero chiuso non dilatabile per via di interpretazione *in malam partem*. E qui non ricorre neppure l'unica ipotesi più generale del conseguimento dello scopo.

Giova osservare al proposito che il fenomeno deve essere riconsiderato integralmente nella prospettiva della invalidità patologica incarnatasi già durante le indagini preliminari e la fase cautelare. Senza trascurare che in via di principio (e soprattutto all'epoca delle captazioni a fine anni '90 e primi anni 2.000) il giudizio abbreviato incarnava una tipologia procedimentale alternativa ove la premialità aveva il suo sinallagma nella rielaborazione contratta della prova, ma non mai costituiva sanatoria non codificata delle nullità[15]. Il diritto alla prevedibilità delle decisioni (meglio noto come principio di legalità europea) àncora l'assetto processuale alle cadenze note o conoscibili all'epoca di instaurazione del rapporto processuale penale.

Chi scrive certamente non ignora l'orientamento di legittimità, invero di carattere settoriale, che fa ampio –ed eccessivo– ricorso all'istituto della sanatoria previsto dall'art. 183 c.p.p., al fine di conferire alla scelta dell'accusato il più ampio valore abdicativo nei confronti delle invalidità eccepibili, potendo sopravvivere all'opzione, sempre secondo questa esegesi, le sole nullità di carattere assoluto e le invalidità patologiche. L'orientamento di legittimità è qui evocato per dimostrare, a scanso di equivoci, la sua natura settoriale e non pertinente ai casi in discorso: al fine di prevenire letture disinvolte ed errate del dato giurisprudenziale, è essenziale chiarire che le pronunce in questione attengono, nella quasi totalità dei casi, ad invalidità "partecipative", nullità a regime intermedio relative all'intervento e alla partecipazione dell'imputato e del suo difensore e non all'idoneità probatoria delle intercettazioni non controllabili: così, ad esempio, l'omesso deposito di atti d'indagine preliminare contestualmente alla notifica dell'avviso di cui all'art. 415-*bis* c.p.p., determina una nullità di ordine generale a regime intermedio –e non una inutilizzabilità– che non può essere dedotta a seguito della scelta del giudizio abbreviato, in

[14] Cfr. Cass., Sez. IV, 24 ottobre 2019, Solimando, cit.; Id., Sez. IV, 15 ottobre 2019, Brandimarte e altri, cit.; App. Firenze, 30 maggio 2024, Marku e altri, ...

[15] Cfr. Cass., Sez. Un., 26 giugno 2014, Squicciarino, in *Cass. pen.*, 2015, 989.

quanto la richiesta del rito speciale opera un effetto sanante della nullità ai sensi dell'art. 183 c.p.p.[16]; ancora, stessa sorte per l'omessa notifica dell'avviso di fissazione dell'udienza preliminare a uno dei due difensori[17], qualora seguito da richiesta di giudizio abbreviato o, similmente, per la notifica omessa dell'avviso di conclusione delle indagini[18] o per la notificazione invalida del decreto di citazione a giudizio[19].
Pertanto, a meno di voler fare un acritico quanto errato riferimento all'orientamento evocato dal quale dedurre in maniera approssimativa che la scelta del rito abbreviato costituisca "pietra tombale" di qualsiasi invalidità[20], occorre sottolineare che nessun filone giurisprudenziale di legittimità si muove in questa direzione, trattandosi, come spiegato, di una serie di decisioni tutte legate alla partecipazione dell'indagato o imputato alla formazione dei protocolli di causa, non pertinenti in argomento, dove il mancato rilascio di copia dei supporti è strettamente legato a un problema di inutilizzabilità probatoria.

3. *Riproducibilità e verificabilità delle operazioni di decodifica dei flussi informatici originali criptati come esigenza difensiva irrinunciabile*. Una volta sufficientemente evidenziati i punti di criticità della decriptazione della messaggistica *pin-to-pin*, negando alla difesa l'accesso ai medesimi programmi dell'accusa, il tema cruciale sul quale occorre impegnarsi per una soluzione efficace, convincente e persuasiva è quello della riproducibilità/irripetibilità /verificabilità delle operazioni di decodifica dei flussi informatici originali.
Questo è un aspetto decisivo sia dal punto di vista della difesa tecnica, e sia dal punto di vista dell'organo predisposto alla decisione, che si trova ad affrontare l'identica problematica non potendo stressare e verificare debitamente l'originario elemento probatorio. Si deve muovere, infatti, dalla premessa che ciò che è stato svolto (in Canada o in Italia) non è riproducibile *esatta-*

[16] Cass., Sez. II, 10 aprile 2018, Apice e altro, Rv. n. 272901.
[17] Cass., Sez. VI, 21 giugno 2017, Aruta e altri, Rv. n. 271097; Id., Sez. II, 22 marzo 2016, Candita, Rv. n. 266748.
[18] Cass., Sez. III, 31 gennaio 2014, Laneve, Rv. n. 258813; Id., Sez. VI, 4 maggio 2010, Leotta e altri, *ivi* n. 247777.
[19] Cass., Sez. III, 27 marzo 2014, Onofrio, Rv. n. 2603377.
[20] In tal senso, inaccettabilmente, Cass., Sez. II, 24 marzo 2022, Lombardo S., n. 18245, in *ItalGiureweb*; In prospettiva provocatoria e di sintesi v. GAITO – VALENTINI, *Stato senza diritto e difesa smaterializzata: la sostanziale inutilità del diritto alla prova*, in *Arch. Pen.*, 2020, n. 3, 643 ss.

mente da parte della difesa perché qualsiasi sistema non originale o comunque differente non può assicurare il medesimo risultato.
In sintesi: è impossibile ricreare un ambiente identico nel quale replicare l'azione investigativa (una sorta di ambiente di *test*) e non è possibile per la difesa entrare in possesso dello stesso identico programma nella stessa versione senza trascurare la mancata ostensione dei flussi originali di traffico.
Epperò è diritto irrinunciabile della difesa quello di richiedere e ottenere la *verificabilità* delle azioni compiute, ossia poter contare su descrizioni dettagliate delle azioni e del comportamento del decifratore (sia automatico ovvero umano) nella vicenda concreta.
Su tale punto diventa fondamentale, anche in riferimento alla utilizzabilità o meno dei risultati della messaggistica intercettata, la modalità di raccolta dei dati una volta che viene intercettato un flusso di dati, ossia un tipo di raccolta che memorizzi i dati delle operazioni "delegate" alla R.I.M. (casa madre canadese del sistema Blackberry) con le dovute garanzie. Si pensi, ad esempio, alla possibilità di verificare chiaramente l'identità dell'agente operante ovvero del *software target* utilizzato, alla tenuta di un registro non solo delle attività effettuate dall'operatore ma anche di quelle generate autonomamente dal *software* per ognuno dei suoi moduli attivati, alla creazione di un supporto inalterabile contenente la copia dei *files* di *log* relativi a tutte le operazioni svolte, alla generazione di un secondo supporto contenente tutto il materiale acquisito durante l'indagine, sino a una descrizione dettagliata di come siano avvenute le procedure di decifrazione, mediante quali codici (e la verificabilità di cosa è successo).
Perché è irrinunciabile una verifica in termini di uguaglianza con i dati cifrati inviati dal Canada, attraverso le *passwords* ed i programmi corretti per decrittarli nonché per accertare se l'intercettazione di base è avvenuta tramite captazione del dato cifrato su infrastrutture di Operatori Italiani oppure direttamente dai *servers* della R.I.M. canadese.
Con ovvie conseguenze a trarne nell'uno o nell'altro caso.

4. *Il mancato rispetto delle regole minime per la corretta catena di conservazione dei dati originali nella esperienza giudiziaria.* Già dagli artt. 2, 13, 14 e 15 Cost. emerge chiaramente un aspetto: nella materia intercettativa non sono consentite attività che, una volta autorizzata l'intercettazione, non possano essere controllate, nel corso dello svolgimento, dall'Autorità giudiziaria e, suc-

cessivamente, con l'ostensione di tutti gli atti relativi all'intercettazione, dall'indagato[21].

Ora, i dati oggetto di duplicazione vengono conservati attraverso appositi sistemi informatici in strutture di *files* detti "dati grezzi" o RAW. A partire da questi dati, con sistemi più o meno automatizzati, si procede alla predisposizione di un brogliaccio. A differenza del dato grezzo che necessita di una interpretazione, il brogliaccio risulta direttamente leggibile e contiene le informazioni (in questo caso i testi delle *chats* intercorse in modalità *pin-to-pin*) derivanti dall'elaborazione del dato grezzo.

È il contenuto del dato grezzo -quello inaccessibile- che viene rielaborato e dunque trasformato, ed è esattamente questa trasformazione che si ritiene necessario poter ripercorrere: per quanto noto, non è stata la mancata fornitura del programma della Procura a impedire l'accesso ai contenuti del brogliaccio, ma ha inibito il controllo dell'esatta corrispondenza dell'interpretazione del dato nel passaggio da elemento grezzo a brogliaccio.

La mancata disponibilità di tale programma ha, in concreto, impedito di poter ripercorrere il processo di produzione del risultato non consentendo la tracciabilità, in funzione di controllo, della catena di conservazione del dato.

In sostanza: nei processi evocati è stato impedito alla difesa di poter fugare ogni dubbio sul fatto che nessuna anomalia informatica abbia agito sulla ricostruzione del dato, portando ad una rappresentazione dei testi –e la relativa attribuzione al *pin* mittente/destinatario– che possa essere considerata corretta ed esaustiva. E se questo diritto al controllo viene di fatto sostanzialmente eluso, non si comprende più perché sia previsto ed obbligatorio il deposito del dato grezzo al termine dell'attività di intercettazione!

Se la procedura prevista per l'intercettazione prevede il deposito anche del dato originale, è proprio perché non è del tutto assente l'ipotesi che un dato possa essere stato erroneamente interpretato o attribuito ad un utente sbagliato: il deposito del materiale originale avviene proprio a garanzia della genuinità dell'informazione, garantendo la correttezza della "catena di conservazione".

Appare chiaro che l'intervento di un soggetto intermediario, che non ha poteri di conservazione e controllo dei dati, non può provvedere a certificare la

[21] In prospettiva di sintesi v. *Riservatezza ed intercettazioni tra norma e prassi, Materiali d'esercitazione per un corso di Procedura penale* raccolti da A. Gaito, Roma, 2010.

genuinità degli stessi, prerogativa che può essere concessa esclusivamente alla società R.I.M. Canada.
L'assenza di un *server* nel territorio dello Stato determina che ai fini della rituale intercettazione delle *chats pin-to-pin* sia necessaria la cooperazione internazionale, risultando qualsivoglia altro strumento un vero e proprio *escamotage* per intercettare quello che non potrebbe essere legittimamente intercettato, e dunque incompatibile, non solo rispetto all'apprensione della prova che è formata, raccolta e custodita, nonché resa intelligibile, all'estero, ma anche con le norme a garanzia della genuinità della prova: è evidente che la mancata conservazione dei dati originali e la mancata certificazione di conformità delle copie rendono incerta e non verificabile la regolarità del procedimento di estrazione, che, al contempo, è ormai atto non più ripetibile.
Per concludere sul punto, nel classico caso di forma che diventa sostanza, solo la funzione esplicata dalla rogatoria è capace di garantire l'integrità della catena di custodia; diversamente, la stessa autenticità del contenuto delle *chats* può, e anzi deve, fondatamente essere posta in dubbio, non risultando bastevole la tranquillante certezza con cui il p.m. e i giudicanti di turno hanno rassicurato che la modalità di trasmissione dei dati dal Canada al *server* della Procura investigante, fosse avvenuta con modalità dirette che impediscono ogni manipolazione.
Insomma: l'unica cosa che rimane da fare è affidarsi all'opera altrui senza possibilità di verificare –ovvero falsificare– le operazioni unilateralmente espletate, con buona pace per l'esercizio delle attività di difesa e di assistenza dell'imputato davanti alla impossibilità di offrire una diversa versione dei fatti.
Un discorso di più ampio respiro non può prescindere, anche, dalla considerazione che l'equità di un giudizio si misura in proporzione allo spazio concesso alle parti del processo –a tutte le parti– in ordine all'introduzione ed assunzione del materiale probatorio in quanto opzione sintomatica, non solo, di un'accettabile democraticità del processo, ma anche, di un'adeguata metodologia di accertamento della verità.
Donde, nell'ordine, le "questioni" acriticamente eluse nella quotidiana esperienza giudiziaria:
a) acquisizione dei dati all'estero in assenza di rogatoria dal Canada;
b) inosservanza delle disposizioni codicistiche previste, a pena di inutilizzabilità, in materia di intercettazioni;

c) violazione dei diritti della difesa circa la verificabilità del risultato probatorio (in relazione agli artt. 178 e ss. c.p.p.).

5. Per un approccio europeisticamente orientato. Da ultimo, una digressione solo apparente, potenzialmente risolutiva.
La Corte costituzionale, con la decisione n. 239 del 15 novembre 2017, ha dichiarato non fondate le questioni di legittimità costituzionale dell'art. 360 c.p.p., «*ove non prevede che le garanzie difensive previste da detta norma riguardano anche le attività di individuazione e prelievo di reperti utili per la ricerca del DNA*», sollevate, in riferimento agli artt. 24 e 111 Cost., dalla Corte d'assise d'appello di Roma. Nella sentenza evocata, la Consulta ha ritenuto priva di fondamento la tesi del giudice rimettente secondo certe attività di acquisizione di dati, per loro natura, avrebbero caratteristiche tali da farle assimilare in ogni caso a un accertamento tecnico preventivo e da richiedere quindi le medesime garanzie difensive. Il rilievo o il prelievo di reperti utili per la ricerca del DNA –ha affermato la Corte– ha natura di atto di indagine e il suo peculiare oggetto non giustifica di per sé la sottoposizione a un regime complesso come quello previsto dall'art. 360 c.p.p.
Ad esempio, il prelievo di capelli non si differenzia dal prelevamento di altri reperti e non ci sarebbe ragione di effettuarlo con le forme stabilite per gli accertamenti tecnici. Anzi, le forme dell'art. 360 c.p.p. potrebbero assai spesso risultare incompatibili con l'urgenza, nel corso delle indagini, di eseguire il prelievo delle tracce di materiale biologico.
Del resto, come evidenziato dalla Corte costituzionale, il passaggio dalle investigazioni al dibattimento è cruciale, in quanto nel dibattimento l'imputato ha la possibilità di verificare e contestare la correttezza dell'operazione anche attraverso l'esame del personale che l'ha eseguita, oltre che dei consulenti tecnici e dell'eventuale perito nominato dal giudice. Inoltre, secondo il Giudice delle leggi, è inconferente il richiamo all'art. 117 disp. att. c.p.p., poiché questa disposizione non riguarda genericamente tanto i «rilievi» quanto gli «accertamenti tecnici», ma riguarda solo questi ultimi, e per la sua applicabilità presuppone perciò l'avvenuta individuazione della natura dell'atto.
Di assai più rilevante interesse è la seconda parte della decisione, che si è premurata di evidenziare come e perché qualora l'operazione tecnica sia particolarmente complessa e, cioè, richieda, in casi particolari, valutazioni e scelte circa il procedimento da adottare, oltre che non comuni competenze e abi-

lità tecniche per eseguirlo, allora, in questo caso –specifica la Corte costituzionale– può ritenersi che quell'atto di indagine costituisca a sua volta oggetto di un accertamento tecnico, prodromico rispetto all'altro da eseguire poi sul reperto prelevato. In tal caso, infatti, «*anche l'attività di prelievo assurge alla dignità di operazione tecnica non eseguibile senza il ricorso a competenze specialistiche e dovrà essere compiuta nel rispetto dello statuto che il codice prevede per la acquisizione della prova scientifica*»[22].

In altre parole, se l'operazione normalmente di *routine* comporta specifiche valutazioni tecniche dovranno sempre essere applicate le garanzie difensive enucleate nell' art. 360 c.p.p.: avviso all'indagato, alla persona offesa e ai difensori, nomina del consulente, riserva di incidente probatorio. È con un apprezzamento in concreto che il giudice deve stabilire se si tratti o meno di mero rilievo «esecutivo», non comportante valutazioni.

Pertanto, ove e quando le usuali operazioni di intercettazione travalichino la semplice problematica dell'instradamento, dell'ascolto o della visione o della lettura, per entrare nel terreno sofisticato della decifratura dei messaggi criptati, non si può negare che si entri nel diverso di attività non meramente esecutive che comportano l'intervento di esperti, per di più stranieri. E allora, in situazione di fatto e di diritto assolutamente identica, non ci si può discostare dal sopravvenuto insegnamento della Corte costituzionale, in quanto non si può più affermare semplicisticamente che le operazioni conseguenti ad attività di intercettazione sono tutte ugualmente semplici: quando le operazioni si discostano dall'usuale, imponendo l'interpello di esperti per elaborare il dato telematico essenziale per le indagini, allora le operazioni di decifrazione delle *chats* utili per le indagini devono essere in ogni caso assimilate a un accertamento tecnico non ripetibile. Ed in tal senso sarebbe auspicabile che fosse prospettata una nuova *questio de legitimitate*, in riferimento agli artt. 3, 24, 111 e 117 Cost., degli artt. 266-271 e 360 c.p.p., nella parte in cui non prevedono che alle operazioni collegate e conseguenti alle intercettazioni telematiche complesse si applicano le garanzie difensive previste per gli accertamenti tecnici dall'art. 360 c.p.p. così come interpretato da Corte cost., sent. n. 239 del 2017.

In questa ortodossa prospettiva si è collocata, da ultimo, la Grande Sezione della Corte di Giustizia U.E. con la sentenza 30 aprile 2024, specificamente a

[22] Cass., Sez. II, 27 novembre 2014, Santangelo, Rv. n. 261865, evocata dalla Corte costituzionale.

proposito proprio delle comunicazioni elettroniche (telefoniche e telematiche) criptate[23], puntualizzando *sub* § 105 come e perché «... *per quanto riguarda segnatamente il diritto a un processo equo, si deve ricordare in particolare che un organo giurisdizionale, qualora consideri che una parte non sia in grado di svolgere efficacemente le proprie osservazioni in merito a un elemento di prova idoneo ad influire in modo preponderante sulla valutazione dei fatti, deve constatare una violazione del diritto ad un processo equo ed escludere tale mezzo di prova al fine di evitare una violazione di questo tipo [v., in tal senso, sentenza del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche) C-746/18, EU:C:2021:152, punto 44]*».

E francamente sarebbe paradossale che le medesime attività di investigazione e di captazione di conversazioni criptate fossero meno garantite se e quando compiute interamente dai soggetti pubblici nostrani ma fossero assistite da presidi di controllo e garanzia effettivi ed apprezzabili ma unicamente se e quando rientranti nella cooperazione internazionale tra Stati, con non tollerabile inversione del rapporto di sussidiarietà tra garanzie europee minime e garanzie interne, così come sempre praticato a far data dalla storica sentenza Pupino[24].

A venire fortemente in discussione, altrimenti, sarebbero i principi di eguaglianza, di proporzionalità e di legalità.

[23] Nella causa C-670/22, in contraddittorio con i rappresentanti dei Governi tedesco, ceco, estone, irlandese, spagnolo, francese, olandese, polacco, svedese, in assenza di un rappresentante italiano.

[24] Corte Giust. C.E., sent. 16 giugno 2005, causa C-105/03 in proc. Pupino.