DALLA RIFORMA DEI TABULATI A NUOVI MODELLI DI INTEGRAZIONE FRA DIRITTI DI DIFESA E TUTELA DELLA PRIVACY

di Giulia Lasagni
(Ricercatrice in procedura penale, Università di Bologna)

1. Sostiene Edward Snowden, forse il più celebre *whistleblower* dei nostri tempi, che interrogarsi circa i regimi di *protezione* dei dati personali sia in realtà un problema fittizio. La vera questione da affrontare si trova infatti a monte: e cioè nella ingiustificata, ancora troppo diffusa, presunzione di legittimità dei regimi di acquisizione e conservazione che consentono di avere accesso a tali informazioni[1].

Nelle sue linee argomentative fondamentali, un simile approccio non è di per sé innovativo ed emerge in diversi settori del diritto. In ambito processuale, ad esempio, esaminare l'effettività delle garanzie difensive impone, in prima battuta, di porre in discussione le modalità con cui gli elementi di prova sono stati reperiti e messi a disposizione degli inquirenti.

L'affermazione citata, però, è utile ad evidenziare un elemento dirompente nel contesto attuale. Si tratta della tendenza degli interpreti di applicare, in maniera crescente, i criteri e i modelli teorici sviluppati a tal fine con riguardo al diritto alla riservatezza anche al di fuori del loro tracciato originario. Il processo penale è certamente uno degli ambiti coinvolti da questa tendenza; si pensi al caso, assai comune, in cui le informazioni che potranno assumere valore probatorio si presentano sotto forma di "dati", magari digitali[2].

* Un ringraziamento sincero va a Michele Caianiello e Isadora Neroni Rezende per i loro commenti e le loro osservazioni alle prime bozze di questo articolo.

[1] Questione, di per sé, tutt'altro che scontata, come ribadito da ultimo nel 2019: «*The problem isn't data protection; the problem is data collection [...] Regulating the protection of data presumes that the collection of data in the first place was proper, that it was appropriate, that it doesn't represent a threat or a danger. That it's okay to spy on everybody all the time whether they're your customers or whether they're your citizens, so long as it never leaks, so long as only you are in control of what it is that you've sort of stolen from everybody*», cfr. *Verdict 3incrypt*, Issue 11, Winter 2019. V. anche il dialogo online fra Edward Snowden e Max Schrems in *Privacy Provided* (26 ottobre 2021).

[2] Nozione di per sé ampia e alquanto diversificata nella sua vaghezza, cfr. N. Purtova, *The law of everything. Broad concept of personal data and future of EU data protection law*, in *Law, Innovation and Technology*, 10, 1, 2018, 40 ss; M. Gali, R. Gellert, *Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab*, in *Computer Law & Security Rev.*, 40, 2020, 1 ss; W.G. Urgessa, *The Protective Capacity of the Criterion of Identifiability under EU Data Protection Law*, in *Eur. Data Prot. L. Rev.*, 2, 2016, 521 ss.

Il fenomeno appare in tutta la sua ineluttabilità: nella "società algoritmica"[3] in cui siamo immersi, i regimi di raccolta e conservazione dei dati stanno assurgendo a chiave di lettura essenziale per misurare la portata effettiva di gran parte dei diritti fondamentali, non solo in materia di privacy.

È a partire da questa prospettiva che si possono apprezzare luci ed ombre della recente riforma della disciplina di raccolta dei dati esterni alle comunicazioni, così come risultante dalla conversione del d.l. 30.9.2021 n. 132[4].

Come noto, la novella ha interessato essenzialmente il codice della privacy e segnatamente l'art. 132, che contiene, appunto, la disciplina sulla raccolta e conservazione dei tabulati ai fini di accertamento e repressione dei reati[5]. L'assetto normativo attuale, che nella fase di conversione ha accolto gran parte dei rilievi critici sollevati dalla dottrina verso il testo iniziale[6], presenta diversi tratti innovativi e alcune lacune di non poco conto.

Il pregio principale della riforma è costituito certamente dalla predisposizione di un regime specifico per l'acquisizione dei tabulati, in precedenza rimesso in larga parte alla discrezionalità del pubblico ministero[7]. La struttura del modello disegnato, in particolare, è strettamente ricalcata su quella delle intercettazioni, sebbene con alcune differenze significative[8].

Innanzitutto, si è (nuovamente) sottratta la competenza per l'accesso ai dati al magistrato dell'accusa[9]. Quest'ultimo, quindi, oggi deve fare richiesta motivata al

[3] J.M. Balkin, *The Three Laws of Robotics in the Age of Big Data,* in *Ohio State Law Journal* 2017, 78, 1219.

[4] Convertito in legge, con modificazioni, dalla l. 23.22.2021 n. 178. Per una definizione ampia di tabulati o dati esterni alle comunicazioni, si veda C. Marinelli, *Tabulati telefonici (dir. proc. pen.)*, in *Enciclopedia del diritto. Annali*, 2010, 1122 ss.

[5] Con l'eccezione, non inerente però al tema in oggetto, del correttivo introdotto all'art. 267 Cpp e relativo al decreto che autorizza l'intercettazione tra presenti mediante inserimento di captatore informatico su dispositivo elettronico, che oggi richiede di indicare le *specifiche* ragioni che giustificano la richiesta. Cfr. la Relazione n. 67/2021 del 2 dicembre 2021 della Corte Suprema di Cassazione, Ufficio del Massimario e del Ruolo, Servizio penale, sulla Conversione in legge, con modificazioni, del decreto-legge 30 settembre 2021, n. 132, recante misure urgenti in materia di giustizia (legge 23 novembre 2021, n. 178) – in seguito indicata come "Relazione n. 67/2021", § 6.

[6] Fra cui si vedano, *ex multis*, F. Resta, *La nuova disciplina dell'acquisizione dei tabulati*, in www.giustiziainsieme.it, 2 ottobre 2021; G. Battarino, *Acquisizione di dati di traffico telefonico e telematico per fini di indagine penale: il decreto-legge 30 settembre 2021 n. 132*, in *QG* 4 ottobre 2021; C. Parodi, *Sottratto al P.M. il potere di richiedere autonomamente i tabulati*, in *il penalista* 1 ottobre 2021; A. Malacarne, *La decretazione d'urgenza del Governo in materia di tabulati telefonici: breve commento a prima lettura del D.l. 30 settembre 2021, n. 132*, in *SP* 2021; G. Pestelli, *D.L. 132/2021: un discutibile e inutile aggravio di procedura per tabulati telefonici e telematici*, in *QG* 4 ottobre 2021; M. Caianiello, *Increasing Discretionary Prosecutor's Powers: The Pivotal Role of the Italian Prosecutor in the Pretrial Investigation Phase*, in *Oxford Handbook Online on Criminology* (New York, Oxford University Press, 2016), 1 ss.

[7] Valutando in termini negativi l'innovazione invece G. Pestelli, D.L. 132/2021, *op. cit.*

[8] La possibilità di applicazione, in via analogica, il regime delle intercettazioni alla raccolta dei dati esterni delle comunicazioni è stato (sinora) escluso dalla Corte costituzionale, cfr. sentenze n. 81/1993 e 372/2006. Per una ricostruzione completa dell'evoluzione giurisprudenziale in materia, si veda A. Camon, *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Cass. pen.* 2005, 596-599.

[9] La disposizione si contraddistingue infatti per numerose oscillazioni, undici con la riforma in commento (fra cui si segnala un precedente esperimento di attribuzione della competenza al giudice, nel 2004; su cui si veda A. Camon, *L'acquisizione dei dati, op. cit.*); per una breve ma completa ricostruzione della evoluzione normativa, v.

giudice procedente, che provvederà eventualmente all'autorizzazione della richiesta con decreto motivato. Con questo intervento, si è voluta affermare la necessità di lasciare l'ultima parola in materia di trattamento dei dati esterni alle comunicazioni ad una figura di garanzia, che non rappresenti alcun interesse di parte nel procedimento.

Notoriamente, infatti, l'esercizio di una funzione pubblica di interesse generale, come quella dell'accusa, può fungere da garanzia contro eventuali abusi, ma, visto dalla prospettiva dell'indagato, ma non certo rendere neutrale l'attività del pubblico ministero[10]. In altre parole, né il principio di legalità, né il dovere generale di "ricerca della verità" anche durante la fase delle indagini[11], né lo *status* indipendente del requirente[12] valgono ad escludere la presenza di (legittimi) interessi investigativi[13]. Ciò

---

la Relazione n. 55/2021 del 13 ottobre 2021 della Corte Suprema di Cassazione, Ufficio del Massimario e del Ruolo, Servizio penale, sulle Misure urgenti in tema di acquisizione dei dati relativi al traffico telefonico e telematico a fini di indagine penale (art. 1. d.l. 30 settembre 2021, n. 132) – in seguito indicata come "Relazione n. 55/2021", 2.

[10] In tema, *ex multis*, E. Andolina, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, Milano 2008, 120-125; F. Iovene, *Data retention tra passato e futuro. Ma quale presente?*, in *Cass. pen*. 2014, 12, 4274-4282; M. Caianiello, *Poteri dei privati nell'esercizio dell'azione penale*, Torino, 2003, 25; Id., *Increasing Discretionary Prosecutor's Powers, op. cit.*, part IV; C.E. Gatto, *Il principio di proporzionalità nell'ordine europeo di indagine penale*, in *DPC* 2019, 2, 87; I. Neroni Rezende, *Dati esterni*, *op. cit.*, 190; N. Zanon, *Pubblico ministero e Costituzione*, Padova 1996, 88-89; P. Sechi, *Convalidare il sequestro probatorio da parte del p.m. non è esercizio di funzione giudicante*, in *Giur. Cost*. 2002, 2, 788; C. Morselli, *voce "pubblico ministero"*, in *Dig. Disc. Pen*., Vol. X, Torino 1995, 501; S. Sottani, *Aggiornamento alla voce "pubblico ministero"*, in *Enc. Giur. Trec.*, Tomo II 2005, 1245 e, volendo, G. Lasagni, *Tackling phone searches in Italy and in the US. Proposals for a technological re-thinking of procedural rights and freedoms*, in *NJECL* 2018, 9, 396-397.

[11] In virtù dell'obbligo di «vegliare» «alla osservanza delle leggi, alla pronta e regolare amministrazione della giustizia, alla tutela dei diritti dello Stato, delle persone giuridiche e degli incapaci», secondo l'art. 73, Regio decreto 30 gennaio 1941, n. 12, nonché di non limitare l'accertamento e i doveri di *disclosure* ai soli elementi a carico della persona sottoposta alle indagini, cfr. ad esempio, artt. 309, comma 5, e 358 Cpp.

[12] Almeno nel nostro ordinamento, nonostante le differenze organizzative che distinguono la figura del pubblico ministero da quella del magistrato giudicante (cfr., ad esempio, G. Di Federico (a cura di), *Ordinamento giudiziario. Uffici giudiziari, CSM e governo della magistratura*, Bologna 2019). La posizione dell'organo di accusa sotto questo profilo è invece assai differente in molti sistemi nell'Unione, cfr. I. Neroni Rezende, *Dati esterni*, *op. cit.*, 190. Si pensi, ad esempio, alla nutrita giurisprudenza della Corte sviluppata in materia di MAE, che ha visto i giudici del Lussemburgo esprimersi sui requisiti di indipendenza dei pubblici ministeri in Germania (Minister for Justice and Equality, 27 maggio 2019, cause riunite C-508/18 e C-82/19 PPU, commentato da T. Wahl, *CJEU: German Public Prosecution Office is not a "Judicial Authority" in the EAW Context*, in *EUCRIM* 2019, 1, 30-31), Francia (*JR e YC*, 12 dicembre 2019, cause riunite C-566/19 PPU e C-626/19 PPU), Svezia (*XD*, 12 dicembre 2019, causa C-625/19 PPU) e Belgio (*ZB*, 12 dicembre 2019, causa C-627/19 PPU), su cui si veda ancora T. Wahl, *CJEU Clarifies its Case Law on Concept of "Judicial Authority" Entitled to Issue EAWs*, in *EUCRIM* 2019, 4, 242-245.

[13] In tal senso, si è inoltre evidenziato come una visione "imparziale" dell'inquirente non potrebbe che tradursi in una sorta di "assurdità psicologica": sembra infatti inverosimile richiedere alla stessa persona fisica di svolgere al meglio le indagini, senza sviluppare, al tempo stesso, un interesse al loro esito. Sul punto si vedano P. Calamandrei, *Elogio dei giudici scritto da un avvocato*, Firenze 1954, 56; M. Caianiello, *Poteri dei privati, op. cit*., 11; F. De Leo, *Note a margine della legge sull'acquisizione e conservazione dei dati di traffico telematico*, in *Dir. Proc. Pen*. 2004, 1272. La questione tocca il complesso tema della qualificazione del pubblico ministero quale "parte imparziale", la cui trattazione merita approfondimenti ben più ampi di quelli possibili nel presente contributo; sul punto si vedano per tutti G. Vassalli, *La potestà punitiva*, Torino 1942, 170 ss; R. Orlandi, *Qualche rilievo intorno alla vagheggiata figura del pubblico ministero europeo*, in *Possibilità e limiti di un diritto penale dell'Unione europea*, a cura di L. Picotti, Milano 1999, 211, nonché, per un inquadramento alla luce dei principi costituzionali e una ricostruzione della (sinora) ambigua giurisprudenza costituzionale in materia, V. Zagrebelsky, *Indipendenza del pubblico ministero e obbligatorietà dell'azione penale,* 16-17 e M. Nobili, *Accusa e burocrazia. Profilo storico-costituzionale*, in *Pubblico ministero e accusa penale*, a cura di G. G. Conso, Bologna

è tanto più evidente quando, durante le indagini, vengono adottate misure che limitano in modo significativo i diritti dell'indagato – diritti di difesa o, come nel caso dei tabulati, anche di riservatezza.

Naturalmente, non ci si nasconde che, nella prassi, il mero intervento del giudice non vale ad assicurare, di per sé ed in ogni caso, un aumento effettivo del livello di tutela dell'indagato. Vista la sostanziale e crescente importanza dei dati in tutte le indagini penali, il rischio che tale modifica di fatto comporti solo un ulteriore passaggio burocratico di scarso valore sostanziale non è da sottovalutare[14]. Ciò nonostante, lo sforzo di coerenza compiuto dal legislatore pare andare nella direzione, apprezzabile, di adeguare il sistema normativo alle nuove sfide e ai relativi rischi posti dalla dimensione sempre più digitale della vita quotidiana e del processo penale, che richiedono sempre più una tutela effettiva in materia di dati, intensi in senso ampio.

La necessità di ricorrere all'autorizzazione del giudice procedente si applica, ai sensi dell'art. 132, comma 3, cod. priv., anche al difensore dell'indagato o imputato, della persona offesa e delle altre parti private[15]. La riforma, pertanto, ha precluso il potere di accesso diretto non solo al pubblico ministero, ma anche al difensore dell'imputato che, in precedenza, poteva invece fare leva sulla previsione di cui all'art. 391-*quater* Cpp[16]. il La disciplina riprende tuttavia dal paradigma delle intercettazioni anche la predisposizione di una procedura di urgenza, che consente al magistrato requirente la immediata acquisizione dei dati se "vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini", fatta salva la necessità di ottenere comunque una convalida dal giudice entro 48 ore dalla comunicazione del decreto[17].

1979, 118 ss. Sul lato giurisprudenziale, cfr. Cass. Sez. 3, 5.12.2002, no. 40974, Rv. 222908, Scarpa et al. (in *Arch. nuova proc. pen*., 2003, fasc. 5, 475) e, in un certo senso, anche la decisione Cass., Sez. III, 19 aprile 2019 (dep. 23 agosto 2019), n. 36380 (su cui si veda oltre, n 25).

[14] In questo senso, G. Pestelli, *D.L. 132/2021, op. cit.*

[15] Sottolineando la criticità di una tale interpretazione alla luce della normativa privacy, in quanto di fatto limitante il diritto di ogni utente di conoscere i dati esteriori delle proprie comunicazioni, A. Malacarne, *La decretazione d'urgenza*, *op. cit.*, 8-9; L. Filippi, *La nuova disciplina dei tabulati: il commento a "a caldo" del Prof. Filippi*, in *Penale, Dir e Proc* ottobre 2021, 11.

[16] Secondo il testo previgente dell'art. 132, comma 3, ultimo periodo («Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'articolo 391-*quater* del codice di procedura penale, ferme restando le condizioni di cui all'articolo 8, comma 2, lettera f), per il traffico entrante»). Sulla necessità di una modifica per ricondurre la disposizione al principio di parità delle parti, si era già espressa da tempo parte della dottrina, si veda E. Andolina, *Il potere del difensore di acquisizione diretta dei dati del traffico telefonico relativi al proprio assistito: limiti normativi e prospettive* de iure condendo, in *Arch. Nuova proc. pen*. 2018, l ss; G. Capoccia, *Tabulati telefonici: tanti dubbi sulla nuova normativa*, in *Cass. pen*. 2005, 289, da ultimi ripresi anche nella Relazione n. 55/2021, 28.

[17] V. art. 132, comma 3-*bis*, cod. priv.: «Quando ricorrono ragioni di urgenza e vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, il pubblico ministero dispone la acquisizione dei dati con decreto motivato che è comunicato immediatamente, e comunque non oltre quarantotto ore, al giudice competente per il rilascio dell'autorizzazione in via ordinaria. Il giudice, nelle quarantotto ore successive, decide sulla convalida con decreto motivato». La necessità di ripristinare una disciplina di urgenza era già stata indicata da I. Neroni Rezende, *Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di data retention*, in *SP* 2020, 5, 194.

Il secondo cambiamento radicale apportato con la legge in esame riguarda la limitazione del potere di accesso ai dati ad una gamma predeterminata di reati. Essi sono identificati, da un lato, con riferimento ad un massimo edittale non inferiore a tre anni e, dall'altro, con rimando alla determinazione puntuale di alcune fattispecie criminose e, segnatamente, alle condotte gravi dei reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono[18].

Come nel caso di intercettazioni in materia di mafia e terrorismo, oggi è inoltre richiesta la sussistenza di "sufficienti indizi di reato" per giustificare l'adozione del mezzo investigativo. L'accesso ai tabulati, in aggiunta, è limitato ai soli casi in cui ciò sia "rilevante per l'accertamento dei fatti"[19]. Quest'ultimo parametro non sembra, a ben vedere, particolarmente stringente, poiché applicabile indistintamente a tutti i tipi di richieste, senza distinguere a seconda dalla loro intrusività (e, quindi, a prescindere dalla capacità dei dati che si vuole acquisire di fornire una profilazione dei soggetti interessati).

Elemento centrale del nuovo regime, infine, è la norma di chiusura dell'art. 132, comma 3-*quater*, cod. priv., secondo la quale i dati acquisiti in violazione dei requisiti illustrati "non possono essere utilizzati". La legge di conversione, a tal riguardo, ha operato quindi un apprezzabile chiarimento rispetto al decreto-legge, allineando anche sotto questo profilo il regime dei tabulati al modello previsto per le intercettazioni[20].

Da ultimo, la normativa approvata risulta innovativa anche rispetto alla reintroduzione di una disciplina transitoria, presente nella proposta iniziale del governo, ma poi non riportata nel decreto-legge. I dati relativi al traffico telefonico, telematico e alle chiamate senza risposta acquisiti nei procedimenti penali in data precedente al 30 settembre 2021, difatti, possono essere utilizzati a carico dell'imputato solo unitamente ad altri elementi di prova ed esclusivamente per l'accertamento dei

[18] La mancanza di una definizione precisa del requisito di "gravità" è stata già criticata dai primi commentatori della riforma, cfr. per tutti G. Pestelli, *D.L. 132/2021, op. cit.* e C. Parodi, *Sottratto al PM, op. cit.,* soprattutto rispetto al reato di molestia o disturbo, la cui versione aggravata non trova gli stessi riscontri normativi della minaccia grave (artt. 339 e 612, comma 2, c.p.). A tal proposito, la Corte di cassazione ha però sottolineato come un supporto significativo può trovarsi nella Relazione illustrativa al d.d.l. di conversione (Camera dei deputati, Legislatura XVIII, A.C. 3298, 8), che fa riferimento ad una valutazione in concreto ed al principio di proporzionalità (cfr. Relazione n. 55/2021, 24), su cui criticamente L. Tavassi, *Acquisizione di tabulati, tutela della privacy e rispetto del principio di proporzionalità*, in *Arch. Pen*. 2022, 1, 11.

[19] Nella versione precedente alla conversione, il testo recitava «ove rilevanti ai fini della prosecuzione delle indagini»; formula che diversi commentatori avevano già ritenuto troppo limitativa per la implicita esclusione delle eventuali esigenze acquisitive in capo al difensore o al giudice dibattimentale, cfr. C. Parodi, *Sottratto al PM, op. cit.;* G. Amato, *Nella "costruzione" normativa si è sminuito il ruolo del Pm*, in *Guida al diritto* 2021, 39, 20. La critica è stata recepita nella legge di conversione, risultando nel testo attualmente in vigore, cfr. Relazione n. 67/2021", § 2.

[20] In origine, come noto, la disposizione si riferiva, in modo esplicito, esclusivamente al mancato rispetto dei presupposti di legge all'interno della procedura di urgenza. Come rilevato dai primi commentatori, ciò lasciava incertezze significative rispetto alla possibilità di estendere la invalidità anche in altre circostanze (ad esempio, per acquisizioni relative a reati diversi da quelli previsti). La versione finale della normativa, in tal senso, accoglie gli inviti già espressi da alcuni commentatori e dalla stessa Cassazione in commento al decreto-legge, cfr. per tutti, Relazione n. 55/2021, 30.

reati indicati nella nuova normativa[21]. Questo limite si riferisce esplicitamente solo all'utilizzo delle informazioni a carico dell'imputato[22]; la norma, quindi, sembra consentire in ogni caso un uso dei dati raccolti a favore dello stesso[23].

L'effetto retroattivo della disciplina transitoria ha consentito al legislatore di venire incontro alle esigenze di chi aveva visto i propri diritti alla riservatezza e di difesa compromessi dal regime previgente. Tale scelta, di grande impatto pratico, sembra rispondere in modo netto all'orientamento maggioritario della giurisprudenza interna, che, nonostante l'incalzare della dottrina[24] e di numerose di decisioni sovranazionali in merito, aveva sinora sminuito simili richieste[25].

2. Il nuovo articolo 132 cod. priv., infatti, si inserisce nel solco tracciato dalle due Corti europee.

Innanzitutto, dalla Corte di Strasburgo, che per prima ha delineato le condizioni essenziali per legittimare interferenze nel diritto alla riservatezza, con riferimento all'esistenza sia di una normativa nazionale prevedibile, sia di un meccanismo di controllo da parte di una autorità indipendente ed imparziale, preferibilmente di natura giudiziaria[26].

Anche nel contesto dell'Unione, l'elaborazione di un simile ventaglio di limiti al potere legislativo esprime il portato di una solida linea interpretativa. Inaugurato nel 2014 con la decisione *Digital Rights Ireland*[27], questo orientamento giurisprudenziale ha segnato la risposta alle rivelazioni sull'adozione di programmi di sorveglianza di massa da parte degli Stati Uniti anche sul territorio europeo[28]. La necessità, politica e giuridica al tempo stesso, di ribadire un livello di protezione del diritto alla privacy più elevato di quello oltreoceano, però, non ha portato immediatamente alla definizione di parametri operativi.

---

[21] Cfr. art. 1, comma 1-*bis*, d.l. 132/2021, così come modificato in sede di conversione. Sulla necessità di tale intervento, cfr. G. Battarino, *Acquisizione di dati, op. cit*. In questo senso, la legge di conversione sembra aver tolto di significato al ricorso già pregiudiziale presentato dal Tribunale di Rieti, Sezione penale, con ordinanza del 4 maggio 2021. Critico sulla disposizione e sulla sua collocazione G. Pestelli, *D.L. 132/2021*, op. cit.

[22] Né, in modo esplicito, per l'indagato; per il quale, però, può sopperire il riferimento all'art. 61 Cpp.

[23] In questo senso, v. Relazione n. 67/2021, 8.

[24] Cfr., *ex multis*, J. Della Torre, *L'acquisizione dei tabulati telefonici nel processo penale dopo la sentenza della Grande Camera della Corte di Giustizia UE: la svolta garantista in un primo provvedimento del g.i.p. di Roma*, in SP 29 aprile 2021; C. Parodi, *Tabulati telefonici e contrasti interpretativi. Come sopravvivere in attesa di una nuova legge*, in *Il penalista* 3 maggio 2021; L. Lupària Donati, *Data retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Diritto di internet* 2019, 4, 753 ss; I. Neroni Rezende, *Dati esterni*, *op. cit.*

[25] Fra cui Cass., Sez. III, 19 aprile 2019 (dep. 23 agosto 2019), n. 36380, con nota di L. Lupària Donati, *op. cit.*, 753 ss; e I. Neroni Rezende, *Dati esterni*, *op. cit.*, 183 ss. Sul punto, si veda anche la ricostruzione illustrata nella Relazione n. 55/2021, § 4.1.

[26] Cfr. *Roman Zakharov c. Russia*, 4 dicembre 2015, ric. n. 47143/06, § 233, sebbene talvolta il requisito sia stato applicato in modo non del tutto coerente dalla Corte, v. ad es. *Ben Faiza c. Francia*, 8 febbraio 2018, ric. n. 31446/12, § 69 ss (riferito all'uso dei dati esterni delle comunicazioni al "solo" fine del pedinamento elettronico).

[27] CGUE, Grande Sezione, *Digital Rights Ireland Ltd*, 8 aprile 2014, cause riunite C-293/12 e C-594/12, § 60 ss, su cui si veda, *ex multis*, S. Marcolini, *L'istituto della data retention dopo la sentenza della Corte di giustizia del 2014*, in *Cybercrime, Trattato Omnia*, diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Milano 2019, 1582 ss.

[28] Il riferimento è, soprattutto, alle rivelazioni di Edward Snowden o Chelsea Manning.

Nel 2014, con l'annullamento della cd. Direttiva Frattini e proprio in riferimento ai dati esterni delle comunicazioni, la Corte di giustizia aveva identificato nella sussistenza di un regime *ad hoc* per delimitare l'accesso alle informazioni un elemento essenziale[29]. Tuttavia, al di là delle affermazioni di principio, solo in tempi più recenti e tramite una serie di pronunce storiche, i giudici del Lussemburgo hanno iniziato a dare risposte più pragmatiche ai giudici nazionali che la interrogavano per ricercare il corretto bilanciamento fra esigenze securitarie o repressive e diritto alla riservatezza. Si è così iniziato a chiarire quali siano effettivamente i parametri di riferimento che consentono di operare la raccolta e la acquisizione dei dati entro confini di legittimità[30].

Prokuratuur, decisione esplicitamente menzionata nel preambolo del decreto-legge, rientra appieno in questo filone giurisprudenziale, prendendo posizione sia rispetto alla "qualità" della base giuridica nazionale su cui si devono fondare le operazioni di raccolta dei dati, sia in relazione ai caratteri distintivi dell'autorità competente a decidere eventuali limitazioni dei sottesi diritti fondamentali, come richiesto dall'art. 8 della Carta[31].

La riforma della disciplina dei tabulati, aprendosi a queste direttrici, ha inteso introdurre, sul piano interno, il portato garantista dell'*acquis* europeo. Il successo dell'intervento, che sarà possibile apprezzare in modo più concreto solo con la disamina della giurisprudenza di merito e legittimità, presenta però già tratti significativi su cui è possibile aprire una riflessione.

A fronte della introduzione di casi tassativi per l'utilizzo del mezzo di indagine e dell'affidamento della competenza al giudice, infatti, altri parametri devono essere considerati per misurare la portata dell'intervento legislativo.

---

[29] Ad esempio, in *Prokuratuur*, i giudici del Kirchberg avevano affermato la necessità per le normative nazionali in materia di «fondarsi su criteri oggettivi per definire le circostanze e le condizioni in presenza delle quali deve essere concesso alle autorità nazionali competenti l'accesso ai dati in questione. A questo proposito, un accesso siffatto può, in linea di principio, essere consentito, in relazione con l'obiettivo della lotta contro la criminalità, soltanto per i dati di persone sospettate di progettare, di commettere o di aver commesso un illecito grave, o anche di essere implicate in una maniera o in un'altra in un illecito del genere» (CGUE, Grande Sezione, *Procedimenti penali c. H.K* (*Prokuratuur*), 2 marzo 2021, causa C-746/18, § 50).

[30] Il percorso argomentativo si è sviluppato con una serie di pronunce della Grande Sezione: *Tele2 -Watson*, 21 dicembre 2016, cause riunite C-203/15 e C-698/15; *Ministerio Fiscal*, 2 ottobre 2018, causa C-207/16; *La Quadrature Du Net*, 6 ottobre 2020, causa C-66/18 e *Privacy International*, 6 ottobre 2020, causa C-623/17. Per una ricostruzione di tale evoluzione giurisprudenziale si veda, da ultimo, M. Catanzariti, *Procedural Rights through the Lenses of Data Protection*, 259 ss, in *Effective Protection of the Rights of the Accused in the EU Directives. A Computable Approach to Criminal Procedure Law*, a cura di G. Contissa, G. Lasagni, M. Caianiello, G. Sartor, Leiden 2022. Da ultimo, la Corte ha ribadito tali principi nella decisione *G.D. c The Commissioner of the Garda Síochána,* 5 aprile 2022, causa C-140/20.

[31] Cfr. *Prokuratuur*, § 48: «per soddisfare il requisito di proporzionalità, tale normativa deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura in questione e fissino dei requisiti minimi, di modo che le persone i cui dati personali vengono in discussione dispongano di garanzie sufficienti che consentano di proteggere efficacemente tali dati contro i rischi di abusi. Tale normativa deve essere legalmente vincolante nell'ordinamento interno e precisare in quali circostanze e a quali condizioni possa essere adottata una misura che prevede il trattamento di dati del genere, in modo da garantire che l'ingerenza sia limitata allo stretto necessario».

Da un lato, taluni profili, a partire dalla disciplina dei termini di conservazione dei dati, pur ampiamente trattati nella giurisprudenza UE, continuano a non trovare riscontro soddisfacente nel nostro ordinamento (§ 3).

Dall'altro, né la Corte di giustizia, né la legislazione UE, né quella interna sembrano aver affrontato sinora in modo soddisfacente alcuni temi centrali che emergono (anche) dall'analisi della disciplina dei tabulati e che hanno un effetto diretto nel determinare concretamente la tenuta dei diritti dei soggetti coinvolti dalle misure acquisitive (§ 4). Innanzitutto, rimane una grande incertezza su come definire il rapporto fra indagini preventive e repressive, specialmente quando l'oggetto dell'indagine sono metadati. La sovrapposizione fra questi piani nella prassi, infatti, rischia di rendere vana la distinzione giuridica su quali livelli di protezione dei diritti si applichino nei diversi casi.

In secondo luogo, nonostante la dimensione sempre più digitale del quotidiano, si registra ancora un approccio assai confuso rispetto a quali debbano essere le conseguenze di eventuali violazioni della normativa privacy nell'ambito del processo penale. L'emergere di queste criticità richiede l'adozione di soluzioni innovative: su questo fronte, la riforma dei tabulati, sebbene in modo indiretto (e forse involontario) offre qualche spunto di riflessione interessante (§ 5).

3. Prima di occuparsi di tali aspetti, però, è opportuno soffermarsi brevemente su alcuni profili rispetto ai quali la disciplina interna si discosta dagli *standard* sovranazionali, nonostante indicazioni piuttosto chiare in materia.

Innanzitutto, l'approccio *privacy-oriented* sviluppato dalla giurisprudenza europea si riferisce indifferenziatamente a tutti i soggetti interessati dall'acquisizione dei dati. Il nostro sistema, invece, non prevede invece nessun tipo di tutela particolare per i soggetti terzi a cui tali informazioni si riferiscano[32].

In secondo luogo, come già rilevato dai primi commentatori, la novella ha modificato solo parzialmente l'articolo 132 cod. priv. e, in particolare, non ha toccato la disciplina dei termini di conservazione dei dati da parte dei *service providers*[33]. Come chiarito sin da *Digital Rights Ireland*, però, la mera previsione di termini di conservazione non è di per sé sufficiente a rendere una normativa rispettosa del principio di proporzionalità, né, quindi, a legittimare automaticamente tutte le conseguenti restrizioni al diritto di riservatezza. Affinché ciò si verifichi, è necessario che questi siano previsti in modo non generalizzato e comunque adeguato al rischio specifico per cui il trattamento dei dati è stato predisposto[34].

Invece, la normativa attuale, applicabile sia a fini di indagine penale, sia alle attività di prevenzione, non sembra differenziare in modo sufficiente i termini di conservazione secondo il principio di proporzionalità [35]. La questione è particolarmente problematica soprattutto alla luce della estensione a settantadue mesi

[32] Cfr. in tal senso anche L. Tavassi, *Acquisizione, op. cit.*, 11.
[33] Cfr. per tutti, F. Resta, *La nuova disciplina, op. cit.*, § 3.
[34] *Digital Rights Ireland Ltd,* § 63 ss o, più recentemente, *Prokuratuur*, § 48.
[35] Art. 132, commi 1 e 1-*bis*, cod. priv.

della *data retention* per tutti i reati di cui agli artt. 51, comma 3-*quater*, e 407, comma 2, lettera a), Cpp[36].

Da un lato, il periodo di conservazione appare di per sé piuttosto elevato e persino più ampio di quello a suo tempo censurato nella Direttiva Frattini[37]. Dall'altro, la determinazione concreta dei termini rischia di essere rimessa ad una valutazione indifferenziata. Infatti, non potendo determinare *ex ante* per quale tipo di reato i dati potrebbero essere utilizzati, appare ragionevole ritenere che i *service providers* del settore procedano alla conservazione dei dati per il periodo più elevato previsto dalla legge, salvo eventualmente differenziare successivamente l'accesso in base alla fattispecie criminosa. Peraltro, i reati per cui la conservazione è determinata in settantadue mesi non sono necessariamente caratterizzati da un livello di gravità omogeneo e, in concreto, potrebbero dare esito a valutazioni di rischio diverse. L'allineamento della normativa interna con gli *standard* europei, quindi, avrebbe ragionevolmente richiesto una modifica anche di questi profili[38].

4. L'adeguamento alla necessità, paventata nella giurisprudenza UE in termini assai meno operativi, di restringere la possibilità di trattamento dei dati anche su base soggettiva è invece assai più complesso. L'idea sarebbe quella di limitare l'accesso soltanto ai dati di quelle persone "sospettate di progettare, di commettere o di aver commesso un illecito grave, o anche di essere implicate in una maniera o in un'altra in un illecito del genere"[39]. La realizzazione pratica di un sistema di *data retention* ispirato a tale principio, però, è tutt'altro che di facile acchito.

I principi espressi dalla Corte di giustizia, infatti, non distinguono fra indagini preventive e repressive. La considerazione è comprensibile se vista dal punto di vista del diritto alla privacy, dove il tema cruciale è quello della raccolta dei dati e del loro accesso, più che della specifica finalità per cui tali attività sono realizzate. Ciò però comporta, allo stesso tempo, difficoltà pratiche e di coordinamento di indubbio rilievo.

Difatti, mentre selezionare le persone cui i dati si riferiscono appare una operazione normale nell'ambito delle indagini penali, lo stesso non può dirsi

[36] Formalmente per implementare l'art. 20, Direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo, che, per la verità, non richiede invece nulla di specifico in merito e si limita a richiedere agli Stati Membri di adottare «le misure necessarie affinché le persone, le unità o i servizi incaricati delle indagini o dell'azione penale per i reati di cui agli articoli da 3 a 12 dispongano di strumenti di indagine efficaci, quali quelli utilizzati contro la criminalità organizzata o altre forme gravi di criminalità». Cfr., d'altro canto, l'art 132, comma 5-*bis*, cod. priv e l'art. 24, Legge 20 novembre 2017, n. 167, secondo cui «In attuazione dell'articolo 20 della Direttiva (UE) 2017/541 [...], al fine di garantire strumenti di indagine efficace in considerazione delle straordinarie esigenze di contrasto del terrorismo, anche internazionale, per le finalità dell'accertamento e della repressione dei reati di cui agli articoli 51, comma 3-quater, e 407, comma 2, lettera a), del codice di procedura penale il termine di conservazione dei dati di traffico telefonico e telematico nonché dei dati relativi alle chiamate senza risposta [...] è stabilito in settantadue mesi, in deroga a quanto previsto dall'articolo 132, commi 1 e 1-bis, del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196».

[37] In cui il termine massimo era stabilito in 24 mesi, cfr. *Digital Rights Ireland Ltd,* § 63 ss.

[38] In questo senso, si era già espresso il Garante per la protezione dei dati personali, *Parere sullo schema di decreto-legge per la riforma della disciplina dell'acquisizione dei dati relativi al traffico telefonico e telematico a fini di indagine penale*, 10 settembre 2021, § 2 e la stessa Cassazione, v. Relazione n. 55/2021, 3.

[39] *Prokuratuur*, § 50.

all'interno delle indagini preventive. Da una parte, le esigenze di prevenzione spingono per una raccolta il più ampia possibile delle informazioni potenzialmente rilevanti; dall'altra, una selezione *ex ante* dei soggetti potrebbe portare a disparità di trattamento di non poco conto. In particolare, è critica l'indicazione della CGUE di delimitare la conservazione e l'accesso ai "dati relativi ad un periodo di tempo e/o a una zona geografica e/o una cerchia di persone suscettibili di essere implicate in una maniera o in un'altra in una violazione grave"[40]. È inevitabile, infatti, che la identificazione in via preventiva di determinati gruppi di persone "a rischio", oltre ad essere piuttosto ardua in pratica, esponga a possibili discriminazioni, ad esempio su base etnica o geografica. Si assiste, in questo senso, ad un paradosso, per cui, tutto sommato, potrebbe risultare più democratico un sistema di *data retention* generalizzato a "tutti gli abbonati ed utenti iscritti e [che…] non prevede alcuna differenziazione, limitazione o eccezione in funzione dell'obiettivo perseguito"[41].

La riluttanza del legislatore ad inserire riferimenti espliciti a criteri identificativi dal punto di vista soggettivo nella riforma dei tabulati, quindi, appare assai comprensibile[42]. La questione, peraltro, si lega ad un tema classico molto più ampio, che non trova sinora una soluzione soddisfacente né nella legislazione europea, né, tutto sommato, in quella domestica: dove e come tracciare un confine fra indagini preventive e repressive[43].

La mancanza di linee di demarcazione chiare fra queste sfere di azione non è, naturalmente, solo il portato di una visione *privacy-oriented* al problema. Il fenomeno, però, oggi è osservabile in modo particolarmente evidente in tutto il dibattitto su come lo sviluppo tecnologico possa o debba essere integrato nelle attività di indagine. La ricerca di un equilibrio fra esigenze securitarie o repressive e diritti individuali in questo frangente presenta diverse impasse e contraddizioni, rispecchiate anche nella giurisprudenza europea.

Da un lato, non si può ignorare come il rendere più stringenti i requisiti di accesso ai dati ai fini dell'accertamento penale rischi di incentivare un uso ampio dei poteri preventivi di raccolta ed analisi delle informazioni. In altre parole, a fronte di immutate esigenze di acquisizione di informazioni, la formalizzazione di una via di accesso ai dati potrebbe spingere gli inquirenti a fare maggiormente leva sulle maglie, assai più flessibili, delle indagini preventive, cercando poi in qualche modo di lasciare alle regole processuali penali solo la acquisizione formale di elementi già identificati. In tal senso, vale la pena ricordare come la riforma del 2021 ha interessato solo l'acquisizione dei tabulati a fini di indagine penale, lasciando invariata invece la disciplina delle relative indagini preventive[44].

D'altro lato, anche ove sussistano disposizioni che cercano di regolamentare il passaggio di informazioni fra fase preventiva e penale, la tenuta di queste ultime è seriamente messa in difficoltà dalla molteplicità di usi a cui i dati possono essere

[40] Cfr., ad es. *Digital Rights*, § 59, *Tele 2/Watson*, § 106.
[41] Cfr., ad es. *Digital Rights*, §§ 57-58, *Tele 2/Watson*, § 105.
[42] In tal senso, anche A. Malacarne, *La decretazione d'urgenza*, *op. cit.*, 11.
[43] Sul tema, ampiamente, A. Ashworth e L. Zedner, *Preventive Justice*, Oxford 2014, 95 ss.
[44] Profilo alquanto criticato da F. Resta, *La nuova disciplina, op. cit.*, § 3.

sottoposti e dalla varietà di informazioni che da questi possono essere estratte. Il riferimento va a norme come l'art. 220 disp. att. Cpp o l'art. 132, comma 3-*quater*, cod. priv. che, come sopra illustrato, sancisce l'inutilizzabilità dei dati acquisiti in violazione dei nuovi limiti introdotti dalla riforma. Norme di questo tipo, peraltro non frequenti sul piano comparato europeo[45], rappresentano uno strumento importante per la tutela dei diritti di difesa. Esse, però, rischiano di non rappresentare una barriera sufficientemente solida a fronte di conservazioni di massa dei dati, né di offrire una risposta adeguata ai soggetti terzi coinvolti nelle operazioni di contrasto in caso di eventuali violazioni del diritto alla riservatezza.

La problematica sussiste perché considerare il diritto alla privacy come un profilo tendenzialmente recessivo alle istanze di tutela tipiche del processo penale appare una posizione sempre meno sostenibile alla luce della crescente integrazione fra analisi dei dati e attività di indagine penale[46]. In altre parole, il sistema attuale sembra troppo schiacciato sul versante di una tendenziale irrilevanza degli effetti degli atti di indagine sul diritto alla privacy. In tal senso, la disciplina dei tabulati rappresenta un punto di vista privilegiato dal quale osservare il progredire della necessità di un coordinamento fra le potenziali violazioni del diritto alla riservatezza e delle norme processuali penali.

Da una parte, tale approccio può sembrare formalmente sufficiente: in verità, non solo la prevenzione e la repressione dei reati rientrano fra gli obiettivi che giustificano una limitazione alla privacy, ma anche la legislazione sovranazionale in materia (tendenzialmente più attenta sul punto) concede in questi casi ampi spazi di discrezionalità all'azione delle autorità di contrasto. Si pensi ai limiti, assai blandi, che tutelano il diritto alla riservatezza nella Direttiva 2016/680[47] o ai margini di manovra, assai criticabili, lasciati persino nella gestione agli strumenti di Intelligenza Artificiale classificati come "ad alto rischio" nella Proposta di Regolamento in fase di negoziato[48].

D'altra parte, la possibilità di derogare in modo significativo al diritto alla privacy in nome delle esigenze repressive o securitarie si rivela sempre meno accettabile nella società democratica moderna. Ciò è tanto più evidente considerando come il livello di digitalizzazione trasformi anche le più ordinarie misure di indagine penale (come

[45] Specie in sistemi di stampo inquisitorio, su cui si veda, in generale, M. Caianiello, *Adversarial v. Inquisitorial Procedure*, in *Encyclopedia of Criminal Law and Criminal Justice*, a cura di P. Caeiro, S. Gless, V. Mitsilegas (in corso di pubblicazione), § 2.

[46] Sul tema, assai ampio e complesso, si vedano per tutti S. Rodotà, *Privacy, libertà, dignità*, Discorso conclusivo della 26a Conferenza internazionale sulla protezione dei dati; M. Orofino, *Diritto alla protezione dei dati personali e sicurezza: osservazioni e critiche su una presunta contrapposizione*, in *MediaLaws* 2018, 2, 82 ss; L. Califano, Privacy e sicurezza, in *Democrazia e sicurezza*, 3, 2013; O. Pollicino, *Costituzionalismo, privacy e neurodiritti*, in *MediaLaws* 2021, 1, 9 ss.; M. Riccardi, *Dati esteriori delle comunicazioni e tabulati di traffico. Il bilanciamento tra privacy e repressione del fenomeno criminale nel dialogo tra giurisprudenza e legislatore*, in *DPC* 2016, 157 ss.

[47] Cfr. art. 15, Direttiva (UE) 2016/680 del 27 aprile 2016 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.

[48] V. art. 6 ss, Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale, Bruxelles, 21.4.2021COM(2021) 206 final 2021/0106 (COD), su cui si veda G. Contissa, F. Galli, F. Godano, G. Sartor, La nuova Proposta di Regolamento europeo sull'intelligenza artificiale: questioni giuridiche e approcci regolatori, in *Nuove questioni di informatica forense*, a cura di R. Brighi, Roma 2022, 387 ss.

perquisizioni o ispezioni) in strumenti di potenziale profilazione verso indagati, imputati o soggetti terzi. Detto altrimenti, la polivalenza dei dati pone in luce le contraddizioni di un modello di giustizia penale che non ha ancora preso piena consapevolezza del peso rivestito dal diritto alla privacy all'interno dei propri meccanismi di accertamento.

La necessità di fornire una "tutela effettiva"[49] anche a questi profili, invece, impone l'elaborazione di nuovi paradigmi strutturali nel processo penale o ad integrazione di esso. In altre parole, emerge il bisogno di stabilire procedure innovative, che consentano una mitigazione degli effetti avversi anche rispetto al diritto alla riservatezza, riconducendoli a confini di maggiore tollerabilità.

5. L'esigenza di contemperare la tutela dei diritti in gioco con la necessità di non appesantire troppo lo svolgimento degli accertamenti, però, pone sfide sostanziali al modo tradizionale di svolgere le indagini. Individuare un bilanciamento soddisfacente non è un esercizio banale, né sul piano teorico, né su quello pratico, e dottrina e giurisprudenza si stanno da tempo interrogando sul tema, formulando e sperimentando diverse opzioni interpretative ed operative.

In tale contesto, ad esempio, si possono collocare le proposte di applicazione estensiva di istituti come l'accertamento tecnico irripetibile o l'incidente probatorio durante l'acquisizione di dati digitali. L'idea, in questi casi, è essenzialmente quella di trovare un punto di equilibrio fra gli interessi delle parti, attraverso una procedura partecipativa "anticipata" che, nel complesso, riduca al minimo necessario l'interferenza con i diritti fondamentali (almeno) dell'indagato[50].

Dalla riforma dei tabulati emerge un modello normativo ulteriore. Il riferimento va al novellato art. 132, comma 3-*ter*, cod. priv., che propone la figura del Garante dei dati personali come "mediatore" fra le esigenze di tutela della privacy e quelle di indagine. Secondo tale disposizione, in particolare, i "diritti dell'interessato" possono essere esercitati "anche tramite il Garante", che è tenuto ad informare l'interessato stesso "di aver eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonché del diritto [...] di proporre ricorso giurisdizionale"[51].

Ora, la disposizione in oggetto rispecchia quanto indicato all'art. 17 della Direttiva 680/2016; di per sé, quindi, essa ripropone un paradigma già presente nei meccanismi di tutela dei dati personali. L'attribuzione dell'intermediazione del Garante all'interno di una previsione che delinea un atto finalizzato all'accertamento e repressione dei reati, però, presenta tratti di interesse significativi.

---

[49] Come indicato pontualmente dalla Corte di Strasburgo nella sua giurisprudenza, cfr., ad esempio, la già menzionata decisione *Zakharov c. Russia*, § 80.

[50] Sul punto si vedano R. Brighi, M. Ferrazzano, *Digital Forensics: Best Practices and Perspective* e, volendo, L. Bartoli, G. Lasagni, *Antifraud Investigation and Digital Forensics: A Comparative Perspective*, entrambi in *Digital Forensic Evidence: Towards Common European Standards in Antifraud Administrative and Criminal Investigations*, a cura di M. Caianiello, A. Camon, Milano 2021, rispettivamente 46 ss e 227 ss.

[51] Art. 132, comma 3-*ter* in combinato disposto con l'art. 2-*undecies*, comma 3, terzo, quarto e quinto periodo, cod. priv. L'opzione ad oggi è prevista solo in via eventuale e non sostitutiva in toto delle prerogative del soggetto interessato.

De iure condendo, infatti, può valere la pena riflettere sulla possibilità di attribuire ad un soggetto terzo ed imparziale, come il Garante, il controllo di proporzionalità sulle richieste di accesso ai dati. Detto altrimenti, l'intervento del Garante potrebbe rivelarsi una soluzione apprezzabile per garantire le istanze della difesa, ponendo un limite, privo di interessi partigiani, alle pretese acquisitive degli inquirenti. In principio, questo modello potrebbe applicarsi sia nel contesto dei tabulati sia, più in generale, agli atti di indagine che prevedono l'acquisizione di dati personali (soprattutto se in formato digitale). Rispetto alla disciplina dei tabulati, però, a fronte di tale prospettiva si aprono in verità almeno due interrogativi.

In primo luogo, si potrebbe dubitare dell'utilità di un ruolo potenziato del Garante alla luce della funzione di controllo già conferita al giudice. La presenza in questo contesto di un ulteriore soggetto terzo e imparziale, infatti, potrebbe essere vista come una duplicazione superflua nella riforma del 2021.

Inoltre, non ci si può nascondere come un impiego in via massiva del Garante, in funzione di controllo su casi individuali, richiederebbe un ripensamento generale del ruolo di questo ufficio, con diverse difficoltà pratico-organizzative. Il Garante, infatti, dovrebbe dotarsi di strutture (e budget) adeguati a effettuare valutazioni più specifiche e al tempo stesso su una scala molto più ampia rispetto ai compiti attuali. Senza un tale intervento, prendere in carico l'enorme volume di richieste riguardanti i dati esterni alle comunicazioni a fini di indagine [52] risulterebbe verosimilmente insostenibile. Gli studi di settore, difatti, denunciano da tempo la generale inadeguatezza di personale e mezzi a disposizione delle autorità garanti, anche per lo svolgimento delle funzioni già loro assegnate[53].

La consapevolezza di tali criticità, però, non fa venire meno l'interesse per questo modello alternativo di tutela dei diritti individuali. Anzi, la necessità – riconosciuta da ultimo anche nel d.l. 132/2021 – di *prendere sul serio* il diritto alla privacy, non solo in quanto tale ma anche nella prospettiva del processo penale, suggerisce una motivazione per realizzare un salto di qualità nella definizione dei compiti del Garante.

Ciò potrebbe rivelarsi significativo soprattutto in contesti nei quali non è (ancora) previsto l'intervento di un'autorità giudiziaria imparziale. Si pensi, ad esempio, ai casi in cui i dati personali sono raccolti da autorità di contrasto settoriali e poi direttamente utilizzati per porre in essere misure afflittive, oltre che eventualmente comunicati a fini di indagine penale[54]. Fra tutti, particolarmente indicativo è l'ambito delle indagini preventive in materia di antiriciclaggio e antiterrorismo, ad esito delle quali le Unità di informazione finanziaria possono procedere al congelamento delle transazioni

[52] A cui si sommano anche problemi legati, per esempio, alla mancanza di formati condivisi nella fornitura dei dati, cfr. P. Reale, *I dati telefonici e telematici per l'autorità giudiziaria: la necessità di convergere su modelli di dati e procedure condivise,* in *Informatica e diritto*, XLI annata, Vol. XXIV 2015, 1-2, 333-344.

[53] Si vedano, a tal proposito, European Data Protection Board, *Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities*, 5 agosto 2021, 4 ss; Garante dei dati personali, *Relazione annuale 2020*, 241 ss: "dal 2013 si registra un trend crescente di Paesi che hanno aggiornato la propria normativa in materia di protezione dei dati; per molti Paesi la sfida principale per attuare quanto previsto dalle Privacy Guidelines resta l'insufficienza di risorse".

[54] Nonché, in ambito processualpenalistico, alle perquisizioni, almeno fino alla entrata in vigore delle direttive contenute nella Riforma Cartabia (su cui si veda oltre, sub § 6).

finanziarie[55]. In questo campo, infatti, i flussi informativi avvengono oggi per lo più all'interno di quadri normativi flessibili, che consentono un grande margine di discrezionalità alla parte pubblica e offrono tutele assai limitate, se non nulle, ai privati coinvolti[56].

In simili procedimenti, la valorizzazione del ruolo del Garante tramite l'assunzione di compiti di tutela particolari (*case-by-case*), sostenuti dalla creazione di uffici specializzati all'interno dello stesso, sembra un'ipotesi da non scartare[57]. Il potenziamento dell'Autorità, detto altrimenti, potrebbe rappresentare una soluzione interessante per sopperire alle carenze di un sistema globalmente ancora troppo poco attento alle sovrapposizioni, sempre più frequenti, del diritto alla privacy con i diritti di difesa e del giusto processo.

6. I numerosi aspetti innovativi della riforma spingono infine ad una ultima considerazione, già sollevata in precedenza da parte della dottrina e da taluna giurisprudenza europea e che però, anche a seguito del d.l. 132/2021, continua a rimanere in ombra: ha ancora senso distinguere nel livello di tutela fra contenuto e dati esterni alle comunicazioni?

Da tempo gli interpreti più attenti sottolineano come i rischi derivanti dall'analisi dei dati, specie se su larga scala o con tecniche di cosiddetta *data mining*, possono produrre violazioni non meno rilevanti della captazione del contenuto delle comunicazioni[58]. Paradossalmente, si potrebbe anzi sostenere che, in principio, la persona media è in grado di misurare le proprie affermazioni all'interno delle comunicazioni verbali (anche se naturalmente il contesto può rendere l'operazione più

[55] In Italia, l'Unità di informazione finanziaria, collocata presso la Banca d'Italia, v. UIF, *Rapporto annuale 2020*, Roma, maggio 2021, secondo quanto previsto dall'art. 6, comma 7, let. c), D. lgs. 21 novembre 2007, n. 231 (Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione).

[56] B. Vogel, *Reinventing EU Anti-Money Laundering. Towards a Holistic Legal Framework*, in *National and International Anti-Money Laundering Law. Developing the Architecture of Criminal Justice, Regulation and Data Protection*, a cura di B. Vogel, J-B. Maillart, Cambridge – Antwerp – Chicago 2020, 881 ss. Sulle difficoltà delle autorità di settore nel far fronte al crescente numero di segnalazioni, i rischi di sanzioni indirette sui privati (cd. *de-risking*) e sulle più recenti proposte di adeguamento complessivo del sistema nel nostro ordinamento, si veda, volendo, G. Lasagni, *Public Private Partnerships nell'antiriciclaggio e antiterrorismo: una nuova forma di Outsourcing del processo penale?, in Riv. Trim. Dir. pen.* 2021, 3, 153-167.

[57] Di per sé, un ruolo generale del Garante è comunque previsto dalla Direttiva 680/2016 o dal GDPR, ma le possibilità di intervento ivi previste sono assai diverse, almeno nel loro attuale dispiego, dall'esercizio di funzioni di controllo individualizzanti e specializzate nel senso sopra illustrato.

[58] Cfr. da ultimo I. Neroni Rezende, *Dati esterni*, *op. cit.*, 194 ss. In tal senso si veda anche Corte EDU, *Big Brother Watch c. Regno Unito*, 13 settembre 2018, ric. n. 58170/13, 62322/14 e 24960/15, § 356: «*In addition, the Court is not persuaded that the acquisition of related communications data is necessarily less intrusive than the acquisition of content. For example, the content of an electronic communication might be encrypted and, even if it were decrypted, might not reveal anything of note about the sender or recipient. The related communications data, on the other hand, could reveal the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. In bulk, the degree of intrusion is magnified, since the patterns that will emerge could be capable of painting an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with*».

difficile, in pratica). Lo stesso però non può dirsi con riguardo al *digital trail* lasciato dall'utilizzo dei numerosi *devices* che caratterizzano la nostra vita quotidiana: a meno di particolari competenze informatiche (e talvolta anche nonostante ciò), infatti, la produzione di metadati è un fenomeno che, per l'utente medio, si pone essenzialmente al di fuori della propria sfera di controllo. Considerando quante informazioni, spesso individualizzanti e utilizzabili a fini di profilazione, possono essere estratte da tali tracce, le ragioni per ritenere che i metadati possano essere soggetti ad un regime di tutela inferiore rispetto a quello previsto per le intercettazioni sembrano quindi progressivamente sgretolarsi.

In tal senso, la riforma dei tabulati rappresenta un passo nella giusta direzione, ma non un punto di arrivo in termini di ripensamento sistematico e coerente dell'apparato di garanzie. Ad esempio, non si vede perché l'intervento del giudice, invece del pubblico ministero, debba applicarsi solo alla raccolta dei dati esterni delle telecomunicazioni e non anche ad altri tipi di dati, potenzialmente altrettanto o anche maggiormente sensibili (si pensi, ad esempio, a dati clinici o relativi a transazioni finanziarie). Esigenze di tutela analoghe, peraltro, sembrano emergere anche rispetto ad altri atti di indagine, soprattutto concernenti la dimensione virtuale (si pensi, ad esempio, alle perquisizioni o ispezioni online o al monitoraggio in tempo reale dei dati finanziari), in cui le possibilità di ledere in modo sostanziale i diritti dei soggetti interessati sono particolarmente elevate[59].

La tendenza a concentrarsi sui singoli istituti, invece di guardare alla dimensione sistemica del problema, peraltro, sembra ritrovarsi anche in altri interventi normativi recenti. Nella legge delega della riforma Cartabia, ad esempio, si riscontra un altro caso in cui il legislatore ha ritenuto di sottoporre l'operato del pubblico ministero al vaglio del giudice. La disposizione deriva dalla censura mossa all'Italia dalla Corte EDU nel noto caso *Brazzi*, in cui, fra altri motivi, il nostro paese veniva condannato proprio per la mancanza di un meccanismo di controllo imparziale nel caso di perquisizioni non seguite da sequestro[60]. In questo contesto, che naturalmente può includere anche casi di acquisizione di dati, il progetto di riforma mira ad introdurre il diritto della persona sottoposta alle indagini e dei soggetti interessati di proporre opposizione al giudice per le indagini preliminari avverso il decreto di perquisizione[61]. Anche questa proposta, quindi, pur apprezzabile di per sé, si limita a sanare una lacuna relativa ad una situazione specifica, senza prendere una posizione chiara sul quale sia (o debba essere) l'approccio del nostro sistema rispetto all'acquisizione di dati a fini di indagine penale.

L'entità del problema, naturalmente, non rende semplice definire una soluzione coerente dal punto di vista sistematico. Ciò non toglie che approcci diversi da quelli attualmente adottati possano essere esplorati.

---

[59] Cfr., volendo, G. Lasagni, *Banking Supervision and Criminal Investigation. Comparing the EU and US Experiences*, Cham 2019, 339 ss.

[60] *Brazzi c. Italia*, 27 settembre 2018, ric. n. 57278/11, §§ 48 e 50. Tale condizione, peraltro, è rimasta invariata anche nella più recente giurisprudenza EDU in materia di *mass surveillance* che, per altri versi, si è invece distanziata, almeno in linea di principio, dalle decisioni della Corte di giustizia, cfr. per tutti Grande Camera, *Big Brother Watch c. Regno Unito,* 25 maggio 2021, ric. n. 58170/13, 62322/14 e 24960/15, § 351 ss.

[61] Art. 1, comma 24, L. 134/2021, menzionando esplicitamente la decisione *Brazzi c. Italia*.

Ad esempio, invece di attribuire un grado di tutela differenziato in base al binomio contenuto/dato esterno, si potrebbe assumere a parametro di riferimento il livello di intrusione nella vita privata dei soggetti interessati[62]. Seguendo questo approccio, una eventuale differenziazione fra modelli di tutela si avrebbe piuttosto fra captazione di informazioni (contenuto o metadati) *ex post* e captazione in tempo reale; nel secondo caso, infatti, l'acquisizione informativa è tendenzialmente segreta e perdura nel tempo, con pregiudizio più intenso verso i diritti dei soggetti interessati. Ad oggi, una prospettiva simile trova in Italia solo un limitato riscontro sul piano normativo[63]. In particolare, il riferimento potrebbe andare a quanto previsto all'art. 20 del decreto di recepimento della Direttiva OEI, relativo al monitoraggio in tempo reale dei dati[64]. Secondo tale disposizione, infatti, l'atto di acquisizione in tempo reale dei dati bancari, che non trova altrimenti una disciplina specifica nel nostro ordinamento, può essere eseguito su richiesta di uno Stato membro secondo le modalità previste dagli artt. 266 ss Cpp[65].

Sebbene in un frangente ancora limitato, l'estensione del regime delle intercettazioni al monitoraggio in tempo reale dei dati sembra corroborare la possibilità di superare finalmente la distinzione fra contenuto e metadato, adottando un modello che pare più aderente alle necessità delle società digitali moderne. La riforma dei tabulati del 2021 può essere letta come un ulteriore passo in quella direzione che, ci si augura, venga finalmente condiviso anche dalla giurisprudenza interna.

---

[62] F. Nicolicchia, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in *DPC* 2018, 1-17; Id., *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Milano 2020, 57 ss e, volendo, G. Lasagni, *Banking Supervision*, *op. cit*., 327 ss.

[63] La situazione non è molto diversa sul piano giurisprudenziale. A fronte di pronunce costituzionali (risalenti) che sinora hanno escluso una equiparazione fra contenuto e dati esterni alle comunicazioni (v. *supra*, n 8), infatti, nel 1998 le Sezioni unite avevano riconosciuto la applicabilità del regime di cui all'art. 266-*bis* Cpp anche ai tabulati (Cass., Sez. U, sent. n. 21 del 13/07/1998 (dep. 24/09/1998) Rv. 211197 - 01, *Gallieri*, annotata da G. Melillo, *L'acquisizione dei tabulati relativi al traffico telefonico fra limiti normativi ed equivoci giurisprudenziali,* in *Cass. pen*. 1992, 465 ss; R. Brichetti, *Estesa la disciplina delle intercettazioni mentre la giurisprudenza si riscopre divisa*, in *GD* 1998, 48, 60 ss; I. Calamandrei, *Acquisizione dei dati esteriori di una comunicazione ed utilizzazione delle prove cosiddette incostituzionali*, in *Giur. it*. 1999, 8, 1691 ss). Già nel 2000, però, le stesse Sezioni unite tornavano sui propri passi, propendendo per l'applicabilità del solo art. 256 Cpp in caso di dati esterni alle comunicazioni (Cass., Sez. U, sent. n. 16 del 21/06/2000 Ud. (dep. 30/06/2000) Rv. 216247 – 01, *Tammaro*, annotata, per il tema qui rilevante, da F. Cassibba, *Inutilizzabilità degli atti e poteri probatori del giudice nel "nuovo" giudizio abbreviato*, in *Cass. pen*. 2001, 400 ss). Anche dopo l'entrata in vigore del cod. priv., peraltro, il coordinamento fra la disposizione di cui all'art. 265 Cpp e l'art. 132 cod. priv. rimane alquanto incerto, v. C.E. Gatto, *Il principio di proporzionalità, op. cit.,* 83 ss.

[64] D.lgs. 21 giugno 2017, n. 108 con cui il Governo ha dato attuazione alla delega ricevuta due anni prima dal Parlamento (legge 9 luglio 2015, n. 114).

[65] M. Caianiello, *L'attuazione della direttiva sull'ordine europeo di indagine penale e le sue ricadute nel campo del diritto probatorio*, in *Cass. pen.* 2018, 6, 2205 ss. Più in generale, su questo strumento di indagine anche a livello europeo, si veda, volendo G. Lasagni, *Banking Supervision*, *op. cit*., 285 ss.