ALESSANDRO MALACARNE – GAIA TESSITORE

La ricostruzione della normativa in tema di *data retention* e l'ennesima scossa della Corte di giustizia: ancora inadeguata la disciplina interna?

Lo scritto, muovendo da un esame generale dei rapporti tra sicurezza e diritti di libertà, si sofferma sull'analisi dell'evoluzione della disciplina interna ed europea in tema di *data retention*. In argomento, le numerose pronunce della Corte di giustizia dell'UE – tra le quali, da ultimo, la sentenza *G.D* del 5 aprile 2022 – consentono di mettere in luce come l'attuale normativa italiana, nonostante la recente interpolazione ad opera d.l. n. 132/2021, si riveli particolarmente carente sotto il profilo delle garanzie difensive dell'indagato.

Reconstruction of data retention legislation, yet another jolt from the Court of Justice: is the national regulation still unsatisfactory?

The article, beginning with a general examination of the relations between security and freedom rights, focuses on the analysis of the evolution of national and European regulations on data retention. On this issue, the several rulings of the Court of Justice of the EU – including most recently the G.D. judgment of 5 April 2022 – make it possible to highlight how the current Italian legislation, although the recent modification by Law Decree no. 132/2021, proves to be particularly weak in terms of the suspect's defence guarantees.

1. *Sicurezza e libertà: alla ricerca di un equilibrio impossibile?*

«Il rapporto fra sicurezza e diritti è stato sempre fondamentale nella impostazione costituzionale dello Stato garantista di derivazione liberale»[1]. Con queste parole autorevole dottrina giuspubblicistica ha posto efficacemente in luce lo stretto legame che intercorre tra la necessità di tutelare la pacifica convivenza dei *cives* e le

Pur essendo il frutto di una riflessione congiunta, i parr. 1, 4, 5 sono stati redatti da Alessandro Malacarne, mentre i parr. 2, 3 e 6 da Gaia Tessitore.

[1] VERGOTTINI, *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normativa*, in *Rivista AIC*, 2019, 4, 84.

libertà fondamentali che ogni ordinamento giuridico dovrebbe garantire ai propri cittadini.

A tal proposito, non può dubitarsi di come la sicurezza – secondo accreditate ricostruzioni dogmatiche – rappresenti un valore «superprimario»[2] che si pone quale substrato necessario di ogni collettività giuridica e, contestualmente, quale valore individuale[3] ed essenziale che incide sui bisogni della singola persona[4]. Al contempo, tuttavia, deve parimenti riconoscersi come la necessità di garantire efficacemente la *tranquillitas* collettiva possa contribuire a porre in pericolo la salvaguardia di alcune libertà fondamentali.

Sotto questo profilo, se, ad avviso di taluni studiosi, il rapporto tra diritti e sicurezza non dovrebbe essere ricostruito in termini antagonistici – poiché i valori in questione non sarebbero tra loro negoziabili[5] e, di conseguenza, bilanciabili –, è comunque possibile affermare che la limitazione dei diritti di libertà a vantaggio di esigenze di sicurezza pubblica (fenomeno, quest'ultimo, che dovrebbe avere natura eccezionale, perlomeno in un sistema basato sul primato della persona umana come quello adottato dalla nostra Carta fondamentale[6]) possa dirsi legittima solo qualora venga disposta «in modo da non compromettere i

---

[2] Così, CERRINA FERONI-MORBIDELLI, *La sicurezza: un valore superprimario*, in *Percorsi Costituzionali*, 2008, 1, 31. PINTORE, *Non c'è libertà senza sicurezza*, in *Ragion pratica*, 2018, 1, 106 parla di un «bene collettivo di valore eminente». In una differente prospettiva, v., rispettivamente ed *ex plurimis*, RUOTOLO, *Diritto alla sicurezza e sicurezza dei diritti*, in *Democrazia e Sicurezza*, 2013, 2, 1 ss.; BARBERIS, *Non c'è sicurezza senza libertà. Il fallimento delle politiche antiterrorismo*, Bologna, 2017, *passim*.

Per un'efficace *summa*, seppur sintetica, delle posizioni assunte dalla dottrina costituzionalistica sul tema della sicurezza, v. RUBECHI, *Sicurezza, tutela dei diritti fondamentali e* privacy: *nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*, in *www.federalismi.it*, 30 novembre 2016, 5 ss.; per un recente *excursus* sul versante penalistico sostanziale, cfr. FORZATI, *La sicurezza fra diritto penale e potere punitivo*, Napoli, 2020.

[3] In questo senso, v. FROSINI, *Diritto alla sicurezza e tutela delle libertà: un crinale sottile che esalta le democrazie*, in *Guida dir.*, 2005, 32, 5 ss.

[4] Il riferimento, com'è intuibile, va alla nota classificazione proposta dallo psicologo Abraham Maslow che, nella sua costruzione piramidale dei bisogni umani (*Hierarchy of Needs*), colloca la sicurezza tra i bisogni necessari alla sopravvivenza dell'individuo (cfr. MASLOW, *A Theory of Human Motivation*, in *Psychological Review*, 1943, 50, 370 ss.).

[5] CERRINA FERONI, *Sicurezza e diritti, la tutela della libertà nel "permanente stato d'eccezione"*, in *www.ildubbio.it*, 17 dicembre 2020.

[6] FORZATI, *La sicurezza fra diritto penale e potere punitivo*, cit., 324.

principi garantisti propri dello Stato costituzionale»[7] e, perciò, nel rispetto, tra gli altri, dei canoni di stretta necessità e proporzionalità.
Cercando di calare le predette considerazioni all'interno del sistema di giustizia penale (e, più nello specifico, nella procedura penale), ciò che appare davvero indubitabile è come il rapporto tra le istanze di sicurezza collettiva e la garanzia dei diritti fondamentali abbia da sempre costituto un terreno particolarmente scivoloso con il quale il Legislatore e gli interpreti sono stati chiamati a confrontarsi nell'ambito di quella delicata opera di costruzione di un modello processuale costituzionalmente orientato[8]. Il quesito al quale occorre rispondere, invero, è sempre il medesimo, e tende a riproporsi, immutato, in ogni epoca: «il bene dell'amministrazione della giustizia [...] può essere prevalente al punto da subordinarvi beni ed interessi, come quelli della difesa, della libertà personale [...], della riservatezza?»[9].
Sotto tale profilo, si ritiene di poter affermare come, sul versante processualpenalistico, il diritto alla sicurezza risulta intimamente connesso al principio di accertamento e di repressione dei reati che, sebbene non trovi espressa menzione all'interno della nostra Carta fondamentale, appare senz'altro meritevole di tutela alla luce del combinato disposto degli artt. 2 e 112 Cost[10]. La repressione ed il perseguimento delle condotte illecite, difatti, non può che considerarsi la più evidente estrinsecazione del bisogno di sicurezza, a sua volta

[7] DE VERGOTTINI, *Una rilettura del concetto di sicurezza*, cit., 71.
[8] CHIAVARIO, voce *Diritto processuale penale*, in *Enc. dir.*, *Annali IX*, Milano, 2016, 309, ove si richiama il noto concetto, di matrice tedesca, di diritto processuale penale come «diritto costituzionale applicato» (*angewandtes Verfassungsrecht*). In argomento, v, da ultimo, NEGRI, *Diritto costituzionale applicato: destinazione e destino del processo penale*, in *Proc. pen. giust.*, 2019, 2, 553 ss.
[9] Testualmente, benché in altro contesto, GIARDA, *Persistendo 'l reo nella negativa*, Milano, 1980, 10. Per una rappresentazione del procedimento penale come luogo nel quale i «diritti individuali stanno in un rapporto di costante tensione con l'esigenza di garantire l'effettività dell'iniziativa processuale e, in definitiva, con l'esigenza repressiva», v. ORLANDI, *Garanzie individuali ed esigenze repressive (ragionando intorno al diritto di difesa nei procedimenti di criminalità organizzata)*, in *Studi in ricordo di Giandomenico Pisapia*, vol. II, Milano, 2000, 552.
[10] In questo senso, CONTI, *Sicurezza e riservatezza*, in *Dir. pen. proc.*, 2019, 1572. Non si ignora, invero, come l'idea che la sicurezza collettiva costituisca un bene destinato a ricevere tutela nel processo penale sia certamente anteriore all'avvento delle costituzioni "moderne"; per una celere ma assai efficace esemplificazione delle tesi sostenute, tra gli altri, da M. Pagano, G. Romagnosi e L. Ferrajoli, v. CAPRIOLI, *Sicurezza dei cittadini e processo penale*, in *Sicurezza e diritto penale*, a cura di Donini-Pavarini, Bologna, 2011, 143 s.

manifestazione di «un interesse pubblico primario, costituzionalmente rilevante, il cui soddisfacimento è assolutamente inderogabile»[11].

Da quanto detto, non può certo ricavarsi l'assunto secondo cui il processo penale dovrebbe essere concepito in termini repressivi[12]: esso, com'è noto, ha finalità cognitive, atte a tutelare, nel rispetto delle garanzie individuali (che, in questo senso, costituiscono il limite all'operatività del potere pubblico punitivo[13]), l'accertamento giurisdizionale del fatto di reato. Il processo penale, cioè, ha «il compito di proteggere l'imputato», assurgendo in tal modo a «mezzo di difesa e di tutela»[14] di quest'ultimo.

Se quanto detto appare indubitabile, è appena il caso di notare, tuttavia, come il rito criminale, legandosi intimamente al "dovere di punire", costituisce l'unico strumento idoneo a consentire la realizzazione di quella funzione "incriminatrice" propria del diritto penale sostanziale; di talché, esso, com'è stato autorevolmente osservato, concorre ad assolvere, sebbene indirettamente, una finalità di difesa sociale-collettiva[15].

Tali considerazioni introduttive, sebbene di carattere generale, risultano imprescindibili allorquando si intenda prendere in esame il complesso rapporto che intercorre tra l'interesse alla persecuzione penale e la legittima pretesa di ogni cittadino alla tutela della vita privata (artt. 2 Cost. e art. 8 C.E.D.U.), nonché della segretezza delle proprie comunicazioni (art. 15 Cost.), quali libertà dei

---

[11] Così, Corte cost., n. 366 del 1991.

[12] Come ricorda ORLANDI, *Garanzie individuali ed esigenze repressive*, cit., 555, n. 14 «l'esigenza repressiva trova la propria principale affermazione nel diritto penale sostanziale, non in quello processuale». V. anche LA ROCCA-GAITO, *Il "controlimite" della tutela dei diritti processuali dell'imputato: visioni evolutive dalle Corti europee tra legalità e prevedibilità*, in *questa Rivista*, 2019, 6, secondo i quali «la funzione del rito penale non è affatto quella di compartecipazione dell'obiettivo sanzionatorio».

[13] CORDERO, *Procedura penale*, Milano, 1983, 584.

[14] Testualmente, SABATINI, *Principi di diritto processuale penale*, vol. I, Catania, 1948, 33.

[15] In questi termini, GREVI, *Garanzie individuali ed esigenze di difesa sociale nel processo penale*, in *Garanzie costituzionali e diritti fondamentali*, a cura di Lanfranchi, Roma, 1997, 261 s. Nel distinguere tra «scopi generali» e «scopi specifici» del processo penale, la dottrina, nelle more del vecchio codice, identificava lo «scopo generale mediato» proprio «con lo scopo del diritto penale come quello che è diretto alla realizzazione dello stesso, onde è qui pure la difesa sociale, in ampio senso intesa, contro la delinquenza» (così, FLORIAN, *Principi di diritto processuale penale*, II ed., Torino, 1932, 52). È muovendo da simili considerazioni, peraltro, che deriverebbe la necessità di tutelare il processo penale «con mezzi che [...] possono risolversi in più o meno intensi doveri di sopportazione imposti ai singoli e in più o meno drastiche compressioni di diritti individuali» (ORLANDI, *Garanzie individuali ed esigenze repressive*, cit., 554).

singoli individui che, trasfuse nel procedimento penale, assumono una consistenza di particolare vigore, specialmente in una società nella quale il ricorso a strumenti a contenuto tecnologico si pone ormai quale regola fondante il quotidiano vivere comune.
Prendendo le mosse da tale inquadramento, si può osservare come il dibattito sviluppatosi sul tema abbia finito per esasperare, in maniera niente affatto condivisibile, una netta contrapposizione tra la sicurezza collettiva (*rectius*, intervento penalprocessuale repressivo) e le garanzie fondamentali della persona.
Entrambe le istanze, a ben considerare, meritano di essere prese sul serio, non foss'altro perché, in assenza della prima – come si è accennato – verrebbe meno la ragion d'essere dello stesso ordinamento statuale che, per sua natura, si fonda sulla necessità di garantire la comune e civile convivenza tra cittadini[16].
Parimenti, il diritto alla riservatezza *lato sensu* inteso, in ragione della repentina e ineluttabile evoluzione tecnologica, è divenuto ormai un pilastro delle società moderne e democratiche, imponendo riflessioni financo sulla necessità di individuare il fondamento costituzionale di "nuovi diritti", atti a tutelare in maniera più efficace le libertà dei singoli individui[17].
Se un tanto è vero, la menomazione delle suddette garanzie aprirebbe le porte ad un controllo di massa sull'intera collettività, e l'incongruenza del sistema, oltre ad essere palese, parrebbe senza alcun dubbio irragionevole: in nome di quella legittima esigenza securitaria si finirebbe per calpestare quelle stesse libertà che si vorrebbero efficacemente tutelare.
Ebbene, nella prospettiva appena evidenziata accade troppo spesso di imbattersi in «approcci sbilanciati nella direzione di una aprioristica tutela della

[16] BECCARIA, *Dei delitti e delle pene*, (1764), Parigi, 1828, 6 ss., 51.
[17] Il pensiero corre, anzitutto, ai "nuovi diritti tecnologici" coniati dalla Corte costituzionale tedesca, quali il «diritto alla garanzia della segretezza e integrità dei sistemi informatici» e, prima ancora, il «diritto all'autodeterminazione sull'uso di dati personali» (cfr., rispettivamente, BverfG, 27 febbraio 2008, in *BVerfGE 120*, 274 ss.; BverfG, 15 dicembre 1983, in *BVerfGE 65*, 1 ss.), nonché, più di recente, all'idea, avanza in dottrina, di un «diritto all'intangibilità della vita digitale» (SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018, 69 ss.). In argomento, cfr., per tutti, CAPRIOLI, *Tecnologia e prova penale: nuovi diritti e nuove garanzie*, in *Dimensione tecnologica e prova penale*, a cura di Luparia-Marafioti-Paolozzi, Torino, 2019, 46 ss.; ORLANDI, *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, in *Riv. it. dir. proc. pen.*, 2014, 1134 ss.

privacy»[18], liquidando «ogni istanza relativa alla sicurezza [...] come meramente "securitaria" o demagogica, e perciò solo non degna di seria attenzione»[19], senza tener conto, invece, che il bisogno di sicurezza – a determinate condizioni – ben può giustificare una limitazione delle libertà individuali, tra le quali rientrano, a pieno titolo, i diritti sanciti agli artt. 2 e 15 Cost.

Al contempo, tuttavia, non è raro assistere a "derive inquisitorie"; si tratta di quei fenomeni nei quali, cioè, la sicurezza, da pre-condizione necessaria per l'esercizio dei diritti, diviene strumento per un ingiustificato ampliamento del controllo penale[20], specialmente qualora si tratti di esaminare le ricadute processuali del ricorso ai nuovi mezzi tecnologici di ricerca della prova[21] ai quali, per loro stessa natura, viene comunemente attribuita una capacità euristica superiore a quella degli strumenti di prova tradizionali.

Impostato in questi termini, il dibattito non può che portare ad una polarizzazione del conflitto[22] tra due visioni estreme che, in quanto tali, appaiono entrambe prive di ragionevolezza: «garantismi inquinati» o «oltranzisti della difesa sociale»[23]?

L'alternativa è da ricercare altrove. Il nucleo del problema, ad una lettura meno superficiale, sta nell'individuare il giusto equilibrio tra esigenze di sicurezza collettiva e tutela della *privacy*, nonché della segretezza.

---

[18] Così, SIGNORATO, *Novità in tema di* data retention. *La riformulazione dell'art. 132 codice* privacy *da parte del d.lgs. 10 agosto 2018, n. 101*, in *Dir. pen. cont.*, 2018, 11, 160.

[19] Testualmente, ZANON, *Un diritto fondamentale alla sicurezza?*, in *Dir. pen. proc.*, 2019, 1557. In una prospettiva più generale, FORZATI, *La sicurezza penale fra rassicurazione sociale,* conservatio ordinum *e criminalizzazione del corpo estraneo*, in *questa Rivista* web, 31 dicembre 2018, 1 s., sottolinea come l'idea di sicurezza sia stata abbandonata «dalla dottrina penalistica nella seconda metà del secolo scorso [...], come un padre nobile di cui potersi agevolmente disfare», poiché giudicata quale «concetto tautologico e superfluo [...], condannat[o] all'oblio ed all'indeterminatezza definitoria».

[20] In questi termini, PELISSERO, *Il potenziamento delle sanzioni punitive e delle misure di prevenzione personali nel nuovo decreto sicurezza*, in *Studium iuris*, 2017, 10, 1100.

[21] Per una panoramica, v. SIGNORATO, *Le indagini digitali*, cit. Si riferisce icasticamente ai diritti fondamentali (quali, ad esempio, la riservatezza e la segretezza) come oggetto, nell'odierna società digitale, di un «"bombardamento tecnologico" in grado di annichilirli completamente», MARCOLINI, *Regole di esclusione costituzionali e nuove tecnologie*, in *Criminalia*, 2006, 389.

[22] ROJSZCZAK, *The Uncertain Future of Data Retention Laws in the EU: Is a Legislative Reset Possible?*, in *Computer Law & Security Review*, 2021, 41, 11. In una prospettiva più generale, v. PULITANÒ, *Sicurezza e diritto penale*, in *Riv. it. dir. proc. pen.*, 2009, 556.

[23] GIARDA, *Persistendo 'l reo nella negativa*, cit., 10.

A tal riguardo, si può agevolmente notare come una siffatta operazione, non solo si mostri assai complessa, ma appaia, sotto certi aspetti, destinata a sicuro fallimento, nella misura in cui l'incedere tecnologico non consente una precisa e statica determinazione di un punto di equilibrio valevole in ogni tempo e luogo[24].

L'implementazione di strumenti digitali ad alta pervasività, infatti, impone doveri di intervento al Legislatore ai quali quest'ultimo, troppo spesso, non è in grado far fronte: una sorta di "rincorsa disperata" alla normativizzazione dell'ultima tecnica investigativa che non può certamente dirsi il preludio di una disciplina efficace ed effettiva.

Ed invece, pur dovendo necessariamente soppesare l'interesse della sicurezza pubblica e l'efficacia dell'applicazione della legge penale con i diritti fondamentali e i principi dello Stato di diritto, non possiamo esimerci dal mettere in luce come entrambe le esigenze di cui si discute costituiscano «*important public interests in a democratic constitutional State*»[25].

Le brevi e rapsodiche considerazioni che precedono possono essere senz'altro calate anche nel contesto della presente trattazione.

Il fervente dibattito che ruota attorno al tema della *data retention* per finalità di prevenzione e repressione dei crimini[26] viene sovente dipinto, in effetti, come

---

[24] In tale direzione sembrano collocarsi quelle tesi che, esaminando le ricadute sul piano processuale dei nuovi mezzi tecnologici di ricerca della prova, auspicano l'introduzione di categorie probatorie generali che possano fungere da "guida" ogniqualvolta si tratti di limitare le garanzie fondamentali dei cittadini (cfr. MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen.*, 2015, 789 s.; NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*, Milano, 2020, *passim*, e NOCERINO, *Il tramonto dei mezzi di ricerca della prova nell'era 2.0*, in *Dir. pen. proc.*, 2021, 1730).

[25] ROVELLI, *Case Prokuratuur: Proportionality and the Independence of Authorities in Data Retention*, in *European Papers - A Journal on Law and Integration*, 2021, 6, 208.

[26] Sul tema, la bibliografia è ormai sterminata. Per una panoramica generale sulla disciplina interna, v., tra i contributi più recenti e senza alcuna pretesa di completezza, ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, Padova, 2018; DINACCI, *L'acquisizione dei tabulati telefonici tra anamnesi, diagnosi e terapia: luci europee e ombre legislative*, in *Proc. pen. giust.*, 2022, 2, 301 ss.; FLOR-MARCOLINI, *Dalla* data retention *alle indagini ad alto contenuto tecnologico. La tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato. Aspetti di diritto penale processuale e sostanziale*, Torino, 2022; FLOR, Data retention *e giustizia penale in Italia*, in *Diritto penale dell'informatica*, a cura di Parodi-Sellaroli, Milano, 2020, 683 ss.; RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, in *Dir. pen. cont.*, 2016, 3, 156 ss.; FILIPPI, *Riservatezza e* data retention*: una storia infinita*, in *www.penaledp.it*, 23 giugno 2022; nonché, volendo, TESSITORE, *Acquisizione*

«*a "clash" between those who seek to defend liberty and those who seek more security*»[27].

Questa visione del fenomeno, come si è poc'anzi osservato, non appare affatto convincente.

La *privacy*, al pari della segretezza, non può essere considerata alla stregua di un diritto assoluto e «tiranno»[28]; essa, come ogni libertà, vive in un sistema complesso in cui ogni diritto, compresi quelli costituzionalmente garantiti, deve essere bilanciato con principi concorrenti[29]. Le indagini penali, in questo senso, nient'altro sono se non una forma di "attentato legalizzato" ai valori della riservatezza[30] e della segretezza: il problema, casomai, è individuarne i presupposti e i limiti.

Parimenti, la crescente consapevolezza circa l'esistenza di pratiche di conservazione in massa di "informazioni collaterali" legate alle comunicazioni telefoniche e telematiche – in base alle quali possono essere registrati i dati di persone che neppure sono sospettate di aver commesso gravi reati[31] – dovrebbe indurre a riflettere con maggior attenzione sulla compatibilità di simili strumenti con la presunzione di innocenza[32], nella sua peculiare declinazione di regola

---

dei tabulati telefonici e privacy: *l'interpretazione della Corte di Cassazione e le ultime modifiche normative*, in *Proc. pen. giust.*, 2022, 2, 472 ss. Sul versante costituzionale, si rinvia all'approfondita analisi di FORMICI, *La disciplina della* data retention *tra esigenze securitarie e tutela dei diritti fondamentali. Un'analisi comparata*, Torino, 2021.

[27] Così, JUSZCZAK-SASON, *Recalibrating Data Retention in the EU. The Jurisprudence of the CJEU – Is this the End or the Beginning?*, in *Eucrim*, 2021, 4, 259.

[28] Il riferimento, com'è noto, va a Corte cost., n. 85 del 2013.

[29] Cfr. PISTORIO, *La sicurezza giuridica. Profili attuali di un problema antico*, Napoli, 2021, 136 ss.

[30] CENTORAME, *Le indagini tecnologiche ad alto potenziale intrusivo fra esigenze di accertamento e sacrale inviolabilità dei diritti della persona*, in *Riv. it. dir. proc. pen.*, 2021, 501.

[31] Si pensi, ad esempio, al cd. caso *Pegasus*, *malware* utilizzato in taluni ordinamenti per tracciare e intercettare attivisti per i diritti umani, giornalisti, avvocati e politici (cfr. PRIEST-TIMBERG-MEKHENNET, *Private Israeli spyware used to hack cellphones of journalists, activists worldwide. NSO Group's Pegasus spyware, licensed to governments around the globe, can infect phones without a click*, in *www. washingtonpost.com*, 18 luglio 2021). Per un approfondimento, v. ROJSZCZAK, *EU Criminal Law and Electronic Surveillance: The Pegasus System and Legal Challenges It Poses*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2021, 29, 290 ss.

[32] Cfr. MILAJ-MIFSUD BONNICI, *Unwitting Subjects of Surveillance and the Presumption of Innocence*, in *Computer Law & Security Review*, 2014, 419 ss.; STOYKOVA, *Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence*, in *ivi*, 2021, 42, 4 s. Più in generale, cfr. anche LUPARIA, *La presuncion de inocencia en la Carta de los derechos fundamentales de la Union Europea*, in *Revista Vasca de Derecho Procesal Y Arbitraje*, 2017, 2, 199.

trattamentale e, più in generale, sul delicato rapporto tra sicurezza e diritti individuali di libertà. Questi ultimi, manifestazione di principi generali e sovente qualificati in termini di "inviolabilità", non possono essere elisi *in toto*, neppure per far fronte ad esigenze repressive, ancorché eccezionali o contingenti.
Tale considerazione ben pare giustificarsi alla luce della moderna ed attuale esegesi offerta del concetto di *privacy*: lungi dall'essere interpretato come un mero «*right to be let alone*»[33], il diritto alla riservatezza ha subito una profonda evoluzione, che, com'è noto, ne ha ampliato la portata applicativa.
Da una dimensione essenzialmente negativa (diretta, cioè, ad escludere terzi dalla propria sfera privata), si è giunti ad affermare l'esistenza di un vero e proprio *habeas data*[34], espressione di un generale diritto al monitoraggio e al controllo sui propri dati personali.
Quest'ultima esigenza, come si può agevolmente constatare, si è fatta sempre più pressante in una società nella quale la raccolta e l'elaborazione massiva di informazioni costituisce ormai la prassi in ogni attività umana connotata dall'impiego di strumenti tecnologici. Il crescente ricorso a tecniche informatizzate che consentono di produrre un'immensa quantità di informazioni, d'altro canto, non poteva non riflettersi sulla nascita di un corrispondente diritto del singolo cittadino a «governare i dati che intimamente lo riguardano»[35].
Sennonché, il processo penale, quale macchina che, per sua stessa natura, «si "nutre" di informazioni»[36], contribuisce a mettere in serio pericolo l'effettivo esercizio di siffatto diritto.
Il timore che si va facendo strada (se di semplice timore si può ancora parlare), in effetti, è che i dati, da "croce e delizia" del processo penale, si stiano ma mano tramutando in strumenti per limitare le garanzie del singolo individuo.
Ne deriva, di riflesso, la necessità che la legge penal-processuale – dando così concreta attuazione al diritto di governare il "passato, il presente e il futuro" dei propri dati – assicuri ad ogni indagato la più ampia operatività di quei «diritti

[33] Secondo la nota definizione offerta dai "padri" della *privacy*, WARREN-BRANDEIS, *The Right to Privacy*, in *Harward Law Review*, 1890, 4, 193.
[34] Per un'ampia trattazione del tema, anche in una prospettiva europea, v. PÉREZ-LUÑO ROBLEDO, *El procedimiento de Habeas Data. El derecho procesal ante las nuevas tecnologías*, Madrid, 2017.
[35] Efficacemente, LUPARIA, Privacy, *diritto della persona e processo penale*, in *Riv. dir. proc.*, 2019, 1464.
[36] ORLANDI, *Il processo nell'era di* internet, in *Dir. pen. proc.*, 1998, 140. Ovvero, come affermato da LUPARIA, Privacy, *diritto della persona e processo penale*, cit., 1455, quale «recettore di dati».

conoscitivi» che contribuiscono ad individuare la variegata «ricchezza contenutistica» del diritto di difesa, così per come sancito agli artt. 24, comma 2 e 111, comma, 3, Cost.[37].

2. *La definizione di tabulato telefonico e l'autonomia del concetto*. Negli ultimi anni il controllo sulle nostre vite è stato favorito dall'uso della tecnologia che, per la sua intrusività, come detto, consente il monitoraggio di grandi flussi di informazioni che possono contenere numerosi elementi da cui desumere abitudini, frequentazioni, geolocalizzazione, quantità e modalità di comunicazioni delle persone.
In quest'ottica, tra gli strumenti messi a disposizione per utilizzare nuove metodologie investigative, il tabulato telefonico rappresenta, di certo, uno strumento sulla cui evoluzione ha inciso fortemente l'espansione delle tecnologie.
È noto che attraverso la raccolta di dati esterni concernenti le comunicazioni (i tabulati, appunto) non si accede al loro contenuto, ma è possibile ottenere informazioni sensibili e potenzialmente disponibili per un tempo prolungato (in base alla normativa sul punto, di cui si dirà).
Anzi, a ben vedere, i tabulati possono contenere dati più significativi delle conversazioni – nelle quali, non è inusuale che si utilizzino linguaggi cifrati o si presti molta attenzione – come intensità dei contatti e localizzazione del chiamato e del chiamante: aspetti che possono dire molto di più che il contenuto di una conversazione[38].
Occorre premettere che i tabulati telefonici – sulla cui disciplina di conservazione si tornerà in seguito – sono registrati e conservati dai gestori di telefonia mobile e fissa per ragioni inerenti all'attività svolta da quest'ultimi, e trattengono elementi esterni delle comunicazioni telefoniche, in quanto, come base rappresentativa esprimono dati di contatto (le utenze cui corrisponde la telefonata

[37] GAITO-VALENTINI, *Stato senza diritto e difesa smaterializzata: la sostanziale inutilità del diritto alla prova*, in *questa Rivista* web, 7 gennaio 2021, 2 s.
[38] Invero, secondo TAVASSI, *Acquisizione di tabulati, tutela della* privacy *e rispetto del principio di proporzionalità*, in *questa Rivista* web, 20 gennaio 2022, 3, la preoccupazione ha anche riguardo il fatto che «le informazioni offerte dai tabulati telefonici serbano un'altissima potenzialità euristica: dall'analisi della durata, della frequenza delle chiamate, delle utenze contattate, dei siti *internet* visitati, della permanenza in una data area geografica, possono ricostruirsi in dettaglio i comportamenti di un individuo, magari del tutto estraneo alla vicenda processuale».

intercorsa, se una chiamata è di entrata o di uscita, la durata del colloquio, la data e l'ora della telefonata, da quale luogo è stata effettuata o ricevuta, se fra le utenze il contatto è di natura sporadica o frequente) che possono essere utili in un determinato e specifico contesto probatorio[39].
È evidente che l'acquisizione probatoria di questi dati non può che avvenire attraverso il supporto cartaceo o informatico che riveste la struttura e la funzione del documento[40]. Epperò, questa risoluzione semplificatrice delle problematiche relative all'acquisizione di quel tipo di dato ha comportato un lungo dibattito sulla necessità o meno di estensione delle stesse tutele di altri istituti *simili* in quanto, per stabilire i limiti acquisitivi, si classificava il tabulato come documento, con le relative regole di acquisizione probatoria, sia in fase investigativa che, successivamente, dibattimentale.

2.1. *Gli approdi costituzionali per il riconoscimento di garanzie "minime"*. Il riconoscimento di adeguate garanzie, trattandosi di strumento incidente su diritti tutelati a livello costituzionale quali la riservatezza e la segretezza delle comunicazioni, ha richiesto un complesso e costante intervento della giurisprudenza, sia costituzionale che di legittimità, con cui non si è mancato di mettere in evidenza le difficoltà interpretative in merito alla compatibilità della disciplina di acquisizione *ex* art. 234 c.p.p. ovvero di quella di cui all'art. 256 c.p.p. del tabulato.
Con riferimento alla giurisprudenza costituzionale, è possibile rinvenire una prima cauta apertura, risalente ai primi anni di entrata in vigore del "nuovo" codice di procedura penale, in cui la Corte ebbe a riconoscere – pur

[39] La definizione è di VELE, *Le intercettazioni nel sistema processuale penale. Tra garanzie e prospettive di riforma*, Padova, 2011, 60.
[40] Sulla natura documentale dei tabulati si rinvia a Cass., Sez. I, 6 giugno 1995, n. 6767, Recchia, Rv n. 202909. Già in precedenza, con la sentenza Cass., Sez. I, 3 dicembre 2003, n. 23961, Raucci, Rv n. 22898801, si riteneva che «nella fase dibattimentale l'acquisizione dei tabulati relativi ai dati esterni al traffico di una utenza telefonica può avvenire ai sensi degli artt. 495 e 507 c.p.p. e, pertanto, a mezzo di ordinanza motivata sulla utilità probatoria del giudice, cui la parte interessata abbia presentato richiesta e previa interlocuzione con tutte le parti interessate, considerando, invece, non possibile la diretta produzione in giudizio da parte del pubblico ministero. Di recente, ha tracciato la cronistoria del valore e del significato di tabulato telefonico la Suprema corte con la sentenza Cass., Sez. V, 24 febbraio 2022, n. 8968, in *D&G*, 2022, 55, 6, con commento di GRILLO, *Tabulati telefonici, quando diventano prova di un reato?*

dichiarando la questione sollevata infondata in relazione all'art. 266 c.p.p. – che la tutela alla segretezza delle comunicazioni, di cui all'art. 15 Cost., preclude alla divulgazione ovvero alla conoscibilità da parte dei soggetti estranei alla comunicazione di notizie idonee a identificare i dati esteriori della conversazione (autori, tempo e luogo della stessa) in quanto, proprio grazie alla tutela di rango costituzionale, ne consente la diffusione, in via di principio, ai soli soggetti interessati. Di conseguenza – ad avviso della Corte – pur se la tutela relativa alla riservatezza dei dati che identifichino la comunicazione non è stata oggetto di specifico intervento normativo, l'acquisizione dei tabulati come mezzo di prova deve avvenire nel rispetto delle regole costituzionali ovvero solo sulla base di un atto dell'autorità giudiziaria sorretto da adeguata motivazione, idonea a dimostrare la sussistenza in concreto di esigenze istruttorie volte al fine della prevenzione e repressione dei reati. In quell'occasione, dunque, la Corte concluse che, ferma restando la libertà del legislatore di stabilire più specifiche norme idonee a garantire i principi costituzionali, il livello minimo di garanzie individuato dalla disposizione di cui all'art. 15 Cost. si pone come parametro di validità che spetta al giudice *a quo* applicare nel caso sottoposto alla sua attenzione[41].

Non molto tempo dopo la questione di legittimità fu nuovamente proposta; questa volta facendo leva sulla incompatibilità dell'art. 267, comma 1, c.p.p. con l'art. 3 Cost. nella parte in cui la norma non prevedeva l'adozione del provvedimento autorizzativo del giudice per la rilevazione del traffico telefonico e la individuazione delle utenze chiamate, delle date e dell'ora delle conversazioni, con ciò rendendo iniquo il trattamento in caso di acquisizione, invece, di tabulati telefonici[42].

In questo caso, però, il remittente, condividendo le argomentazioni della già citata pronuncia del 1993, notò che, l'adozione del decreto autorizzativo da

[41] Corte cost., 11 marzo 1993, n. 81, in *www.cortecostituzionale.it*. In dottrina, la sentenza è stata commentata da DI FILIPPO, *Dati esteriori delle comunicazioni e garanzie costituzionali*, in *Giur. it.*, 1995, 107 ss.; DOLSO, *Ipotesi sulla possibilità di un diverso esito utilizzando il parametro della "ragionevolezza"*, *ivi*, 1993, 2111 ss.; POTETTI, *Corte costituzionale n. 81/93: la forza espansiva della tutela accordata dall'art. 15 comma 1 della Costituzione*, in *Cass. pen.*, 1993, 2746 ss.

[42] Corte cost., 17 luglio 1998, n. 281, in *Giur. it.*, 1999, 2006 ss., con nota di LONGO, *Il regime processuale dei dati esterni alla comunicazione: un problema ancora aperto*. La sentenza è stata commentata con favore da DI CHIARA, *Osservazioni a Corte cost. 17 luglio 1998, n. 281*, in *Foro it.*, 1999, 433 ss.

parte del pubblico ministero era idonea a soddisfare il parametro costituzionale di cui all'art. 15, comma 2, Cost. nel quale si prescrive la necessità di un provvedimento motivato dell'autorità giudiziaria, con ciò comprendendo anche il pubblico ministero[43]; e però, non anche quello dell'art. 3 Cost. sotto il profilo della parità di trattamento in quanto il valore della segretezza, leso sia dall'acquisizione dei tabulati che dalle intercettazioni, pure qualificato come inviolabile dalla Costituzione, non sarebbe suscettibile di differenziate e graduate guarentigie, come invece avviene nel caso dei due specifici istituti richiamati.
La Corte dichiarò la questione inammissibile proprio sulla considerazione che le discipline che regolano i due istituti sono diverse e che, con riferimento all'acquisizione dei tabulati, la disciplina a cui fare riferimento è quella di cui all'art. 256 c.p.p. relativo al dovere di esibizione all'autorità giudiziaria di documenti riservati o segreti, a cui pure sono sottese le irrinunciabili garanzie stabilite dall'art. 15, comma 2, Cost.

2.2. *La giurisprudenza di legittimità: un difficile punto di equilibrio.* Se la Corte costituzionale ha posto l'accento sulla necessità di tutele anche per l'acquisizione del tabulato, riconoscendogli un grado di intrusività non scontato, la giurisprudenza di legittimità si è mossa in modo ondivago.
Una delle questioni più delicate che i giudici di legittimità hanno dovuto risolvere attiene alla concreta attuazione delle tutele previste da quell'art. 15 Cost., ritenuto, a ragione, la principale fonte a cui fare riferimento.
Questo perché, facendo leva sulla necessità di un provvedimento da parte dell'autorità giudiziaria, non si è ritenuta unanimemente valida la soluzione secondo la quale, ai fini della acquisizione del tabulato, basta un provvedimento del pubblico ministero.

[43] Occorre richiamare, in verità, il fatto che le disposizioni costituzionali in tema di tutela delle libertà fondamentali hanno necessitato questa impostazione ("l'autorità giudiziaria") in quanto, sotto la vigenza del codice del 1930, il pubblico ministero aveva un autonomo potere di imposizione cautelare che gli consentiva di disporre, cioè, personalmente provvedimenti che restringevano la libertà del soggetto (ordini di cattura o di arresto); pertanto, tenuto conto che all'entrata in vigore della Costituzione era ancora vigente questa possibilità, è stato necessario offrire al sistema esistente una clausola che non fosse di aperta frizione con il codice.

Per una parte della giurisprudenza – minoritaria – la disciplina delle intercettazioni può essere applicata anche all'acquisizione dei dati relativi ai soggetti, al tempo e al luogo della comunicazione[44].
Alla medesima conclusione – con riferimento a tabulati acquisiti *ex* art. 234 c.p.p. dalla polizia giudiziaria – sono giunte, con un primo arresto, le Sezioni unite che, facendo leva sull'introduzione ad opera della legge 23 dicembre 1993 n. 547 dell'art. 266-*bis* c.p.p. e la modifica dell'art. 268 c.p.p., hanno ritenuto i tabulati quale documentazione in forma intellegibile del flusso informatico relativo ai dati esterni al contenuto delle conversazioni; pertanto, la loro acquisizione, rappresentando un momento del trattamento dei dati, non può che soggiacere, quanto a garanzie di segretezza e di libertà delle comunicazioni a mezzo di sistemi informatici, alla stessa disciplina.
Da queste considerazioni è derivato che il divieto di utilizzazione, previsto dall'art. 271 c.p.p., fosse riferibile anche all'acquisizione dei tabulati in tutti in casi di violazione dell'art. 267 c.p.p. e, dunque, in assenza del richiesto decreto motivato.
Secondo le Sezioni unite ciò non toglie che all'inutilizzabilità del tabulato, accertata dal giudice, possa far seguito, nello stesso procedimento, l'emissione del previsto decreto motivato per l'acquisizione dei relativi dati (estranei al contenuto della conversazione) presso l'ente gestore del servizio, dal momento che essi sono conservati, per il relativo trattamento, ai sensi dell'art. 4, comma 2, del d.lgs. 13 maggio 1998 n. 171. Legittima acquisizione che può essere disposta nel corso delle indagini preliminari dal pubblico ministero e dal giudice che procede (art. 267 c.p.p.), o dal giudice del dibattimento o di appello, rispettivamente ai sensi degli artt. 507 e 603 c.p.p.
Siffatta impostazione ha provocato qualche disorientamento[45].

---

[44] In questo senso Cass., Sez. VI, 18 dicembre 1995, n. 1670, in *Cass. pen.*, 1996, 3720 ss., con nota di CAMON, *Sulla inutilizzabilità nel processo penale dei tabulati relativi al traffico telefonico degli apparecchi «cellulari», acquisiti dalla polizia senza autorizzazione dell'autorità giudiziaria.*

[45] La pronuncia a cui si fa riferimento è Cass., Sez. un., 13 luglio 1998, Gallieri, in *Cass. pen.*, 1999, 465 ss., con nota critica di MELILLO, *L'acquisizione dei tabulati relativi al traffico telefonico fra limiti normativi ed equivoci giurisprudenziali.* La sentenza è stata, altresì, commentata da APA, *Ambiguità giurisprudenziali sull'acquisizione dei tabulati del traffico telefonico*, in *Riv. it. dir. proc. pen.*, 2000, 729 ss.; BRICCHETTI, *Estesa la disciplina delle intercettazioni, mentre la giurisprudenza si scopre divisa*, in *Guida dir.*, 1998, 48, 68 ss.; CALAMANDREI, *Acquisizione dei dati esteriori di una comunicazione ed utilizzazione*

Non a caso poco, più di un anno dopo, le stesse Sezioni unite hanno ritenuto di poter superare il precedente arresto ricalibrando la disciplina applicativa[46]. Sul presupposto dell'adeguatezza, allo stato della legislazione vigente in quel momento, della garanzia offerta dalla natura giurisdizionale dell'autorità titolare del potere invasivo e dal dovere di motivazione hanno riportato la richiesta di acquisizione dei tabulati nell'alveo della disciplina di cui all'art. 256 c.p.p.
Si è considerata legittima, per lungo tempo, l'attribuzione del potere di acquisizione al pubblico ministero senza la necessità di alcun tipo di autorizzazione o validazione da parte del giudice.
Su questo schema procedimentale ha però inciso fortemente la giurisprudenza europea.

3. *La ricostruzione nella legislazione italiana della* data retention. Il tema è complesso giacché su di esso si innesta anche quello relativo alla conservazione dei dati.
La disciplina relativa alla conservazione era, inizialmente, inserita nel corpo dell'art. 132 del d.lgs. n. 196/2003[47] in cui si prevedeva, genericamente, che dovessero essere conservati dal fornitore per ventiquattro mesi per finalità di

delle prove cosiddette incostituzionali, in *Giur. it.*, 1999, 1691 ss., e da ZACCHÈ, *Acquisizione di dati esterni ai colloqui telefonici*, in *Dir. pen. e proc.*, 1999, 335 ss.

[46] Cass., Sez. un., 23 febbraio 2000, n. 6, D'Amuri, Rv n. 21584101, che ha statuito il principio secondo cui «ai fini dell'acquisizione dei tabulati contenenti i dati esterni identificativi delle comunicazioni telefoniche conservati in archivi informatici dal gestore del servizio è sufficiente il decreto motivato dell'autorità giudiziaria, non essendo necessaria, per il diverso livello di intrusione nella sfera di riservatezza che ne deriva, l'osservanza delle disposizioni relative all'intercettazione di conversazioni o comunicazioni di cui agli articoli 266 e seguenti c.p.p. (Nell'affermare tale principio la Corte ha altresì precisato che il controllo giurisdizionale sul provvedimento acquisitivo, che attiene ad un mezzo di ricerca della prova, si attua mediante la rilevabilità anche d'ufficio, in ogni stato e grado del procedimento, dell'eventuale inutilizzabilità, essendo l'art. 191 c.p.p. applicabile anche alle c.d. prove "incostituzionali" perché assunte con modalità lesive dei diritti fondamentali)». L'arresto è stato commento positivamente da FILIPPI, *Il* revirement *delle sezioni unite sul tabulato telefonico: un'occasione mancata per riconoscere una prova incostituzionale*, in *Cass. pen.*, 2000, 3245 ss., e da MELILLO, *Intercettazioni ed acquisizioni tabulati telefonici: un opportuno intervento correttivo delle Sezioni unite*, *ivi*, 2595 ss.

[47] Cfr. Codice in materia di protezione dei dati personali, recante "*Disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*", in *Gazz. Uff.*, 29 luglio 2003, n. 174, Suppl. ord. n. 123.

accertamento e repressione dei reati; si prevedeva, poi, che, decorso quel termine, i dati fossero conservati (ancora dal *provider*) per il termine ulteriore di ventiquattro mesi, questa volta, per esclusive finalità di accertamento e repressione dei delitti più gravi elencati dall'art. 407, comma 2, lett. a), c.p.p. nonché per i reati in danno di sistemi informatici e telematici.
Su questa disciplina, riconosciuta, come si è detto, costituzionalmente valida, è intervenuto, però, il d.l. n. 354 del 2003[48] che, ai fini dell'acquisizione, ha previsto la necessità del decreto motivato del giudice, adottato su richiesta del pubblico ministero, dell'indagato o imputato, della persona offesa o delle altre parti private.
Il provvedimento è sembrato recepire tutte le istanze di necessario intervento della giurisdizione per accordare la stessa tutela che opera sul piano delle intercettazioni.
Eppure, poco tempo dopo, si è intervenuti con il d.l. 27 luglio 2005, n. 144, convertito nella legge n. 155/2005[49] (cd. decreto Pisanu) con cui si è prevista, nuovamente, la restituzione al pubblico ministero del potere di autonoma acquisizione dei dati presso il fornitore, anche su istanza delle altre parti; al difensore dell'imputato o della persona sottoposta alle indagini, invece, è stata accordata la facoltà di richiedere, direttamente al *provider*, i dati relativi alle utenze intestate al proprio assistito con le modalità di cui all'art. 391-*quater* c.p.p.
Sul tema, non poteva che avere influenza il diritto sovranazionale. Infatti, da ultimo, il d.lgs. n. 101 del 10 agosto 2018 ha provveduto a dare attuazione al cd. pacchetto europeo di protezione dati[50], novellando l'art. 132 del codice della *privacy*.

---

[48] Recante "*Disposizioni urgenti per il funzionamento dei tribunali delle acque, nonché interventi per l'amministrazione della giustizia*", in *Gazz. Uff.*, 29 dicembre 2003, n. 300. Il d.l. è stato convertito dalla L. 26 febbraio 2004, n. 45, in *Gazz. Uff.*, 27 febbraio 2004, n. 48.
[49] Recante "*Misure urgenti per il contrasto del terrorismo internazionale*", in *Gazz. Uff.*, 27 luglio 2005, n. 173. Il d.l. è stato convertito dalla l. 31 luglio 2005, n. 155, in *Gazz. Uff.*, 1° agosto 2005, n. 177.
[50] Il decreto legislativo ha dato attuazione al Regolamento (UE) 2016/679 – già efficace, in verità, in ragione dell'applicabilità diretta che caratterizza l'atto *de qua* – e alla Direttiva (UE) 2016/680, già attuata ad opera del d.lgs. 18 maggio 2018, n. 51. Il d.lgs. n. 101 del 2018 va ad aggiungersi, dunque, al d.lgs. n. 51 del 2018, con il quale l'ordinamento italiano ha attuato la direttiva 2016/680, 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, completando il recepimento del c.d.

Si è stabilito che, a partire dalla data della comunicazione, i fornitori di servizi di comunicazione abbiano l'obbligo di conservare per ventiquattro mesi i dati di traffico telefonico; per dodici mesi quelli del traffico telematico e per trenta giorni i dati relativi alle chiamate senza risposta.
La disciplina non ha convinto: innanzitutto, perché è irragionevole prevedere tempi di conservazione differenti a seconda del tipo di traffico in rilievo[51]. In secondo luogo, perché la disciplina necessita di coordinamento con quella di cui all'art. 24 della legge 20 novembre 2017, n. 167 (cd. legge europea)[52] che, in deroga a quanto previsto dall'art. 132 cod. priv., stabilisce in settantadue mesi il termine di conservazione per i dati di traffico telefonico, telematico e relativo alle chiamate senza risposta in relazione all'accertamento ed alla repressione dei delitti consumati o tentati con finalità di terrorismo (art. 51, comma 3-*quater*, c.p.p.) nonché dei reati compresi nell'elenco dell'art. 407, comma 2, lett. a), c.p.p.
Ne deriva che il fornitore – al quale non è affatto noto né se l'autorità giudiziaria farà mai una richiesta né per quale tipologia di reato – non potrà che conservare, in ogni caso, i dati di traffico per il lunghissimo termine di settantadue mesi.
In definitiva, a partire dalla legge europea 2017, il tempo di conservazione dei dati è mutato in rapporto all'accertamento ed alla repressione di tutti i reati[53].
Il tema, estremamente delicato, ha interessato in più occasioni anche la giurisprudenza europea, tanto da sollecitare – ai fini dell'adeguamento della normativa interna a quella convenzionale, come interpretata dalla Corte di giustizia – l'intervento del legislatore italiano.

---

pacchetto protezione dati dell'Unione europea. Per le problematiche relative al periodo di conservazione dei dati, per quanto qui di interesse, contenute nel decreto legislativo n. 51 del 2018, si rinvia alle attente considerazioni di GALGANI, *Giudizio penale,* habeas data *e garanzie fondamentali*, in *questa Rivista* web, 4 febbraio 2019, 8 ss. Invero, l'Autrice mette in evidenza come l'intervento del legislatore si sia limitato a replicare pressoché pedissequamente gli enunciati del provvedimento europeo vaghi ed indeterminati. Analizza la connessione tra il diritto alla protezione dei dati personali e l'intelligenza artificiale, alla luce delle tutele (ritenute insufficienti) del citato decreto legislativo, PISATI, *Indagini preliminari e intelligenza artificiale: efficienza e rischi per i diritti fondamentali*, in *Proc. pen. giust.*, 2020, 4, 963 ss.

[51] Già RAFARACI, *Intercettazioni e acquisizioni di tabulati telefonici*, in *Contrasto al terrorismo interno ed internazionale*, a cura di Kostoris-Orlandi, Torino, 2006, 276, sottolineava come la *ratio* della previsione di termini fosse, verosimilmente, quella di ridurre i costi legati alla conservazione dei dati.

[52] Recante "*Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea*", in *Gazz. Uff.*, 27 novembre 2017, n. 277.

[53] Così SIGNORATO, *Novità in tema di* data retention, cit., 157.

Come si vedrà, la normativa europea, all'art. 15, par. 1, della direttiva 2002/58/CE – avente ad oggetto i diritti alla riservatezza delle comunicazioni, dei dati sul traffico e di quelli sull'ubicazione –, consente agli Stati membri di derogare a prescrizioni, divieti ed obblighi fissati per la tutela di quei diritti, con l'adozione di misure restrittive, purché la restrizione costituisca "una misura necessaria, opportuna e proporzionata all'intero di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato, della difesa e della sicurezza pubblica) e la prevenzione, la ricerca, l'accertamento e il perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica".

Così che la memorizzazione e la conservazione dei dati (cd. *data retention*) da parte di persone diverse dagli utenti o senza il loro consenso è ammessa solo ai fini e per il tempo strettamente necessario alla trasmissione della comunicazione, nonché, a date condizioni, per l'attività di fatturazione; diversamente, ogni dato è destinato alla distruzione o ad essere reso anonimo.

La direttiva 2006/24/CE[54], di modifica della direttiva 2002/58/CE[55] ha, poi, perseguito l'obiettivo di armonizzare le disposizioni degli Stati membri quanto all'obbligo per i fornitori di servizi di comunicazione elettronica accessibili al pubblico, o di una rete di comunicazione, di raccogliere e conservare, per un periodo determinato, dati ivi generati o trattati, allo scopo, indicato nell'art. 1, par. 1, ossia quello "di garantire la disponibilità a fini di indagine, accertamento e perseguimento di gravi reati, quali definiti da ciascuno Stato membro nella propria legislazione nazionale".

La questione del bilanciamento tra esigenze statuali di accertamento e repressione dei reati e diritti fondamentali dell'individuo in occasione dell'acquisizione di dati e informazioni presso i *service providers* è stato affrontato da due note sentenze della Grande Camera della Corte di Giustizia[56].

---

[54] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione.

[55] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e la tutela della vita privata nel settore delle comunicazioni elettroniche.

[56] Il riferimento è a Corte giust. UE, 8 aprile 2014, *Digital Rights Ireland Ltd.*, in *www.penalecontemporaneo.it*, 28 aprile 2014, con nota di FLOR, *La Corte di giustizia considera la direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?* Il successivo

Dirompente è stata la pronuncia del 2 marzo 2021, H.K., della Grande sezione (C-746/18)[57], secondo la quale è possibile la limitazione del potere di acquisizione processuale dei dati di traffico ai soli procedimenti per gravi reati o per gravi minacce per la sicurezza pubblica, ed è necessaria la subordinazione all'autorizzazione di un'autorità terza rispetto a quella pubblica richiedente. Infatti, la Corte ha precisato che l'accesso delle autorità nazionali competenti ai dati conservati dev'essere «subordinato ad un controllo preventivo effettuato o da un giudice o da un'entità amministrativa indipendente e (...) la decisione di tale giudice o di tale entità [deve] interven[ire] a seguito di una richiesta motivata delle autorità suddette».

La sentenza riassume i principi delle precedenti ma si sofferma su aspetti fino a quel momento non presi in esame.

La sentenza ha creato allarme nella giurisprudenza interna che ha posto in evidenza come i principi sanciti dal giudice europeo non possano che riguardare

---

arresto è Corte giust. UE, 21 dicembre 2016, *Tele2 e Watson*, in *www.penalecontemporaneo.it*, 9 gennaio 2017, con nota di POLLICINO-BASSINI, *La Corte di Giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico.* Già in passato, pronunce di merito hanno tentato di ridimensionare la portata dei precetti del giudice sovranazionale. Cfr. Trib. Padova, ord. 15 marzo 2017, in *Dir. pen. cont.*, 2017, 3, 356 ss., con nota di FLOR, *Data retention ed art. 132 cod.* privacy: vexata quaestio *(?)*. Critica, invece, la posizione di RUGGIERI, *Data retention e giudice di merito penale. Una discutibile pronuncia*, in *Cass. pen.*, 2017, 2483 ss.

[57] In dottrina, il provvedimento è stato commentato – tra i molti – da BATTARINO, *CGUE e dati relativi al traffico telefonico e telematico. Uno schema di lettura*, in *www.questionegiustizia.it*, 21 aprile 2021; FILIPPI, *Il legislatore deve urgentemente riformare la disciplina dell'acquisizione dei tabulati relativi al traffico e all'ubicazione*, in *www.ilpenalista.it*, 15 marzo 2021; ID., *La disciplina italiana dei tabulati telefonici e telematici contrasta con il diritto U.E.*, in *www.dirittodidifesa.eu*, 20 marzo 2021; DI STEFANO, *La Corte di giustizia interviene sull'accesso ai dati di traffico telefonico e telematico e ai dati di ubicazione a fini di prova nel processo penale: solo un obbligo per il legislatore o una nuova regola processuale?*, in *Cass. pen.*, 2021, 2556 ss.; GIORDANO, *La Corte di Giustizia sull'acquisizione dei tabulati telefonici: la normativa europea osta ad una disciplina nazionale che riconosca la competenza del P.M.*, in *www.ilpenalista.it*, 10 marzo 2021; GRECO, *Quest'acquisizione non s'ha da fare: ennesimo 'no' della Corte di Giustizia alla* data retention *indiscriminata in campo penale*, in *Dir. dell'informazione e dell'informatica*, 2022, 2, 235 ss.; LEO, *Le indagini sulle comunicazioni e sugli spostamenti delle persone: prime riflessioni riguardo alla recente giurisprudenza europea su geolocalizzazione e tabulati telefonici*, in *www.sistemapenale.it*, 31 maggio 2021; RESTA, *Conservazione dei dati e diritto alla riservatezza. La Corte di giustizia interviene sulla* data retention. *I riflessi sulla disciplina interna*, in *www.giustiziainsieme.it*, 6 marzo 2021; SPANGHER, *I tabulati: un difficile equilibrio tra esigenze di accertamento e tutela di diritti fondamentali*, in *www.giustiziainsieme.it*, 3 maggio 2021; TORRE, Data retention: *una ventata di "ragionevolezza" da Lussemburgo*, in *www.consultaonline.it*, 19 luglio 2021. Sia consentito, poi, il rinvio a MALACARNE, *Corte di giustizia e* data retention*: ultimo atto?*, in *Cass. pen.*, 2021, 4105 ss.

solo quegli Stati dell'Unione privi di regolamentazione dell'accesso e della conservazione dei dati del traffico telefonico, ritenendo a contrario che la legislazione italiana si caratterizzi per una specifica regolazione della *data retention*, che prevede, appunto: l'indicazione della finalità di repressione dei reati; la durata massima della memorizzazione e l'intervento dell'autorità giudiziaria (pubblico ministero) capace di vagliare la stretta necessità dell'acquisizione nonché il rispetto del principio di proporzionalità in concreto[58].
La Corte di giustizia, però, ha osservato che la conservazione di tutti i *metadata* rappresenta una ingerenza particolarmente significativa nei diritti garantiti dalla Carta di Nizza (in particolare, dagli artt. 7, 8 e 11) in quanto consente di accedere ad informazioni fondamentali della vita personale dei soggetti nei confronti dei quali vengono raccolti.

3.1. *L'intervento del Legislatore del 2021 e la sollecitazione della giurisprudenza europea.* Così, la sentenza della Corte di giustizia del 2 marzo 2021 ha riacceso il dibattito sulla normativa interna della *data retention*[59].

[58] Già prima della citata pronuncia la giurisprudenza si è occupata del tema, sollecitata dai precedenti arresti. In particolare, Cfr. Cass., Sez. III, 19 aprile 2019, n. 36380, *non mass.* La sentenza è stata commentata da GIORDANO, *L'acquisizione dei tabulati telefonici e il diritto sovranazionale in tema di tutela della* privacy, in *www.ilpenalista.it*, 9 settembre 2019. Aspre le critiche di LUPARIA, Data retention *e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Diritto di Internet*, 2019, 4, 762 ss. Anche la sentenza Cass., Sez. II, 10 dicembre 2019, n. 5741, Rv n. 27856801, ha affermato che la disciplina italiana di conservazione dei dati di traffico è compatibile con le direttive n. 2002/58/CE e 2006/24/CE in tema di tutela della *privacy*, come interpretate dalla giurisprudenza della Corte di giustizia dell'unione europea (Corte giust. UE, 8 aprile 2014, *Digital Rights*, cit.; Corte giust. UE, 21 dicembre 2016, *Tele 2*, C-203/15 e C-698/15), poiché la deroga stabilita dalla norma alla riservatezza delle comunicazioni è prevista per un periodo di tempo limitato, ha come esclusivo obiettivo l'accertamento e la repressione dei reati ed è subordinata alla emissione di un provvedimento da parte di un'autorità giurisdizionale. Più di recente, si rinvia alla pronuncia Cass., Sez. II, 7 settembre 2021, n. 33116, secondo la quale «in tema di acquisizione dei dati contenuti nei cd. tabulati telefonici, la sentenza della Corte di giustizia dell'unione europea del 2 marzo 2021 (*H.K.*, C-746-218) non può trovare diretta applicazione in Italia fino a quando non interverrà il legislatore italiano ed anche europeo; allo stato, dunque, deve ritenersi applicabile l'art. 132 d.lgs. n.196/2003». Si consenta di rinviare, per un commento, al nostro *Acquisizione dei tabulati telefonici e* privacy, cit., 472.
[59] Il dibattito è analizzato da DINACCI, *L'acquisizione dei tabulati telefonici*, cit., 301.

Ci si è chiesti quando e come il legislatore sarebbe intervenuto, con quali conseguenze per i procedimenti in corso e ci si è interrogati sulla condivisibilità o meno delle argomentazioni contenute nella sentenza della Corte di giustizia[60].
Le posizioni della giurisprudenza interna sulla validità della normativa di cui all'art. 132 del d.lgs. 196 del 2003 sono apparse non irrobustite dal confronto con il nucleo essenziale dei diritti della persona riconosciuti dalla normativa sovranazionale.
La questione è stata risolta nel senso di ritenere assente qualsiasi profilo di contrasto tra la disciplina italiana e il diritto europeo, e non necessario sollecitare la stessa Corte di giustizia attraverso lo strumento del rinvio pregiudiziale per l'esatta interpretazione e, eventualmente, prospettare un controllo di legittimità costituzionale con riguardo al parametro della determinatezza della previsione normativa in materia penale.
Nonostante le resistenze, il Legislatore – probabilmente per evitare un'incontrollabile oscillazione giurisprudenziale – è infine intervenuto sul tema con un decreto di urgenza[61].
L'intervento, che non ha riguardato il tempo di conservazione dei dati, ne ha circoscritto l'acquisizione ai soli procedimenti che hanno ad oggetto l'accertamento di reati gravi, selezionati *quoad poenam*; e ha attribuito il controllo preventivo al giudice, salvo i casi d'urgenza per cui ha previsto una disciplina tutt'affatto difforme a quella di cui all'art. 267, comma 2, c.p.p.
La disciplina delineata dal decreto-legge è risultata in alcuni punti imprecisa: infatti, al comma 3 dell'art. 132, che regolava la procedura ordinaria, si era stabilito che «i dati *sono acquisiti* presso il fornitore con decreto motivato del giudice su richiesta...»; di contro, il comma 3-*bis* che, invece, regolamentava la procedura d'urgenza ad opera del pubblico ministero, stabiliva «... il pubblico ministero *dispone* l'acquisizione dei dati con decreto motivato che è comunicato immediatamente, e comunque non oltre quarantotto ore, al giudice

[60] Gli interrogativi sono di PARODI, *Tabulati telefonici e contrasti interpretativi: come sopravvivere in attesa di una nuova legge*, in *www.ilpenalista.it,* 3 maggio 2021.
[61] Nonostante, secondo il Garante della *privacy* sarebbe stato opportuno intervenire anche sulla disciplina della conservazione. Cfr. il parere acquisito dal governo prima dell'emanazione del d.l. 30 settembre 2021 n. 132, *Parere sullo schema di decreto-legge per la riforma della disciplina dell'acquisizione dei dati relativi al traffico telefonico e telematico ai fini di indagine penale*, 10 settembre 2021, consultabile in *www.garantedellaprivacy.it*.

competente per *il rilascio dell'autorizzazione* in via ordinaria». In questo modo, la situazione sembrava differenziarsi a seconda del *modus* con il quale i dati dovessero essere acquisiti, e allora il legislatore, in fase di conversione, ha confermato la natura senz'altro autorizzatoria del provvedimento giudiziale, rimuovendo la complicazione interpretativa dell'asimmetria presente del decreto-legge.

Con riferimento alla fase transitoria il d.l. n. 132 del 2021 non aveva previsto disposizioni *ad hoc* per i dati di traffico telefonico, telematico e alle chiamate senza risposta già acquisiti nei procedimenti pendenti alla data di entrata in vigore del provvedimento.

Nel silenzio del legislatore è stata proposta la soluzione, del tutto condivisibile, del riferimento al principio generale del *tempus regit actum*[62], per consentire l'utilizzabilità dei dati acquisiti nell'ambito di procedimenti pendenti alla data di entrata in vigore del decreto-legge, senza il necessario intervento autorizzativo *ex post* dell'autorità giudiziaria.

In sede di conversione, poi, è stata inserita una disciplina intertemporale – non collocata nel corpo dell'art. 132 ma al comma 1-*bis* aggiunto dalla legge n. 178 del 2021 – secondo cui «[i] dati relativi al traffico telefonico, al traffico telematico e alle chiamate senza risposta, acquisiti nei procedimenti penali in data precedente alla data di entrata in vigore del presente decreto, possono essere utilizzati a carico dell'imputato solo unitamente ad altri elementi di prova ed esclusivamente per l'accertamento dei reati per i quali la legge stabilisce la pena dell'ergastolo e della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'art. 4 del codice di procedura penale e dei reati di minacci e di molestia o disturbo alle persone con il mezzo del telefono, quando la minaccia, la molestia o il disturbo sono gravi».

Ne è derivata, dunque, l'inutilizzabilità dei tabulati telefonici ove non valutati in uno ad altri elementi di prova che vadano in tal senso.

---

[62] Così, BATTARINO, *Acquisizione di dati di traffico telefonico e telematico per fini di indagine penale il decreto-legge 30 settembre 2021 n. 132*, in *www.questionegiustizia.it,* 5 ottobre 2021; GITTARDI, *Sull'utilizzabilità dei dati del traffico telefonico e telematico acquisiti nell'ambito dei procedimenti pendenti alla data del 30 settembre 2021*, in *www.questionegiustizia.it*, 7 ottobre 2021; PESTELLI, *D.L. 132/2021: un discutibile e inutile aggravio di procedura per tabulati telefonici e telematici*, in *www.quotidianogiuridico.it*, 4 ottobre 2021. Per un approfondimento sul tema si rinvia, per tutti, a MAZZA, *La norma processuale penale nel tempo*, Milano, 1999, *passim*.

È appena il caso di osservare che il riferimento al solo imputato è da considerarsi estensibile *ex* art. 61 c.p.p. anche alla persona sottoposta alle indagini[63].
Quanto, poi, alla disciplina dell'inutilizzabilità dei dati acquisiti in violazione della "nuova" procedura di acquisizione, nella formulazione del decreto-legge la sanzione dell'inutilizzabilità era espressamente prevista solo nell'ultimo periodo del comma 3-*bis* che faceva riferimento alla procedura d'urgenza, quale conseguenza della intempestiva (o addirittura mancata) convalida da parte del giudice.
In sede di conversione il legislatore ha esteso la sanzione dell'inutilizzabilità a tutte le ipotesi acquisitive dei dati avvenute in violazione della disciplina, inserendo il comma 3-*quater* secondo il quale «i dati acquisiti in violazione delle disposizioni dei commi 3 e 3-*bis* non possono essere utilizzati», configurando un "divieto probatorio sanzionato con l'inutilizzabilità"[64].
La legge di conversione è sembrata aver ricalibrato la disciplina rendendola compatibile con l'interpretazione offerta dalla Corte di giustizia.

4. *Un breve sguardo oltre i confini nazionali: i due pilastri della giurisprudenza di Strasburgo in tema di* data retention. Sin dalla nota pronuncia *Malone* c. Regno Unito[65], le Corti sovranazionali europee hanno messo in luce la pervasività di un sistema di raccolta, conservazione, elaborazione e successiva utilizzazione di informazioni ricavate dall'analisi dei dati esteriori alle comunicazioni elettroniche.
A livello della "piccola Europa", il primo tassello del complesso percorso evolutivo sul tema della *data retention* viene comunemente identificato nella direttiva 97/66/CE del 15 dicembre 1997, concernente il trattamento dei dati personali e la tutela della vita privata nel settore delle telecomunicazioni.
L'art. 14, nello specifico, prevedeva che gli Stati membri potessero adottare disposizioni legislative volte a limitare la riservatezza delle comunicazioni, e dei dati esterni ad esse correlate, solo qualora tale restrizione costituisse una misura

[63] Sulle novità introdotte dalla legge di conversione si veda TAVASSI, *Acquisizione di tabulati, tutela della* privacy *e rispetto del principio di proporzionalità*, cit., 3 ss.
[64] Così, seppur con riferimento all'originario d.l. n. 132/2021, SPANGHER, Data retention: *svolta garantista ma occorre completare l'impianto*, in *Guida dir.*, 2021, 39, 14.
[65] Corte EDU, 2 agosto 1984, *Malone* c. Regno Unito.

necessaria per la salvaguardia della sicurezza dello Stato ovvero per la prevenzione, la ricerca, l'accertamento e il perseguimento di reati.
Sennonché, il legislatore comunitario – complice la crescita esponenziale dei servizi promossi dalle compagnie di comunicazione elettronica che, con lo sviluppo di *Internet*, avevano offerto nuove possibilità di accesso alla rete, ma, al contempo, rappresentavano una minaccia per i dati personali degli utenti – decideva di intervenire nuovamente sul tema *de quo*, con la finalità dichiarata di aggiornare il contenuto della precedente legislazione europea.
Si giunse così all'adozione della cd. direttiva *e-Privacy*, il cui nucleo essenziale, era – ed è tutt'ora – rinvenibile nell'art. 5, ove viene previsto un generale divieto di memorizzazione e conservazione dei dati sul traffico telefonico e telematico, salvo poi individuare una regolamentazione di carattere eccezionale (art. 15) che consente agli Stati membri di adottare misure dirette a limitare i diritti e gli obblighi fissati dalla direttiva in parola, solo laddove tale limitazione risulti necessaria, opportuna e proporzionata per la salvaguardia della sicurezza nazionale, la tutela della sicurezza pubblica e la repressione dei reati.
A distanza di pochi anni, la crescente minaccia terroristica, acutizzatasi con gli attentati di Madrid e Londra tra il 2004 e il 2005, ha portato il "governo europeo", sulla spinta di esigenze securitarie provenienti dai singoli paesi dell'Unione, ad adottare una nuova regolamentazione della materia che trovava la luce il 15 marzo 2006 nella nota direttiva 2006/24/CE (cd. direttiva Frattini).
La normativa, tuttavia, si è presentata da subito non priva di profili problematici: la mancata delimitazione dei destinatari dell'attività di memorizzazione dei metadati, l'individuazione di una cornice temporale per la conservazione delle informazioni sul traffico eccessivamente estesa (da sei mesi e due anni), nonché l'assenza di un controllo preventivo ed effettivo in fase di acquisizione dei dati, costituivano solo alcuni dei profili di elevata criticità della disciplina[66].
A fronte di un simile quadro, i giudici europei, con la rivoluzionaria pronuncia *Digital Right Ireland*, dopo aver riconosciuto l'esistenza di un interesse generale di ogni ordinamento alla repressione delle «gravi forme di criminalità», sono giunti a dichiarare l'invalidità della predetta direttiva, sottolineando come l'obbligo di una conservazione generalizzata imposto dalla normativa

[66] Per una panoramica dei profili di maggiore criticità della direttiva in questione, v. FLOR-MARCOLINI, *Dalla* data retention *alle indagini ad alto contenuto tecnologico*, cit., 8 ss.

comunitaria costituisse, di per sé, un'ingerenza grave nei diritti dei singoli individui. Di talché, qualunque interferenza con la vita privata del cittadino avrebbe potuto essere giustificata solo dall'esigenza di limitare i diritti e le facoltà previste dal diritto dell'Unione entro i limiti fissati dai principi di proporzionalità e di stretta necessità.

Sulla base di tali premesse, e in mancanza di un qualunque riferimento nella direttiva a parametri oggettivi che consentissero di delimitare l'accesso ai dati di traffico, la Corte ha finito per rilevare il contrasto con i principi di derivazione convenzionale.

La sentenza *Digital Rights* ha senz'altro segnato un decisivo cambio di passo nell'esame delle questioni legate alla preventiva memorizzazione dei dati esteriori alle comunicazioni. In effetti, pur nella genericità del contenuto, non può negarsi come essa abbia dato l'avvio ad una fase di "rinvigorimento" del principio di riservatezza, la cui tutela, come affermato dai giudici europei, passa anzitutto da una rigorosa interpretazione del canone di proporzionalità.

Non potendo passare in rassegna – per ragioni di economia del presente lavoro – le successive pronunce della Corte di giustizia, può comunque individuarsi un *fil rouge* che, in una duplice dimensione, pare legare tutta la giurisprudenza di Strasburgo.

A tale riguardo, può certamente osservarsi, da un primo angolo di visuale, come il nucleo centrale della fase di raccolta preventiva dei dati esteriori sia stato identificato nel divieto generalizzato e indiscriminato di conservazione degli stessi per finalità di tipo repressivo. Una preclusione che, sebbene in un primo momento fosse stata cristallizzata in modo assoluto, è stata in seguito fortemente ridimensionata.

Per un verso, la pronuncia resa nel caso *Ministero Fiscal*[67] – muovendo dall'assunto che l'accesso alle informazioni che non consentono di conoscere la data, l'ora, la durata e i destinatari delle comunicazioni effettuate, né i luoghi in cui tali conversazioni sono avvenute debba ritenersi inidoneo a disvelare le abitudini di vita di un determinato soggetto – ha reso legittime tutte quelle forme di conservazione dei metadati che si giustificano con l'obiettivo di prevenzione di

[67] Corte giust. UE, 2 aprile 2018, *Ministero Fiscal*, C-207/16.

«reati in generale», senza che trovi applicazione il requisito precedentemente individuato della «gravità» del crimine commesso[68].
Per alto verso, con la sentenza *La Quadrature du Net*[69] i giudici comunitari hanno introdotto un'ulteriore eccezione al divieto di conservazione generalizzata fondata, all'esito di un giudizio di proporzionalità, sulla specifica finalità perseguita dallo Stato membro nella fase di prevenzione e repressione dei reati. La questione – che verrà esaminata nel prosieguo – è quella concernente la distinzione tra "sicurezza nazionale" e "sicurezza pubblica", nella parte in cui, con riferimento alla prima, la Corte ha ammesso una forma di memorizzazione indiscriminata dei dati esteriori, pur se per un periodo di tempo limitato e con la garanzia di un controllo preventivo ed effettivo.
In una seconda prospettiva, si colloca la *quaestio* concernente l'individuazione del soggetto titolare del potere autorizzatorio all'acquisizione dei tabulati telefonici.
Come si è già accennato, la tutela effettiva dei canoni di proporzionalità e stretta necessità, nonché delle ulteriori condizioni di accesso prescritte dalla Corte, non può che passare necessariamente da un controllo eseguito da un'entità capace di garantire, in concreto, l'applicazione dei suddetti principi. È in questa direzione, pertanto, che i giudici europei, sin dalla pronuncia *Digital Rights*, hanno affermato come l'accesso, per finalità penal-repressive, ai dati conservati dagli *Internet service provider* (*ISP*) debba essere subordinato ad un controllo preventivo eseguito da «*a court or by an independent administrative body*», la cui decisione sia diretta a vincolare l'acquisizione delle informazioni in questione a quanto «*strictly necessary for the purpose of attaining the objective pursued*»[70].
Sul punto, è appena il caso di notare come negli arresti più risalenti tale specifica questione – sebbene costituisca un pilastro della giurisprudenza

[68] Secondo LUPARIA, Data retention *e processo penale*, cit., 760, la distinzione di «grado così inaugurata dalla Corte tra intrusioni nella *privacy* pare aver complicato ancor di più una materia già assai tormentata». Su questo specifico punto, v., volendo, MALACARNE, *Il ricorso a strumenti investigativi a cd. contenuto tecnologico. La* Data retention *nel procedimento penale alla luce della giurisprudenza europea e della (ondivaga) giurisprudenza di merito italiana*, in *Diritto di internet*, 2021, 4, 612 s.
[69] Corte giust. UE, 6 ottobre 2020, *La Quadrature du Net* e altri, cause riunite C-511/18, C-512/18 e C-520/18.
[70] Corte giust. UE, 8 aprile 2014, *Digital Rights*, cit., par. 62.

comunitaria in materia – non fosse stata trattata in maniera particolarmente approfondita. In effetti, passando in rassegna le principali sentenze che dal 2014 al 2021 hanno avuto modo di soffermarsi sulla *data retention* per finalità di prevenzione e repressione dei reati, ci si accorge di come esse si siano limitate perlopiù a richiamare la necessità di un controllo esercitato da un'autorità indipendente, senza tuttavia specificare alcun elemento ulteriore che potesse offrire indicazioni agli Stati membri nell'ottica di una più efficace armonizzazione delle legislazioni nazionali.

Per un approccio di carattere più specifico e, al contempo sistematico, bisognerà attendere la pronuncia *H.K.* del 2 marzo 2021 che, come si è già visto, nel fornire per la prima volta una vera e propria "interpretazione autentica" dell'espressione «giudice o autorità amministrativa indipendente», ha fatto breccia anche nel sistema italiano (e non solo[71]), riportando in auge il fervente dibattito relativo alla posizione ordinamentale assunta dal pubblico ministero italiano, tanto con specifico riguardo al mezzo di ricerca della prova in oggetto[72], quanto in relazione ad altri strumenti investigativi[73].

5. L'ultimo arresto della Corte di giustizia nel caso G.D.*: non è tutto oro quel che luccica?* Il rapsodico e succinto *excursus* dei profili essenziali trattati dalla giurisprudenza sovranazionale in tema di *data retention* ci consente di soffermare l'attenzione sul recente arresto dei giudici europei che, con la pronuncia

[71] Cfr. POLO ROCA, *La Regulación Sobre la Conservación de Datos en el Sector de las Comunicaciones Electrónicas o Telecomunicaciones: Estado de la Cuestión*, in *Revista de Internet, Derecho y Política*, 2021, 33, 12 ss.; AUDIBERT, *La Conservation et l'Accès aux Données Techniques de Connexion. Vers un Nouveau Paradigme pour les eEnquêtes Judiciaires?*, in *Veille juridique, Centre de recherche de l'Ecole des officiers de la Gendarmerie Nationale*, 2021, 16 ss.

[72] Sulle ricadute interne della pronuncia *H.K.*, con esclusivo riguardo al ruolo assunto dal pubblico ministero, v. GAETA, *Consensi e dissensi sulla indipendenza del p.m. (a proposito del potere di acquisire i tabulati telefonici)*, in *questa Rivista*, 2021; nonché, volendo, MALACARNE, *Corte di giustizia e* data retention, cit., 4115-4121, 4127 s.

[73] Ci si potrebbe domandare, in effetti, se il *dictum* comunitario, sotto questo profilo, possa riverberare i suoi effetti anche con riguardo alla disciplina delle perquisizioni o del tracciamento *GPS*. Per un accenno a quest'ultima possibilità, v. PARODI, *Localizzazione e tracciamento: una nuova disciplina?*, in *www.ilpenalista.it*, 1 dicembre 2021.

del 5 aprile 2022 nel caso *G.D.*[74], hanno avuto modo di confrontarsi nuovamente con le principali questioni in materia.
A seguito di un rinvio pregiudiziale della Corte suprema, i giudici comunitari sono stati chiamati a pronunciarsi sulla compatibilità della legge irlandese in tema di tabulati telefonici[75] con il diritto eurounitario, così per come interpretato dalla stessa giurisprudenza di Lussemburgo.
In via preliminare, deve osservarsi come la pronuncia, benché dal punto di vista contenutistico non possa dirsi realmente innovativa, risulti di specifico interesse, dal momento che consente di apprezzare, in maniera più limpida e, al contempo, dettagliata, alcuni dei princìpi cardine che proprio la Corte di giustizia aveva già enunciato sin dai primi arresti in argomento.

5.1. *Il divieto* bulk data retention *e l'efficacia empirica dei tabulati telefonici.*
Innanzitutto, la Corte ha posto ancora una volta in rilievo il divieto di una conservazione generalizzata e indifferenziata dei dati di traffico ai fini di lotta alla criminalità grave, chiarendo, con maggior vigore espressivo rispetto alle precedenti pronunce[76], che il tabulato telefonico non può essere qualificato alla stregua di un mezzo di ricerca della prova "retrospettivo"[77]. Sotto tale profilo, infatti, occorre tenere ben distinta la fase di memorizzazione dei metadati da quella, successiva, di accesso agli stessi: una disciplina positiva della fase di

[74] Corte giust. UE, 5 aprile 2022, *G.D.*, C-140/20, con nota di IOVENE, *Nuova decisione della Corte di giustizia in materia di tabulati: quali conseguenze per l'ordinamento nazionale?*, in *Cass. pen.*, 2022, 2363 ss. Per un resoconto dei contenuti della pronuncia, v. FILIPPI, *La Corte di Lussemburgo ribadisce lo stop ai tabulati: una fine annunciata*, in *www.penaledp.it*, 14 aprile 2022; SPANGHER, *Spangher: «La Corte di Giustizia della Ue ha sancito la fine del regime dei tabulati»*, in *www.ildubbio.it*, 20 aprile 2022; RESTA, *Dalla conservazione generalizzata a quella mirata e rapida: la Corte di giustizia ridelinea i contorni della* data retention, in *www.giustiziainsieme.it*, 7 aprile 2022; e, nella letteratura straniera, RODRÍGUEZ LAINZ, *La Evolución de la Jurisprudencia del Tribunal de Justicia de la Unión Europea en Materia de Conservación Indiscriminada de Datos de Comunicaciones Electrónicas en la STJUE del Caso G.D. y Comissioner an Garda Síochána*, in *Diario La Ley*, 19 aprile 2022.
[75] Per un'analisi, v. FENNELLY, *Data Retention in Ireland*, in *European Constitutional Courts towards Data Retention Laws*, a cura di Zubik-Podkowik-Rybski, Cham, 2021, 137 ss.
[76] Corte giust. UE, 6 ottobre 2020, *La Quadrature du Net*, cit., par. 116.
[77] VILLALÓN, *Opinion of Advocate General-Digital Rights Ireland*, 12 dicembre 2013, par. 72: «*the collection of such data establishes the conditions for surveillance which, although carried out only retrospectively when the data are used, none the less constitutes a permanent threat throughout the data retention period to the right of citizens of the Union to confidentiality in their private lives*».

acquisizione, per quanto specifica e dettagliata, non potrebbe comunque legittimare una preventiva e generalizzata memorizzazione delle informazioni sul traffico telefonico.
Su tale specifico punto, è interessante notare come il giudice del rinvio abbia sostenuto che la criminalità grave possa essere adeguatamente contrastata ricorrendo esclusivamente ad una conservazione di tipo generalizzata[78].
Sennonché, tale considerazione – com'era prevedibile – è stata censurata dalla Corte di giustizia che, ricorrendo ad un'espressione particolarmente felice, ha affermato come l'efficacia delle azioni penali dipenda non tanto dal ricorso ad un unico strumento di indagine, bensì dall'insieme dei mezzi investigativi a disposizione delle autorità inquirenti.
Quest'ultima precisazione – senz'altro condivisibile – pare richiamare, seppur indirettamente, il tema assai complesso relativo all'efficacia empirica degli strumenti di *data retention* ai fini di contrasto alla criminalità.
Muovendo dal presupposto che l'utilizzo degli *smartphone* e degli altri mezzi di comunicazione ha inciso notevolmente anche sul versante degli illeciti penali (tanto informatici, quanto comuni), si è soliti affermare che il ricorso ai tabulati telefonici è cruciale ed essenziale per investigazioni penali che vogliano dirsi realmente efficienti ed efficaci[79]. Cosicché, l'eliminazione di un obbligo generale di memorizzazione dei dati sarebbe in grado di compromettere gravemente la capacità investigativa della polizia giudiziaria e degli organi di

[78] Corte Suprema irlandese, *Graham Dwyer and The Commissioner of An Garda Síochána, the Minister for Communications, Energy and Natural Resources, Ireland and the Attorney General*, par. 4.4, reperibile all'indirizzo *https://www.statewatch.org/media/documents/news/2020/feb/ie-dwyer-v-commissioner-data-retention-24-2-20.pdf*.
[79] In questo senso, v., ad es., Commissione Europea, *Report from the Commission to the Council and the European Parliament: Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)*, 18 aprile 2011, 23.

intelligence[80], nonché di minare la sovranità statale nel settore della sicurezza nazionale[81].

Occorre domandarsi, tuttavia, se simili affermazioni siano empiricamente dimostrabili.

Risulta di un qualche interesse, cioè, stabilire se vi siano statistiche che mettano in relazione l'esistenza di leggi sulla conservazione dei metadati di traffico e la diminuzione della criminalità nelle principali aree urbane delle città.

La questione è troppo vasta e delicata per essere anche solo sinteticamente tratteggiata in questa sede. Tuttavia, una celere rassegna dei principali (e, invero, rari) studi svolti a livello europeo parrebbe offrire una risposta negativa al quesito *de quo*[82].

Si considerino, ad esempio, gli esiti delle ricerche svolte nel 2011 dal *Max-Planck-Institut*[83] e, più recentemente, dal Centro studi legali del Parlamento europeo[84] che hanno messo chiaramente in luce come non sia possibile individuare, neppure con buona dose di approssimazione, una qualche correlazione diretta tra la presenza o meno di specifiche regolamentazioni sulla conservazione dei dati e le statistiche sull'aumento o la diminuzione dei reati, contribuendo forse a screditare l'opinione di quanti sostengono che la tecnologia,

---

[80] Per questa opinione, CAMERON, *Balancing Data Protection and Law Enforcement Needs: Tele2 Sverige and Watson*, in *Common Market Law Review*, 2017, 1483; ID., *European Union Law Restraints on Intelligence Activities*, in *International Journal of Intelligence and CounterIntelligence*, 5 giugno 2020, 457 s. Cfr., altresì, DREWRY, *Crimes Without Culprits: Why the European Union Needs Data Retention, and How It Can Be Balanced With the Right to Privacy*, in *Wisconsin International Law Journal*, 2016, 33, 739 ss.

[81] Così, BRECHOT, *Clap de Fin pour la Conservation Généralisée des Données de Connexion en Europe ? Note sous CJUE, Gr. Ch., 21 Décembre 2016, C-203/15 et C-698/15. Tele2 Sverige et Watson e.a.*, in *Revue de l'Union européenne*, 2017, 606, 178 ss.

[82] Cfr. Garante europeo della protezione dei dati, *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – "A comprehensive approach on personal data protection in the European Union"*, 23 settembre 2011.

[83] Max-Planck-Institut *Für ausländisches und internationales Strafrecht, Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten*, 2011, 218 ss. Il documento è consultabile all'indirizzo *https://grundrechte.ch/2013/MPI_VDS_Studie.pdf*.

[84] Centro Studi Legali del Parlamento europeo, *General data retention / effects on crime*, 10 dicembre 2019, 3.

nelle fasi di prevenzione ed accertamento dei reati[85], sia «*more effective than non-technical solutions*»[86].
Con ciò, si badi, non vuol certo negarsi che le numerose ed eterogenee informazioni ricavabili dal tabulato telefonico siano prive di una notevole potenzialità euristica. Anzi, non è poi così raro imbattersi in investigazioni penali incentrate, sin dalle prime battute, quasi esclusivamente su una raccolta massiccia di dati[87].
È però opportuno considerare che ogni strumento di ricerca della prova, per quanto tecnologicamente avanzato possa dirsi, deve sempre essere calato nel contesto procedimentale, ovverosia in un ambito nel quale il "dubbio", quale manifestazione processuale del metodo falsificazionista[88], dovrebbe permeare qualunque tipo di attività, tanto giudiziaria, quanto giurisdizionale.

5.2. *La precaria distinzione tra esigenze di "sicurezza nazionale" e "sicurezza pubblica": il caso emblematico del* Conseil d'Etat *francese.* Attenzione particolare merita la *quaestio* – anch'essa trattata nella sentenza *G.D.* – concernente la "gerarchizzazione" tra le singole ipotesi derogatorie previste all'art. 15 della direttiva *e-Privacy*.
Come si è già avuto modo di ricordare, la limitazione della riservatezza, così per come tutelata all'art. 5 della direttiva, può dirsi legittima solo qualora sia ricollegabile ad esigenze di salvaguardia della sicurezza nazionale, della sicurezza pubblica o ai fini della prevenzione di gravi forme di reati.
Com'è noto, nell'esaminare tali specifiche situazioni, la Corte di giustizia, nella pronuncia *La Quadrature du Net*, ha già fornito una definizione

[85] Ad una differente conclusione, dovrebbe senz'altro giungersi con riferimento all'impiego della *tèchne* nell'ambito della cd. informatizzazione del rito penale. Per una recente ed approfondita analisi del fenomeno, cfr. B. Galgani, *Forme e garanzie nel prisma dell'innovazione tecnologica. Alla ricerca di un processo penale "virtuoso"*, Cedam, Milano, 2022, *passim*.
[86] RUCZ-KLOOSTERBOER, *Data Retention Revisited*, pubblicato all'indirizzo *https://edri.org/our-work/launch-of-data-retention-revisited-booklet/*, 19.
[87] CAMON, *La fase che "non conta e non pesa": indagini governate dalla legge?*, in *Dir. pen. proc.*, 2017, 432.
[88] Cfr. CONTI, *Scienza controversa e processo penale: la Cassazione e il "discorso sul metodo"*, in *Dir. pen. proc.*, 2019, 848 ss. Per una differente lettura del metodo popperiano nell'ambito del processo penale, v., di recente, BONIOLO-GENNARI, *Alla* Popper*! Ripensando criticamente al suo mito tra i giuristi*, in *www.sistemapenale.it*, 9 marzo 2022.

dell'espressione «*national security*»[89] in termini relativamente stringenti[90], ovverosia quale interesse primario di tutela delle funzioni essenziali dello Stato e degli interessi fondamentali della società, tra i quali possono annoverarsi – ad avviso dei giudici europei – tutte quelle «attività tali da destabilizzare gravemente le strutture costituzionali, politiche, economiche o sociali di un paese»[91], quali, in particolare, quelle atte a minacciare direttamente la società, la popolazione di uno Stato, come, ad esempio, una attacco terroristico.

A fronte di simili indicazioni, la Corte è giunta ad affermare che l'importanza dell'obiettivo della salvaguardia della sicurezza nazionale supera quella degli altri fini indicati all'art. 15, in ragione della connotazione grave, attuale o prevedibile che contraddistingue quest'ultima esigenza. A differenza del rischio generale e permanente rappresentato dal verificarsi di forme di criminalità, anche gravi, una minaccia alla sicurezza nazionale ha carattere concreto e prevedibile[92], potendo legittimare una normativa interna che abilita ad una conservazione generalizzata e indifferenziata dei dati di traffico, purché tale memorizzazione sia temporalmente limitata ai fini dello stretto necessario e sottoposta al vaglio di un'autorità indipendente.

Apparentemente lineare nelle premesse e nell'*iter* argomentativo, il percorso seguito dalla Corte in quella occasione – e ulteriormente precisato nella sentenza *G.D.*[93] – non ha tuttavia impedito al *Conseil d'Etat* francese di adottare

[89] Per un'analisi storico-giuridica di tale concetto, muovendo dalla prospettiva americana, v. FANCHIOTTI, Security v. fundamental rights *negli Stati Uniti d'America*, in *Dir. pen. proc.*, 2019, 1558 ss. e, specialmente, 1560 ss.

[90] Critico sull'individuazione della «sicurezza nazionale» quale obiettivo in grado di giustificare una conservazione generalizzata dei metadati di traffico, NINO, *La disciplina internazionale ed europea della* data retention *dopo le sentenze* Privacy International *e* La Quadrature du Net *della Corte di giustizia UE*, in *Diritto dell'Unione Europea*, 2021, 1, 115.

[91] Corte giust. UE, 6 ottobre 2020, *La Quadrature du Net*, par. 135.

[92] Sulla difficoltà di definire tali requisiti, v. TZANOU-KARYDA, *Privacy International and Quadrature du Net: One Step Forward Two Steps Back in the Data Retention Saga?*, in *European Public Law*, 2022, 1, 137.

[93] Corte giust. UE, 5 aprile 2022, *G.D.*, par. 56-66.

una recente pronuncia[94] che, ad avviso dei primi commentatori, si è posta in palese violazione del *dictum* comunitario[95].
Il 21 aprile 2021 il giudice amministrativo d'oltralpe – in un caso nel quale il ricorrente censurava la normativa francese in materia di tabulati telefonici[96]– ha invocato proprio il regime eccezionale legato alla sicurezza nazionale per legittimare una conservazione generalizzata e indiscriminata dei dati di traffico telefonico e telematico sull'intero territorio statale. Più in particolare, i requisiti di attualità e concretezza della minaccia, idonei a consentire un regime di sorveglianza massiva, sarebbero legati ad un elevato e persistente rischio di attacco terroristico, così come dimostrerebbero i numerosi attentati che nel periodo 2020-2021 hanno colpito il territorio francese[97].
Un simile approccio alla materia, come si è anticipato, è stato sottoposto ad aspre censure[98] che, in estrema sintesi, hanno sottolineato come la pronuncia *French Data Network* abbia finito per rovesciare il regime "regola-eccezione" ricavabile dalla lettura dell'art. 15 della direttiva 2002/58/CE, assicurando in tal modo alla sicurezza nazionale un ruolo di primo piano nella disciplina in tema di *data retention*.

---

[94] *Conseil d'Etat*, 21 aprile 2021, *French Data Network*. Per un commento, v. MITSILEGAS-GUILD-VAVOULA-KUSKONMAZ, *Data Retention and the Future of Large-Scalesurveillance: the Evolution and Contestation Ofjudicial Benchmarks*, in *Europea Law Journal*, 2022, 23 ss.; DE TERWANGNE, *L'Illégalité Nuancée de la Surveillance Numérique: la Réponse des Juridictions Belge et Française à l'Arrêt La Quadrature du Net de la Cour de Justice de l'Union Européenne*, in *Revue Trimestrielle des Droits de L'Homme*, 2022, 1, 3 ss.; CAHN-BRUNET, *Arrêt French Data Network e.a. Le Conseil d'État Effronté du Dialogue des Juges CJUE (gde ch.), 6 octobre 2020, aff. C-623/17, C-511/18, C-512/18 et C-520/18 et CE (ass.), 21 avril 2021, n°s 393099, 394922, 397844, 397851, 424717 et 424718*, in *Revue du Droit de l'Union Européenne*, 2022, 1, 231 ss.

[95] Cfr., ad es., ROJSZCZAK, *The Uncertain Future of Data Retention*, cit., 12. Per una ricostruzione in parte differente, v. PERLO, *La decisione del Consiglio di Stato francese sulla* Data retention: *come conciliare l'inconciliabile*, in *Rivista di diritti comparati*, 2021, 2, 163 ss. e, specialmente, 183.

[96] Sulla quale v. AZOULAI-RITLENG-BONINI, «L'État, c'est moi»: *il Consiglio di Stato francese, fra salvaguardia della sicurezza nazionale e protezione dei dati (Consiglio di Stato,* Section du Contentieux, 21 aprile 2021, French Data Network e a., *nn. 393099, 394922, 397844, 397851, 424717, 424718)*, in *Rivista Interdisciplinare sul Diritto delle Amministrazioni Pubbliche*, 2021, 4 s.

[97] *Conseil d'État*, 21 aprile 2021, cit., par. 44. Critico su questo specifico aspetto della pronuncia, TURMO, *National Security as an Exception to EU Data Protection Standards: The Judgment of the Conseil d'État in French Data Network and others*, in *Common Market Law Review*, 2022, 219.

[98] Ad avviso di TURMO, *National Security as an Exception*, cit., 208, il «*Conseil d'État is either unaware or wilfully ignorant of core elements of EU constitutional law*».

Assumendo quale postulato argomentativo l'inefficacia delle misure di conservazione mirata o rapida[99], la Suprema corte amministrativa avrebbe optato – secondo taluno – per una visione «hobbesiana del diritto alla sicurezza»[100] che, legandosi intimamente ad un generale obbligo di protezione, imporrebbe ad ogni Stato membro di mettere in campo tutte le misure necessarie per garantire ai cittadini quella *tranquillitas* – ovverosia la pacifica convivenza fra individui – che fonda il concetto stesso di sicurezza.

Le conclusioni del giudice francese, inoltre, si porrebbero in contrasto con il dettato letterale dalla pronuncia resa nel caso *La Quadrature du Net*, ove la Corte ha avuto modo di precisare che la conservazione delle informazioni sul traffico per finalità di lotta al terrorismo «non possono avere carattere sistematico»[101], come accadrebbe qualora si optasse per l'interpretazione proposta dal giudice amministrativo.

Ma non è tutto. Le critiche mosse alla pronuncia *French Data Network* sono state altresì indirizzate ad un profilo direttamente connesso con quanto poc'anzi accennato in tema di efficacia empirica della raccolta di massa dei metadati di traffico.

In un recente parere sulla legittimità di un ipotetico regime di conservazione permanente dei dati di traffico, il giudice emerito europeo Prof. Vadapalas ha affermato che la decisione del tribunale francese non sarebbe condivisibile in quanto dotata di scarsa capacità euristica. Essa, infatti, non dimostrerebbe in concreto alcuna minaccia specifica alla sicurezza nazionale, facendo esclusivo riferimento ad un generico timore di un attacco terroristico sul territorio francese[102].

In un tale contesto, assai complesso, non appare dunque irragionevole ipotizzare che la Corte di giustizia, con la pronuncia resa nel caso *G.D.*, abbia voluto nuovamente precisare i contorni dell'espressione "sicurezza nazionale", e la distinzione che intercorre tra quest'ultima e la prevenzione della criminalità

---

[99] V. *infra*, par. 5.3 e 5.4.

[100] AZOULAI-RITLENG-BONINI, «L'État, c'est moi», cit., 22.

[101] Corte giust. UE 6 ottobre 2020, *La Quadrature du Net*, cit., par. 138.

[102] VADAPALAS, *Legal opinion*, 24 febbraio 2022, 10, reperibile al sito *https://www.patrick-breyer.de/wpcontent/uploads/2022/04/20220407_Legal_Opinion_Data_Retention_Vadapalas_updated-SimeonTC-VV-REV.pdf*.

grave in generale[103], proprio al fine di prevenire future pronunce da parte delle singole corti nazionali che si muovano nella stessa linea interpretativa adottata dal giudice francese[104].

5.3. *La cd. conservazione mirata e i possibili effetti discriminatori: brevi cenni.* Esclusa la legittimità di una qualunque forma di *bulk data retention*, la «pietra angolare»[105] del ragionamento adottato dalla Corte di giustizia, sin dalle pronunce più risalenti, è senz'altro costituita dalla cd. *targeted retention*, ovverosia da una conservazione mirata e limitata dei dati di traffico telefonico che, ad avviso dei giudici europei, risulterebbe conforme ai principi di proporzionalità e necessità.

Questa specifica modalità operativa – di cui si trova traccia, *in primis*, nella sentenza *Tele2*[106] – non presuppone la necessità di una preventiva identificazione delle persone sospettate di essere implicate in un delitto, risultando indispensabile, tuttavia, quantomeno la prova di una connessione, anche indiretta, con il compimento di atti di criminalità grave. Tali soggetti – stando alla consolidata giurisprudenza di Strasburgo – possono essere identificati in coloro che, sulla base di elementi oggettivi e non discriminatori, costituiscono una minaccia per la sicurezza pubblica o la sicurezza nazionale dello Stato membro interessato.

In questa direzione, è nuovamente intervenuta la Corte di giustizia che, nel suo ultimo arresto, ha esemplificato per la prima volta tale categoria ritenendo legittima una misura di conservazione non solo nei confronti di persone «sottoposte a indagine», ma anche con riguardo a coloro che sono «sottoposti a misure di sorveglianza [(*rectius*, cautelari)] in corso o sono iscritti nel casellario

[103] È stata espressamente sconfessata, infatti, la tesi della Commissione europea che tendeva ad un'equiparazione tra forme di criminalità particolarmente gravi e attentati alla sicurezza nazionale (cfr. Corte giust. UE, 5 aprile 2022, *G.D.*, cit., par. 60 ss.).

[104] Sulla necessità che il dibattito sul tema della *data retention* sia incentrato sull'analisi delle pronunce delle Alte Corti degli Stati membri, v. PODKOWIK-RYBSKI-ZUBIK, *Judicial Dialogue on Data Retention Laws: A Breakthrough for European Constitutional Courts?*, in *International Journal of Constitutional Law*, 5 gennaio 2022, 1597 ss. e, in particolare, 1631.

[105] In questi termini si è espresso l'avvocato generale CAMPOS SÁNCHEZ-BORDONA, *Conclusioni presentate il 18 novembre 2021 nel corso delle Cause riunite C-793/19 e C-794/19* Bundesrepublik Deutschland *c.* SpaceNet AG *(C-793/19)* Telekom Deutschland GmbH *(C-794/19)*, par. 43.

[106] Corte giust. UE, 21 dicembre 2016, *Tele2 e Watson*, cit., par. 108.

giudiziario nazionale ove è menzionata una condanna precedente per atti di criminalità grave che possono comportare un elevato rischio di recidiva»[107].
Una simile categorizzazione non può certo dirsi priva di criticità, potendo dare adito a profili discriminatori di notevole portata[108].
Pur non potendo approfondire il tema in questa sede, viene comunque da chiedersi se l'avere a proprio carico iscrizioni nel casellario giudiziario sia sintomo di una futura recidiva e se ciò, eventualmente, possa giustificare una misura di conservazione mirata o, piuttosto, non si ponga in contrasto con la regola di trattamento, corollario imprescindibile della presunzione di innocenza[109].

5.4. Il "blocco" dei dati: la cd. conservazione rapida. Ulteriore modalità di conservazione dei dati di traffico ritenuta legittima dalla Corte di giustizia è quella comunemente conosciuta con il nome di *quick freeze* o *expedited retention*.
Il fenomeno cui si allude, come noto, è quello in base al quale le informazioni contenute nei tabulati telefonici, una volta cessati i termini di conservazione indicati dalle singole legislazioni nazionali, debbono essere cancellate. Tuttavia, è ben possibile che nelle more intervenga la necessità che simili informazioni siano conservate ulteriormente per finalità di repressione dei reati[110].
Ebbene, in simili circostanze, la Corte di giustizia ha autorizzato le autorità competenti ad adottare un provvedimento, soggetto a controllo giurisdizionale, che ordini ai fornitori dei servizi di comunicazione di conservare quei dati per un periodo limitato.
Una simile procedura, tuttavia, deve essere tipizzata dal legislatore nazionale che, più nel dettaglio, dovrebbe indicare tra le ragioni legittimanti questa ipotesi di conservazione esclusivamente la necessità di indagare su reati gravi (e, *a fortiori*, su attentati alla sicurezza nazionale), qualora simili evenienze si siano già verificate ovvero nel caso in cui «la loro esistenza possa essere ragionevolmente

[107] Corte giust. UE, 5 aprile 2022, *G.D.*, cit., par. 78.
[108] V., già in precedenza, CAMPOS SÁNCHEZ-BORDONA, *Conclusioni*, cit., par. 45: «non si può escludere che formule di conservazione mirata basate su tali criteri risultino efficaci e, allo stesso tempo, non discriminatorie» (trad. nostra).
[109] Cfr. JUSZCZAK-SASON, *Recalibrating Data Retention in the EU*, cit., 253 ss.
[110] Si consideri che il nostro sistema, all'art. 132, comma 4-*ter*, cod. priv., prevede già un ordine di congelamento rapido nel settore delle cd. investigazioni preventive.

sospettata»[111]. In questo contesto, la Corte ha poi precisato che i dati richiesti attraverso una misura di congelamento rapido non devono essere limitati alle persone specificamente sospettate di avere progettato o commesso un reato grave, ben potendo essere ricompresi anche individui le cui informazioni possano contribuire all'accertamento di un siffatto reato.

Un simile meccanismo di indagine, per quanto maggiormente in linea con le esigenze di tutela della riservatezza rispetto ad un meccanismo di conservazione generalizzata, non è andato esente da censure.

Un timore che è stato avanzato, in particolare, è quello di assistere a forme che potremmo definire di "congelamento inutile": i metadati disponibili presso gli *ISP* al momento della richiesta di *expedited retention*, infatti, potrebbero essere insufficienti o irrilevanti[112], specialmente allorquando quest'ultima venga effettuata a distanza di tempo dai fatti oggetto di causa.

La critica – che, sotto certi aspetti, sembra cogliere nel segno – non pare però tenere conto a sufficienza dei possibili effetti benefici collegati all'ipotetica previsione di un meccanismo di "congelamento rapido d'urgenza", disposto dalla stessa autorità investigativa. Volendo esemplificare: laddove gli organi di indagine dovessero apprendere la *notitia criminis* in un arco temporale prossimo agli accadimenti, un'eventuale richiesta di questo tipo potrebbe consentire l'acquisizione di tutti quei dati di traffico utili ai fini dell'accertamento del fatto e limitati al solo periodo di interesse investigativo.

È altrettanto evidente, che, laddove quest'ultima dovesse pervenire a distanza di tempo dagli accadimenti, uno strumento modulato nei termini suddetti (e tenuto conto dell'auspicata riduzione dei periodi di conservazione presso gli *ISP*) potrebbe incidere negativamente sullo svolgimento delle investigazioni penali.

---

[111] Corte giust. UE, 6 ottobre 2020, *La Quadrature du Net*, cit., par. 161.

[112] Così, ancora, JUSZCZAK-SASON, *Recalibrating Data Retention in the EU*, cit., 256, ove si sottolinea come *«"quick freeze" merely saves available data from being erased, while the retrograde data that law enforcement authorities are most interested in cannot be retrieved* ex post». Problematiche in parte simili si sono manifestate, peraltro, con riferimento alla richiesta di trasmissione transfrontaliera di prove elettroniche nell'ambito della cooperazione volontaria degli *ISP*. Nel *3rd Annual sirius eu digital evidence situation report* prodotto da Eurojust ed Europol, infatti, è stato evidenziato come il 57,1% delle autorità nazionali intervistate abbia lamentato proprio «*the short data retention periods of the information collected after a preservation request / order is submitted to the private companies*» (*https://www.eurojust.europa.eu/sites/default/files/assets/sirius_eu_digital_evidence_situation_report_2021.pdf.*, 37).

5.5. *La sorveglianza geografica*. Un'ulteriore ipotesi è data dal cd. criterio geografico di conservazione mirata o rapida che, com'è noto, ha fatto la propria comparsa sul panorama sovranazionale con la più volte citata sentenza *Tele2*, ove la Corte di giustizia ha messo in luce come una conservazione dei metadati a titolo preventivo debba essere fondata su elementi oggettivi e non discriminatori, considerando tale il parametro di tipo territoriale, in base al quale risulti che in una o più aree esista un rischio elevato di preparazione o di commissione di reati gravi[113].

Il criterio in questione è tornato nuovamente al centro del dibattito europeo a seguito della sentenza *La Quadrature du Net*[114] e, da ultimo, della pronuncia resa nel caso *G.D.*

Nella recente decisione la Corte di giustizia ha affermato, più in particolare, che le misure di conservazione mirata e rapida possono essere fondate, tra gli altri, proprio su un criterio di tipo geografico, laddove vi siano elementi che facciano supporre ragionevolmente l'esistenza di una situazione di pericolo per l'incolumità pubblica (*rectius*, criminalità grave).

I giudici europei, nell'esemplificare tale parametro, hanno fatto espresso riferimento a luoghi caratterizzati da un numero elevato di atti di criminalità grave ovvero ad aree esposte alla commissione di reati gravi, quali infrastrutture frequentate regolarmente da un numero molto elevato di persone, o ancora, luoghi strategici, quali aeroporti, stazioni o aree di pedaggio (cd. *hotspot*).

In simili circostanze – si è affermato – i legislatori nazionali possono adottare forme di *targeted retention* o *quick freeze* avendo quale criterio guida il «tasso medio di criminalità» di una determinata zona geografica, indipendentemente dalla sussistenza di indizi concreti concernenti la preparazione o la commissione di atti di criminalità grave; cosicché, in simili evenienze, gli *ISP* potrebbero essere legittimati a memorizzare i dati di traffico di tutti gli utenti che, in quel periodo, hanno utilizzato un mezzo di comunicazione nelle aree geografiche preventivamente individuate.

---

[113] Corte giust. UE, 21 dicembre 2016, *Tele2 e Watson*, cit., par. 111.

[114] Corte giust. UE, 6 ottobre 2020, *La Quadrature du Net*, cit., par. 150 e 151, in cui si parla di «luoghi caratterizzati da un numero elevato di atti di criminalità grave».

A conclusione dell'*iter* argomentativo proposto, i giudici europei hanno precisato che una conservazione di questo tipo (tanto mirata, quanto rapida) non possa dirsi discriminatoria, posto che il criterio guida del «tasso medio di criminalità» non sarebbe lesivo del principio di uguaglianza.
Quest'ultimo assunto, tuttavia, non appare pienamente convincente. Al contrario: sembra prestare il fianco a critiche tutt'altro che infondate, in grado di far vacillare, sotto taluni profili, l'intera impalcatura argomentativa proposta dalla Corte.
La giustificazione offerta dai giudici di Lussemburgo, in effetti, pare non tener conto a sufficienza delle ricadute concrete di un criterio, quello geografico, che, a ben riflettere, potrebbe apparire non solo discriminatorio, ma financo sproporzionato.
Non è irragionevole ipotizzare, d'altro canto, che i sistemi di controllo basati sulla delimitazione territoriale possano condurre a forme perverse di profilazione di alcune aree (si pensi, ad esempio, alle zone periferiche delle città).
Alcuni commentatori, in questo senso, non hanno mancato di sottolineare come la Corte di giustizia, aprendo le porte ad un simile criterio, sebbene abbia vietato una «*indiscriminate data retention*», abbia finito per rendere legittima una «*discriminate retention*»[115].
Del resto, un criterio formulato in questi termini potrebbe comportare un'acquisizione in massa dei dati di traffico telefonico propri di soggetti che vivono o transitano frequentemente in determinate aree cittadine, senza che vi sia alcun legame con l'obiettivo di prevenzione dei reati.
Il parametro del «tasso medio di criminalità» – legittimante il ricorso a misure di conservazione mirata o rapida – pare porsi in possibile contrasto con i precedenti assunti fatti propri dalla stessa Corte di Lussemburgo, ove i giudici europei avevano messo in luce la necessità di accertare un'incidenza «elevata» (e, pertanto, superiore alla media) di reati gravi in una determinata area geografica.
La complessità della questione emerge anche dalla lettura di un interessante documento della Commissione europea, datato 10 giugno 2021, con il quale il "governo comunitario" ha cercato di predisporre alcune possibili modalità di

[115] In questi termini, WOODS, *Implications of the EU's Data Retention Ruling. Lawfareblog*, in *LawFare*, 22 dicembre 2016, all'indirizzo *https://www.lawfareblog.com/implications-eus-data-retention-ruling*.

normazione del tema *de quo*, al fine di stimolare l'intervento dei singoli Stati membri.
Per quel che interessa il criterio geografico, la Commissione ha tentato di specificare tale parametro facendo riferimento ad una serie di «*sensitive areas*» come, ad esempio, quelle che si collocano «*in a certain radius around sensitive critical infrastructure sites*» o «*areas with above average crime rates*» o, ancora, luoghi che possono essere bersaglio di gravi reati (si pensi, ad esempio, ai «quartieri ricchi, luoghi di culto, scuole, luoghi di culturali e sportivi, luoghi di incontri politici e vertici internazionali, Parlamenti, tribunali, centri commerciali»[116]).
Neppure una simile proposta, tuttavia, è stata ritenuta conforme ai *dicta* della giurisprudenza europea.
Anzitutto, l'utilizzo della formula «*a certain radius*» per indicare l'ampiezza dell'area geografica oggetto di conservazione mirata o rapida sarebbe in contrasto con quanto affermato dai giudici comunitari che, in proposito, si sarebbero riferiti espressamente alle sole aree sensibili, senza ammettere l'estensione del controllo anche nelle vicinanze di tali luoghi[117].
Una misura delineata in questi termini, inoltre, si esporrebbe anche a censure sotto il profilo del criterio di proporzionalità, posto che occorre tener presente di come in tali aree e, specialmente, in luoghi di culto, vengano svolte attività capaci di svelare dati particolarmente sensibili quali la religione e l'orientamento politico.
Le difficoltà e i numerosi dubbi interpretativi attorno all'adozione del criterio in esame sono altresì testimoniati dal turbolento iter parlamentare che sta attualmente attraversando l'ordinamento belga.
Il 9 giugno 2022, la *Commission de l'Économie, de la Protection des consommateurs et de l'Agenda numérique* ha approvato, in sede di prima lettura, il progetto di legge n. 2575/1 relativo alla *collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités*[118], che si pone quale

[116] Commissione europea, *Working paper*, 6, reperibile al sito https://www.patrick-breyer.de/en/come-back-of-data-retention-former-eu-judge-dismisses-commissions-plans/.
[117] Per questa critica, v. VADAPALAS, *Legal opinion*, cit., 31.
[118] *https://www.dekamer.be/kvvcr/showpage.cfm?section=flwb&language=fr&cfm=flwbn.cfm?lang=N&dossierID=2572&legislat=55.*

obiettivo quello di adeguare la normativa interna ai criteri indicati dalla giurisprudenza sovranazionale.
A seguito della sentenza *La Quadrature du Net*, la *Cour Constitutionelle* belga si è pronunciata, il 22 aprile 2021, dichiarando l'illegittimità della normativa interna in materia di *data retention*[119] che prevedeva una memorizzazione e successiva conservazione generalizzata e indifferenziata delle informazioni sul traffico per scopi di repressione dei reati.
In un simile contesto, il Parlamento ha deciso di intervenire per riformare l'intera regolamentazione della materia, individuando nel criterio geografico il parametro di applicazione della *targeted retention*. In estrema sintesi, il dettato normativo attualmente approvato individua, tra le numerose aree sottoponibili a misure di controllo, i «distretti giudiziari in cui sono stati commessi almeno 3 reati di cui all'articolo 90-*ter* del codice di procedura penale all'anno per 1000 abitanti»[120].
Una simile proposta risulta senz'altro pregevole nella misura in cui cerca di adempiere al *dictum* comunitario, cristallizzando una forma di controllo mirato, così per come enucleata dai giudici di Lussemburgo; tuttavia, la soglia individuata appare, secondo recenti studi statistici[121], così bassa da poter coprire l'intera regione di Bruxelles e, probabilmente, la maggior parte del paese, eludendo, *de facto*, le indicazioni provenienti dalla Corte di giustizia[122].
Da quanto detto, e al netto della condivisibilità o meno delle censure mosse alle diverse proposte di cui si è dato conto, emerge l'estrema difficoltà degli ordinamenti nazionali nel cristallizzare, in una normativa di settore, i numerosi principi enucleati a livello della giurisprudenza di europea. Come si è visto, il ricorso ad un criterio geografico – che, a prima vista, potrebbe apparire come un equilibrato compromesso tra esigenze securitarie e tutela della *privacy* –

[119] Per un'analisi della quale, v. VAN DE HEYNING, *Data Retention in Belgium*, in *European Constitutional Courts towards Data Retention Laws*, cit., 53 ss.
[120] *https://www.lachambre.be/FLWB/PDF/55/2572/55K2572001.pdf,* 181 (trad. nostra).
[121] Si veda, in tal senso, la mappa interattiva *online* predisposta dall'eurodeputato Patrick Breyer che dimostrerebbe come il sistema di controllo belga attualmente in discussione potrebbe riguardare l'intero territorio nazionale (*https://www.patrick-breyer.de/en/targeted-data-retention-online-map-shows-what-the-belgian-government-wants-to-hide/*).
[122] Per ulteriori censure mosse alla proposta di riforma anteriormente alla recente approvazione in Commissione, si rinvia a FORMICI, *La disciplina della* data retention, cit., 314 ss.

mostra, all'atto della sua applicazione, indiscutibili profili critici, destinati forse ad incidere sulla stessa tenuta di quei principi (proporzionalità, necessità etc.) ai quali si vorrebbe dare (condivisibilmente) attuazione.

6. *Conclusioni*. Il recente arresto comunitario sembra imporre un ripensamento della neo-introdotta disciplina ad opera del d.l. n. 132/2021[123].
In effetti, nonostante il legislatore italiano abbia mostrato di recepire alcuni tra i più importanti insegnamenti della Corte di giustizia, il «selettivo»[124] intervento normativo evidenzia alcune lacune di disciplina che, messe nuovamente in luce dalla recente sentenza *G.D.*, assumono una consistenza tutt'alto che irrilevante.
Sembra mettersi in rilievo come l'approccio all'inquadramento della disciplina dell'acquisizione dei tabulati telefonici non si ponga nella prospettiva di una visione d'insieme della tematica. D'altronde non è difficile immaginare che anche nel nostro Paese sia ipotizzabile per utilizzo investigativo una conservazione rapida dei dati contenuti nei tabulati telefonici.
Dunque, le questioni che si pongono sono due: la prima riguarda la possibilità di ottenere dai gestori telefonici la conservazione mirata, per un tempo definito, di tabulati telefonici, e la seconda, l'individuazione dei criteri che giustifichino tale richiesta.
Quanto alla prima questione, tralasciando, perché estranee alle finalità del presente lavoro, il problema della modalità di conservazione di quei dati prima che siano acquisiti dall'autorità giudiziaria, in qualsiasi modo e qualsiasi fine, ovvero presso i *providers* (con la possibilità che parte dei dati possano essere persi o conservati solo parzialmente) questa non può che ritenersi assolutamente possibile alla luce dalla disciplina relativa alla *data retention* come modificata dal Legislatore del 2021.
Più complessa, forse, la soluzione alla seconda problematica. Se, infatti, volessero essere accolti i *dicta* della Corte di giustizia – riconoscendo la illegittimità

[123] Questa è anche l'opinione espressa da FILIPPI, *La Corte di Lussemburgo ribadisce lo stop ai tabulati*, cit.
[124] FORMICI, 'The three Ghosts of data retention*': passato, presente e futuro della disciplina italiana in materia di conservazione e acquisizione dei metadati per scopi investigativi. Commento a margine del d.l. 30 settembre 2021, n. 132 e relativa legge di conversione*, in *Rivista AIC*, 2022, 1, 164, la quale soggiunge condivisibilmente come la novella *de qua*, «riguardando solo la disciplina della acquisizione dei metadati», non sarebbe stata «del tutto puntuale e debitamente approfondita».

di una conservazione generalizzata dei dati – occorrerebbe stabilire sulla base di quali criteri l'autorità giudiziaria possa richiederne la conservazione mirata[125]. Nel nostro ordinamento non sono inusuali discipline differenziate in caso di procedimenti per imputazioni particolarmente gravi (si pensi alla disciplina prevista per l'autorizzazione a disporre intercettazioni ovvero al meccanismo di proroga delle indagini). Sul tema, però, non possono nascondersi le preoccupazioni di parte della dottrina che, proprio con riferimento ai poteri investigativi derivanti dalla scelta in ordine all'iscrizione del pubblico ministero, mette in evidenza che la discrezionalità di cui gode l'organo investigativo al momento della iscrizione della notizia di reato determina, di fatto, l'ambito delle investigazioni consentite senza che sia prevista alcuna forma di controllo da parte del giudice[126]. Non è mancato chi si sia interessato dei possibili abusi – da intendersi

[125] In verità, anche la Corte EDU, Sez. II, 4 giugno 2019, *Sigurður Einarsson* c. Islanda, si è occupata più genericamente di *full collection of data*. In quell'occasione era stato disposto un sequestro di un'enorme mole di documenti digitali riferibili agli indagati e pertinenti ai reati contestati salvo poi effettuare una selezione prima a mezzo di un *software* e poi con una successiva revisione cartacea dei documenti così ottenuti, e solo quest'ultima veniva resa accessibile alla difesa e poi utilizzata in giudizio. Con riferimento al lamentato diritto da parte degli imputati della *full disclosure* del materiale sequestrato, la Corte ha ritenuto che non vi sia stata alcuna violazione dell'art. 6 C.E.D.U. in quanto il materiale non prodotto non è stato tenuto in considerazione dall'accusa, né prodotto in giudizio. Ciononostante, la Corte ha posto l'accento sulla opportunità, almeno in linea di massima, di coinvolgere anche la difesa, in modo che almeno i criteri di selezione dei dati siano condivisi. Sulle possibili implicazioni del principio, non del tutto chiaro e articolato, v. BARTOLI, *Parità delle armi e* discovery *digitale: qualche indicazione da Strasburgo*, in *www.lalegislazionepenale.eu*, 13 gennaio 2022, 7 ss. Ipotizza modalità con le quali effettuare la procedura partecipata per la selezione delle informazioni memorizzate a seguito di sequestro informatico, PISATI, Full collection of data *e diritto di difesa*, in *Riv. it. dir. proc. pen.*, 2019, 2243. L'Autore richiama anche la pronuncia della Corte EDU, 25 luglio 2019, *Rook* c. Germania, nella quale, invece, si lamentava l'impossibilità di disporre del tempo necessario per preparare la difesa in ragione dell'enorme quantità di *files* da esaminare. La Corte, nel rigettare il ricorso, ha ritenuto che nel caso di *full collection of data* sia il diritto di difesa a recedere tenuto conto che la 'ragionevole durata' non può essere pregiudicata dalla quantità di materiale da consultare ma che sia sufficiente, alla difesa, avere la possibilità di ricercare gli eventuali *files* a discarico rilevanti. Nelle conclusioni, condivisibilmente, l'Autore mette in evidenza «la tendenza a rivedere al ribasso, in presenza di *digital forensics*, le garanzie difensive» auspicando «un intervento chiarificatore sulla sussistenza, o meno, dell'obbligo di *disclosure* della *full collection of data*, nonché sui modi, sui costi e sui tempi, prima, della valutazione della rilevanza e, poi, dell'esame della documentazione estratta».

[126] Il problema dei cc.dd. «addebiti sommari e provvisori», che si susseguono durante lo sviluppo procedimentale nella fase *pre-trial*, è analizzato con rigore da RUGGIERI, *La giurisdizione di garanzia nelle indagini preliminari*, Milano, 1996, 159. In particolare, con riferimento all'uso distorto di addebiti

nel senso di comportamenti non necessariamente accompagnati da un elemento soggettivo definibile in termini di dolo o colpa ma, piuttosto, anche secondo quanto affermato dalla giurisprudenza delle Sezioni unite, di esercizio di diritti o facoltà processuali per scopi diversi da quelli dalla legge assegnati[127] – dell'atto processuale ad opera del pubblico ministero nel momento in cui questi effettua le scelte relative all'imputazione[128].

Ferme restando queste preoccupazioni, e fatte salve le considerazioni della Corte circa l'illegittimità di una conservazione generalizzata dei dati, potrebbe ipotizzarsi, allora, il meccanismo per il quale solo previa iscrizione *ex* art. 335 c.p.p. di procedimenti per reati di cui all'art. 51, comma 3-*bis* c.p.p., ovvero – ove volesse ritenersi di assimilare le due discipline – di quelli di cui all'art. 266, comma 2, c.p.p., sia possibile disporre – su autorizzazione del giudice – la conservazione di dati per un termine prestabilito dallo stesso. In questo modo il giudice sarebbe anche in grado di controllare e verificare l'utilità di una successiva acquisizione, e potrebbero superarsi le perplessità per criteri non oggettivabili e potenzialmente discriminatori.

I tempi sembrerebbero essere maturi, poi, affinché il controllo del giudice si spinga oltre la mera valutazione dei presupposti formali circa la scelta del mezzo investigativo operata dal pubblico ministero ma, come da tempo si sostiene, questa verifica potrebbe riguardare anche la corretta qualificazione giuridica del fatto da cui discende la possibilità di utilizzare lo strumento tipico di indagine.

Potrebbe farsi ricorso alle "finestre giurisdizionali" ipotizzate durante i lavori della Commissione ministeriale nominata dalla Ministra Marta Cartabia il 16 marzo 2021 e poi previste nell'art. 1, comma 9, lett. q) e r) della legge n. 134 del 27 settembre 2021[129]; in quel caso il controllo riguarda la verifica della

---

sommari "per eccesso", ed in particolare, per quelli associativi e gli annessi poteri investigativi, v. MAFFEO, *Tempi e* nomina iuris *nelle indagini preliminari. L'incertezza del controllo*, Bari, 2020, 123 ss.

[127] Cass., Sez. un., 29 settembre 2011, n. 155, Rossi ed altri, Rv, n. 251496.

[128] Cfr. CATALANO, *L'abuso del processo*, Milano, 2004, 41; ILLUMINATI, *Abuso del processo, legalità processuale e pregiudizio effettivo*, in *Cass. pen.*, 2011, 3593, e MAFFEO, *Tempi e* nomina iuris *nelle indagini preliminari. L'incertezza del controllo*, cit., 124 s.

[129] Cfr. l. 27 settembre 2021, n. 134 recante "*Delega al Governo per l'efficienza del processo penale nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari*", in *G.U.*, 4 ottobre 2021, n. 237. Il decreto legislativo è stato approvato all'unanimità lo scorso 4 agosto dal Consiglio dei Ministri, su proposta della Ministra della Giustizia Cartabia, ed è stato inviato alle

tempestività dell'iscrizione nel registro di cui all'art. 335 c.p.p. consentendo al giudice la retrodatazione in caso di ingiustificato e inequivocabile ritardo[130].
Nel caso che ci occupa, dunque, potrebbe richiedersi al giudice per le indagini preliminari, competente per la fase, di verificare la corretta qualificazione giuridica del fatto così da evitare una compressione significativa dei diritti di riservatezza e segretezza delle comunicazioni ed assicurare in questo modo spazi di un reale contraddittorio, anche nella fase investigativa, soprattutto in situazioni critiche come quella prospettata.

commissioni parlamentari per i pareri di competenza, obbligatori ma non vincolanti, che dovranno essere resi entro sessanta giorni. Per quanto qui di interesse cfr. *Relazione illustrativa dello schema di decreto legislativo recante attuazione della legge 27 settembre 2021 n. 134 recante delega al governo per l'efficienza del processo penale nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari*, 82. Il testo della relazione è consultabile *on-line* sul sito *www.giustizia.it*.

[130] Occorre dare atto che, una prima proposta, in tal senso, fu sviluppata durante i lavori per l'elaborazione della Bozza di delega legislativa per l'emanazione del nuovo codice di procedura penale ad opera della Commissione, istituita con d.m. 27 luglio 2006, insediatasi il 3 agosto 2006, e presieduta dal Prof. Giuseppe Riccio (27 luglio 2006); alla direttiva 60.5 si era previsto il «potere-dovere del giudice, su istanza dell'interessato, subito dopo il compimento per la prima volta delle formalità di accertamento della costituzione delle parti nell'udienza di conclusione delle indagini preliminari o, se questa manchi, in giudizio, di accertare la data di effettiva acquisizione della notizia di reato, ai fini della valutazione di inutilizzabilità degli atti di indagine compiuti dopo la scadenza del termine di durata massima delle indagini preliminari».