DIRITTO PENALE CONTEMPORANEO

DIRITTO PENALE CONTEMPORANEO

Fascicolo
11/2018

ISSN 2039-1676

Diritto Penale Contemporaneo è un periodico on line, ad accesso libero e senza fine di profitto, nato da un'iniziativa comune di Luca Santa Maria, che ha ideato e finanziato l'iniziativa, e di Francesco Viganò, che ne è stato sin dalle origini il direttore nell'ambito di una partnership che ha coinvolto i docenti, ricercatori e giovani cultori della Sezione di Scienze penalistiche del Dipartimento "C. Beccaria" dell'Università degli Studi di Milano. Attualmente la rivista è edita dall'Associazione "Diritto penale contemporaneo", il cui presidente è l'Avv. Santa Maria e il cui direttore scientifico è il Prof. Gian Luigi Gatta. La direzione, la redazione e il comitato scientifico della rivista coinvolgono oggi docenti e ricercatori di numerose altre università italiane e straniere, nonché autorevoli magistrati ed esponenti del foro.
Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione.

La rivista fa proprio il Code of Conduct and Best Practice Guidelines for Journal Editors elaborato dal COPE (Comittee on Publication Ethics).

***Peer review*.**
Salvo che sia diversamente indicato, tutti i contributi pubblicati nella sezione *papers* di questo fascicolo hanno superato una procedura di *peer review*, attuata secondo principi di trasparenza, autonomia e indiscusso prestigio scientifico dei revisori, individuati secondo criteri di competenza tematica e di rotazione all'interno dei membri del Comitato scientifico. Ciascun lavoro soggetto alla procedura viene esaminato in forma anonima da un revisore, il quale esprime il suo parere in forma parimenti anonima sulla conformità del lavoro agli standard qualitativi delle migliori riviste di settore. La pubblicazione del lavoro presuppone il parere favorevole del revisore. Di tutte le operazioni compiute nella procedura di *peer review* è conservata idonea documentazione presso la redazione.

Modalità di citazione.
Per la citazione dei contributi presenti nei fascicoli di *Diritto penale contemporaneo*, si consiglia di utilizzare la forma di seguito esemplificata: N. COGNOME, *Titolo del contributo*, in *Dir. pen. cont.*, fasc. 1/2017, p. 5 ss.

11/2018

NOVITÀ IN TEMA DI *DATA RETENTION*. LA RIFORMULAZIONE DELL'ART. 132 CODICE *PRIVACY* DA PARTE DEL D.LGS. 10 AGOSTO 2018, N. 101

di Silvia Signorato

Abstract. La disciplina di *data retention* prevista dall'art. 132 codice *privacy* è stata oggetto di numerose riformulazioni. Il presente scritto mira ad analizzare le modifiche da ultimo apportate dal d.lgs. 10 agosto 2018 n. 101. Accanto ad opportune chiarificazioni normative, emergono aspetti più critici. Il tema centrale è rappresentato dalle tempistiche di conservazione dei dati. Al riguardo, l'autrice dimostra come, da una lettura sinottica dell'art. 132 codice *privacy* e dell'art. 24 cd. legge europea 2017, emerga la tendenziale dilatazione a settantadue mesi di tali tempistiche in rapporto alla repressione di tutte le tipologie di reato.

1. Premessa.

Il d.lgs. 10 agosto 2018 n. 101[1] ha riscritto, ritessendola, la trama del codice *privacy*. Si tratta di una riforma di estrema importanza che intende dare attuazione al cd. pacchetto europeo protezione dati[2] e, quindi, sia al Regolamento (UE) 2016/679 – peraltro

[1] Recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 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 (Regolamento generale sulla protezione dei dati).

[2] Consapevole delle problematiche sollevate dal trattamento dei dati personali, il legislatore europeo, con un *iter* iniziato nel 2012, ha da ultimo ripensato l'intera materia con l'obiettivo di regolamentarne ogni ambito. Ne è derivato il cd. pacchetto protezione dati, che fa perno su due atti entrambi pubblicati nella Gazzetta ufficiale dell'Unione europea del 4 maggio 2016, L 119/1. Tali atti si identificano nel:
a) Regolamento (UE) 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 (cd. regolamento generale sulla protezione dei dati

già efficace in virtù dell'applicabilità diretta che lo caratterizza[3] – sia alla Direttiva (UE) 2016/680[4].

---

o GDPR quale acronimo di *General Data Protection Regulation*). Tale Regolamento è direttamente applicabile in tutti gli Stati membri a partire dal 25 maggio 2018 (come previsto dall'art. 99, comma 2, del Regolamento, la data di applicazione dello stesso è stata differita rispetto alla sua entrata in vigore, coincidente con il 24 maggio 2016. Quanto all'oggetto dell'atto, esso attiene al «trattamento interamente o parzialmente automatizzato di dati personali o al trattamento non personale di dati personali contenuti in un archivio o destinati a confluirvi (cfr. art. 2 Regolamento (UE) 2016/679)». Per espressa previsione, restano però escluse dall'ambito di applicazione materiale del regolamento quattro tipologie di trattamenti: quelli che non rientrano nel campo di applicazione del diritto dell'Unione; quelli effettuati dagli Stati membri in relazione alla politica estera ed alla sicurezza comune dell'Unione (si tratta nello specifico dei trattamenti praticati nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo II, TUE); i trattamenti operati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico; infine, i trattamenti effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

b) Il secondo atto che compone il pacchetto protezione dati si identifica nella Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (per un approfondimento della direttiva, cfr. S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018, p. 87 ss.). Tale direttiva è entrata in vigore il 5 maggio 2016 con l'obbligo per gli Stati di conformarvisi entro il 6 maggio 2018. Essa incide su una materia delicatissima, date le significative problematiche che si incuneano nel bilanciamento tra esigenze securitarie e *privacy* e che lo rendono tutt'altro che agevole, essendo sempre presente il rischio di due derive. Da un lato, quella che in nome dell'efficacia investigativa postula il trattenimento indiscriminato di ogni tipo di dato, fino ad arrivare a vere e proprie schedature di massa. Dall'altro, quella che sotto il manto di una nobile, ma mistificata, tutela della *privacy* finisce per propugnare tempistiche di conservazione dei dati a fini d'indagine che minano le fondamenta stessa dell'efficacia investigativa. *Privacy* ed esigenze securitarie non sono esigenze alternative, ma compensative. L'una non esclude l'altra e ciascuna deve essere bilanciata con l'altra.

Se il Regolamento (UE) 2016/679 e la Direttiva (UE) 2016/680 rappresentano gli atti centrali del pacchetto protezione dati, ad esso è peraltro riconducibile anche la Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.

[3] Per un approfondimento ragionato sugli atti normativi dell'Unione europea e sulla loro efficacia cfr., per tutti, R.E. KOSTORIS, *Diritto europeo e giustizia penale*, in R.E. Kostoris (a cura di), *Manuale di procedura penale europea*, III ed., Giuffrè, Milano, 2017, p. 21 ss.

[4] Anche se la denominazione del decreto si riferisce soltanto alle disposizioni del Regolamento (UE) 2016/679, esso non manca di dare attuazione pure alla Direttiva 2016/680, peraltro già attuata ad opera del d.lgs. 18 maggio 2018, n. 51 (*Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio*). In materia di trattamento dei dati personali da parte delle forze di polizia, cfr. anche d.p.r. 15 gennaio 2018, n. *15* recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per finalità di polizia, da organi, uffici e comandi di polizia. Si veda inoltre MINISTERO DELL'INTERNO, DIPARTIMENTO DELLA PUBBLICA SICUREZZA, DIREZIONE CENTRALE PER GLI AFFARI GENERALI DELLA POLIZIA DI STATO, *Circolare illustrativa del nuovo quadro normativo in materia di protezione dei dati personali*, 6 luglio 2018, nonché S. SIGNORATO, *Il trattamento dei dati da parte delle forze di polizia: la nuova disciplina prevista dall'art. 53 codice* privacy *e gli scenari europei*, in R.E.

Nel novellare il codice *privacy*, il d.lgs. 10 agosto 2018 n. 101 ha inciso su norme riconducibili a vari ambiti giuridici, tra cui anche quello del processo. Il presente scritto mira ad esaminare le modifiche apportate dall'art. 11, d.lgs. 10 agosto 2018 n. 101 all'art. 132 codice *privacy*. Quest'ultima previsione appare di particolare rilievo nell'ambito processuale penale[5], ma travagliatissima per i continui cambiamenti e ritocchi che l'hanno interessata.

Per comprendere la riformulazione operata dal d.lgs. 10 agosto 2018 n. 101, occorre preliminarmente ricordare come i fornitori di comunicazione elettronica (si pensi a coloro che erogano servizi di comunicazioni di telefonia mobile) possano disporre di dati dal rilievo talora strategico in ambito investigativo quali i numeri telefonici di chi effettua le chiamate e di chi le riceve, la durata della conversazione, i dati relativi alla localizzazione del dispositivo mobile, l'indirizzo IP. Proprio la possibile valenza investigativa ed accertativa di tali dati ha determinato l'emanazione di discipline cd. di *data retention*, vale a dire di discipline volte a fissare in capo ai fornitori di comunicazione elettronica, per finalità di accertamento e repressione dei reati, specifici obblighi di conservazione di taluni dati per predeterminati archi temporali. Un simile obbligo attiene però ai soli dati esterni alle comunicazioni[6], restando sempre preclusa la conservazione dei contenuti comunicativi, al fine di salvaguardare quantomeno la libertà e la segretezza delle comunicazioni.

Nel nostro ordinamento, la disciplina di *data retention* è fissata in via primaria all'art. 132 codice *privacy*. L'art. 11 del d.lgs. 10 agosto 2018 n. 101 ne ha da ultimo modificato i commi 3 e 5 ed ha inserito un nuovo comma 5-*bis*. È proprio da quest'ultimo che sembra opportuno muovere, perché esso recepisce, riaffermandolo, il previgente stravolgimento, passato peraltro inosservato, dei tempi di conservazione dei dati fissati dalla disciplina dell'art. 132 codice *privacy*.

Kostoris – F. Viganò (a cura di), *Il nuovo 'pacchetto' antiterrorismo*, Giappichelli, Torino, 2015, p. 91 ss.; ID., *Il trattamento dei dati personali per fini di prevenzione e repressione penale,* in *Riv. dir. proc.*, fasc. 6, 2015, p. 1484 ss.

[5] Si può rilevare come il considerando 20 della direttiva (UE) 2016/680 faccia un espresso riferimento alle norme di *procedura penale* quale ambito in cui specificare le operazioni e le procedure di trattamento dei dati personali effettuate da autorità giurisdizionali e da altre autorità giudiziarie.

[6] Parte della dottrina pone in luce come gli sviluppi tecnologici rendano talora non agevole la separazione tra dati comunicativi e non comunicativi. In argomento, cfr. L. BACHMAIER WINTER, *Criminal investiagation and right of privacy: the case-law of the European Court of Human Rights and its limits*, in *Lex ET Scientia*, Juridical Series, vol. 2, 2009, p. 12, nonchè G. DI PAOLO, voce *Prova informatica (diritto processuale penale),* in *Enc. Dir., Ann.*, vol. VI, Milano, 2013, p. 754. Per un approfondimento sull'acquisizione dei dati esterni delle comunicazioni nel quadro dell'ordine europeo di indagine penale e del relativo decreto attuativo, cfr. M. CAIANIELLO, *L'attuazione della direttiva sull'ordine europeo di indagine penale e le sue ricadute nel campo del diritto probatorio*, in *Cass. pen.*, 2018, p. 2211 ss. L'autore non manca di rilevare il rischio «che il nostro paese sconti un deficit di tutela strutturale, di certo non cagionato (ma potenzialmente amplificato) dall'operare della direttiva».

2. *Data retention:* verso i settantadue mesi di conservazione per tutte le tipologie di reato. La necessità di una lettura sinottica tra art. 132 codice *privacy* riformato ed art. 24 della cd. legge europea 2017.

Probabilmente nell'ottica di fugare ogni dubbio interpretativo sul piano della successione delle leggi nel tempo il nuovo comma 5-*bis* dell'art. 132 codice *privacy* prevede che è «fatta salva la disciplina di cui all'articolo 24 della legge 20 novembre 2017, n. 167[7]» (cd. legge europea 2017). In una prospettiva di contrasto al terrorismo, quest'ultimo articolo stabilisce che, in deroga all'art. 132 codice *privacy*, il termine di conservazione dei dati di traffico telefonico, telematico e relativo alle chiamate senza risposte sia di settantadue mesi in rapporto all'accertamento ed alla repressione, da un lato, dei delitti consumati o tentati con finalità di terrorismo (art. 51 comma 3 *quater* c.p.p.) e, dall'altro, dei reati ricompresi nell'elenco fissato all'art. 407 comma 2 lett. a c.p.p.[8].

Tale disciplina dilata di molto i tempi di conservazione dei dati previsti per le altre tipologie di reato dall'art. 132 codice *privacy*. Infatti, quest'ultimo prevede che, a partire dalla data della comunicazione, i fornitori di servizi di comunicazione sono obbligati a conservare per ventiquattro mesi i dati di traffico telefonico; per dodici mesi quelli di traffico telematico; per trenta giorni i dati relativi alle chiamate senza risposta. Si tratta di uno scaglionamento che solleva non poche perplessità. Anzitutto, i tempi di conservazione dei dati attinenti alle chiamate senza risposta risultano spesso incompatibili non solo con le tempistiche investigative ma, talora, addirittura con quelle relative alla stessa apprensione della notizia di reato. In un'epoca in cui le comunicazioni elettroniche hanno ormai preso il sopravvento su quelle di telefonia classica, appare poi del tutto irragionevole che i dati di traffico telematico debbano essere conservati per una tempistica dalla durata dimidiata rispetto a quella dei dati di traffico telefonico. Parimenti irragionevole sembra anche la previsione di tempi di conservazione differenti a seconda del tipo di traffico che venga di volta in volta in rilievo[9].

Da una lettura sinergica delle discipline fissate dall'art. 132 codice *privacy* e dall'art. 24 legge europea, si potrebbe pensare che il quadro complessivo della disciplina in tema di *data retention* si moduli in una sorta di doppio binario a seconda del tipo di reato perseguito. Da un lato, i tempi di conservazione sarebbero di regola scanditi nelle tempistiche di ventiquattro mesi, dodici mesi, trenta giorni previste dall'art. 132 codice *privacy*. Dall'altro, nei casi in cui vengano in rilievo reati a matrice terroristica o previsti

---

[7] Recante disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea.

[8] Si tratta dei delitti di cui agli artt. 285 c.p. (devastazione, saccheggio e strage), 286 c.p. (guerra civile), 416-*bis* c.p. (associazioni di tipo mafioso anche straniere), 422 c.p. (strage), 291-*ter*, limitatamente alle ipotesi aggravate previste dalle lettere a), d) ed e) del comma 2, e 291-*quater*, comma 4, del testo unico delle disposizioni legislative in materia doganale approvato con decreto del Presidente della Repubblica 23 gennaio 1973, n. 43.

[9] Sottolinea come la *ratio* originaria fosse verosimilmente quella di ridurre i costi legati alla conservazione dei dati, T. RAFARACI, *Intercettazioni e acquisizioni di tabulati telefonici*, in R.E. KOSTORIS – R. ORLANDI (a cura di), *Contrasto al terrorismo interno e internazionale,* Giappichelli, Torino, 2006, p. 276.

dall'art. 407 comma 2 lett. a, i tempi di conservazione sarebbero dettati dalla legge europea 2017 e, quindi, coinciderebbero in settantadue mesi.

Una lettura in termini di doppio binario si caratterizzerebbe però per un parziale errore di parallasse. Una simile impostazione finirebbe infatti per dimenticare che nel momento in cui il fornitore è chiamato a conservare i dati non gli è affatto noto né se quei dati gli verranno prima o poi richiesti da un'autorità giudiziaria (e, quindi, se atterranno o no ad un reato), né per quale tipologia di reato potranno essergli eventualmente richiesti. Ne deriva che il fornitore, per adempiere ai suoi obblighi, non potrà fare altro che conservare in ogni caso tutti i dati di traffico per settantadue mesi, a meno che la richiesta di trasmissione di dati gli giunga entro i termini previsti dal codice *privacy* ed attenga alla repressione di un reato non previsto dalla legge europea 2017.

In conclusione, a partire dalla legge europea 2017, il tempo di conservazione dei dati deve ritenersi mutato in rapporto all'accertamento ed alla repressione di *tutti* i reati. Infatti, a prescindere dal tipo di reato perseguito il periodo di conservazione dei dati finisce sempre più spesso per coincidere con quello di settantadue mesi.

La conseguenza è tutt'altro che di scarsa rilevanza. L'entrata in vigore dell'art. 24 della legge europea 2017 (di cui l'art. 11 del d.lgs. 10 agosto 2018 n. 101 fa salva la vigenza, rimarcandola mediante l'introduzione del comma 5-*bis*), erode l'applicabilità dell'art. 132 comma 1 ed 1 *bis* codice *privacy* per la parte in cui esso fissa le tempistiche di conservazione dei dati. La disciplina emergenziale stabilita per il terrorismo tende quindi a divenire disciplina ordinaria.

L'art. 132 comma 1 ed 1 *bis* codice *privacy* conserva peraltro operatività sotto un altro profilo. Per comprenderlo, occorre ricordare che nel momento della trasmissione dei dati all'autorità giudiziaria il fornitore è obbligato a verificare che gli stessi siano riconducibili al periodo di conservazione che, a seconda del tipo di reato perseguito, risulta fissato dall'art. 132 comma 1 ed 1 *bis* codice *privacy* o dalla legge europea 2017. Se, ad esempio, un dato da conservarsi per ventiquattro mesi (ma di fatto conservato per settantadue mesi per la ricordata ragione che è impossibile conoscere a priori per quale tipo di reato quel dato verrà richiesto), fosse richiesto dopo ventiquattro mesi ed un giorno sarebbero illegittime tanto la sua trasmissione quanto la sua acquisizione da parte dell'autorità giudiziaria[10].

In definitiva, un conto è la tempistica di conservazione che tende ad assestarsi in settantadue mesi, altro conto è invece la tempistica che rende legittimamente trasmissibili all'autorità giudiziaria e legittimamente acquisibili dalla stessa i dati conservati all'interno di un determinato arco temporale.

[10] Già prima dell'ultima riforma, la giurisprudenza aveva affermato l'inutilizzabilità dei dati relativi al traffico telefonico contenuti nei tabulati acquisiti dall'Autorità giudiziaria successivamente al decorso dei termini previsti dall'art. 132 del d.lgs. 30 giugno 2003 n. 196, atteso il divieto di conservazione degli stessi da parte del gestore oltre il periodo normativamente predeterminato. Per questa impostazione, tra le altre, cfr. Cass. pen., Sez. V. 25 gennaio 2016, n. 7265, nonché Cass. pen., Sez. V, 5 dicembre 2014, n. 156113.

3. Le modifiche apportate dalla novella ai commi 3 e 5 dell'art. 132 codice *privacy*.

Come si è visto, l'introduzione nell'art. 132 codice *privacy* del comma 5-*bis*, pur limitandosi a riaffermare l'esistente, finisce per avere una portata di largo impatto sul sistema. Facendo salva la vigenza dell'art. 24 della cd. legge europea 2017, tale disciplina contribuisce infatti a rimarcare la tendenziale ordinarietà di un regime concepito invece come eccezionale.

Quanto alle modifiche apportate ai commi 3 e 5 dell'art. 132 codice *privacy*, esse appaiono di coordinamento o di chiarificazione della previgente disciplina.

Nello specifico, la novella attua una modifica del comma 3 nella parte che regola l'acquisizione di dati relativi alle chiamate in arrivo (cd. traffico in entrata)[11]. In proposito, la versione precedente stabiliva che tale acquisizione potesse avvenire ad opera del difensore dell'imputato o della persona sottoposta alle indagini mediante richiesta diretta al fornitore «ferme restando le condizioni di cui all'art. 8, comma 2, lettera f, per il traffico entrante» (norma che fissa la necessità di dimostrare che la richiesta dei dati sia volta a prevenire il verificarsi di un pregiudizio effettivo e concreto per le indagini difensive). Opportunamente, la riforma semplifica la lettura della norma. Essa elimina il riferimento all'art. 8, comma 2, lettera f, sostituendolo con la seguente previsione: «La richiesta di accesso diretto[12] alle comunicazioni telefoniche in entrata può essere effettuata solo quando possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397».

In un'ottica di armonizzazione con il Regolamento (UE) 2016/679, al comma 3 dell'art. 132 codice *privacy* viene inoltre stabilito che i diritti dell'interessato previsti dagli articoli da 12 a 22[13] del Regolamento possano essere esercitati secondo le modalità fissate

---

[11] Come è noto, la norma detta una disciplina differente per l'acquisizione del traffico «in entrata» e «in uscita». Solo in quest'ultimo caso, infatti, risulta la richiesta del difensore corredata dell'atto di conferimento dell'incarico. Diversamente, nel caso del traffico «in entrata» è anche necessario che dalla non acquisizione possa derivare un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397. In dottrina si registrano posizioni differenti in ordine alla ragionevolezza di tale differenziazione. Da un lato, infatti, vi è chi afferma che «il ragionamento che ha portato il legislatore a distinguere le chiamate in entrata da quelle in uscita, tutelando le prime più delle seconde, rimane piuttosto misterioso» (cfr. A. CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv.it.dir.proc.pen.*, 2005, p. 612). Dall'altro, vi è invece chi ritiene «agevolmente decifrabili, e comprensibili, le ragioni della separazione normativa delle comunicazioni "in uscita" da quelle "in entrata"» (cfr. E. ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, Wolters Kluver-Cedam, 2018, p. 131.

[12] Quindi, senza la necessità dell'emissione di un decreto motivato a seguito di istanza del difensore dell'imputato o della persona sottoposta alle indagini.

[13] Quanto ai contenuti di tali articoli, essi si sostanziano nei seguenti: informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato (art. 12); informazioni da fornire qualora i dati personali siano raccolti presso l'interessato (art. 13); informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato (art. 14); diritto di accesso dell'interessato (art. 15); diritto di rettifica (art. 16); diritto alla cancellazione o diritto all'oblio (art. 17); diritto di limitazione di trattamento (art. 18); obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento (art. 19); diritto alla portabilità dei dati (art. 20); diritto di opposizione (art. 21); processo decisionale automatizzato relativo

dall'«articolo 2-*undecies*, comma 3, terzo, quarto e quinto periodo», che attengono all'esercizio dei diritti per il tramite del Garante[14]. Sul piano della tecnica normativa, si può rilevare come il riferimento addirittura ai periodi contenuti all'interno di un comma finisca per ostacolare la lettura e la comprensione della previsione.

Venendo alla modifica apportata al comma 5 dell'art. 132 codice *privacy*, occorre ricordare come, *ante* riforma, tale norma prevedesse che il trattamento dei dati personali fosse effettuato con l'osservanza delle misure e degli accorgimenti a garanzia dell'interessato previsti dall'art. 17 in tema di trattamento che presenta specifici rischi. La novella elimina il riferimento all'art. 17, stabilendo che gli accorgimenti e le garanzie sono quelli fissati dal Garante secondo le modalità individuate dall'articolo 2-*quinquiesdecies* per i trattamenti dal rischio elevato in rapporto all'esecuzione di un compito di interesse pubblico. Occorrerà inoltre tenere conto anche della necessità di indicare le modalità tecniche che verranno impiegate per la periodica distruzione dei dati[15].

4. Conclusioni.

Gli apporti tecnologici e la possibilità di combinare ed elaborare tra loro i dati rendono ormai possibile una sorta di "mappatura" di abitudini, gusti, orientamenti politici, religiosi di una persona sino a poterne determinare una sorta di controllo orwelliano su scala globale.

Si assiste ad una progressiva reificazione dello stesso concetto di persona che, allontanandosi dal proprio nucleo fondativo, finisce per identificarsi nell'insieme di dati da commercializzare o comunque utilizzare. L'incidenza che il trattamento dei dati personali può determinare sul piano dei diritti fondamentali è dunque davvero significativa e plurima, sia per la molteplicità dei diritti coinvolti (si pensi ad esempio al diritto alla protezione dei dati personali, al diritto all'oblio, alla libertà di pensiero e di espressione, ecc.), sia per il grado di lesione che ciascuno di tali diritti può subire nel caso specifico.

Il rischio che il trattamento di dati personali si trasformi in un mezzo di controllo e di dominio è effettivo. Per questo motivo, anche a livello normativo, si rimarca come esso «dovrebbe essere al servizio dell'uomo»[16]. Invero, l'uso dell'indicativo "deve" in luogo del condizionale "dovrebbe" sarebbe parsa una scelta lessicale più adeguata essendo in gioco la stessa concezione di persona e la stessa libertà dell'individuo almeno in talune sue significative forme di espressione.

---

alle persone fisiche, compresa la profilazione (art. 22).

[14] Secondo le modalità di cui all'art. 160 codice *privacy*.

[15] L'art. 11, comma 2, lett. i, n. 5, d. lgs. 10 agosto 2018 n. 101 elimina invece il riferimento alla previsione di specifici sistemi di autenticazione informatica e di autorizzazione degli incaricati del trattamento di cui all'allegato B.

[16] Cfr. considerando n. 4, Regolamento (UE) 2016/679.

Resta comunque la necessità di bilanciare adeguatamente le esigenze che presiedono al trattamento dei dati personali con gli altri diritti che di volta in volta vengono in rilievo. Una simile calibratura appare però tutt'altro che agevole. Lo stesso legislatore europeo sembra essersi imbattuto, con la direttiva 2006/24/Ce (cd. direttiva Frattini[17]), nelle secche di un inadeguato bilanciamento tra diritto alla protezione dei dati personali ed esigenze di pubblica sicurezza, se è vero che tale direttiva è stata dichiarata invalida dalla Corte di Giustizia proprio per violazione del principio di proporzionalità nel contemperamento tra tali fattori[18].

La disciplina di *data retention* si configura quindi come un terreno minato, in cui si misurano le spinte e le controspinte tra esigenze securitarie e *privacy*. L'attuale previsione italiana di conservazione dei dati esterni alle comunicazioni per settantadue mesi (sei anni) delinea una tempistica particolarmente dilatata, dissonante rispetto agli orientamenti europei in materia.

È noto come in nome della *privacy* si tenda infatti a restringere il più possibile il periodo di conservazione dei dati. Al riguardo, individuare però un arco temporale ideale non è agevole, anche se, tenendo conto della realtà investigativa e difensiva, qualsiasi eventuale riforma dovrebbe almeno assicurare un periodo di trentasei mesi, senza però superare quello di settantadue[19].

Si è consapevoli che una simile impostazione si scontra con quella prevalente, anche sul piano europeo, volta ad affermare la necessità di tempi di conservazione assai più brevi. Non di rado si tratta però di approcci sbilanciati nella direzione di una aprioristica tutela della *privacy*. Sia chiaro: la *privacy* rappresenta un diritto fondamentale da garantire al massimo grado; ma non bisogna dimenticare che la *privacy* è pur sempre un diritto che deve essere contemperato con altre esigenze. Non solo quella di accertamento dei reati[20], ma anche quella di difesa, se è vero che tabulati telefonici e dati come l'indirizzo IP possono talora assurgere a prova dell'infondatezza degli addebiti.

---

[17] Per un'analisi in chiave critica di tale direttiva, cfr. C. CONTI, *L'attuazione della direttiva Frattini: un bilanciamento insoddisfacente tra riservatezza e diritto alla prova,* in S. LORUSSO (a cura di), *Le nuove norme sulla sicurezza pubblica,* Cedam, Padova, 2008, p. 3 ss.

[18] Cfr. C. Giust., Grande Sezione, 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Right Ireland Ltd c. Minister for Communications, Marine and Natural Resources*. Al riguardo, cfr. R. FLOR, *La Corte di Giustizia considera la direttiva europea 2006/24 sulla cd. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Dir. pen. cont. – Riv. trim.*, n. 2/2014, p. 178 ss. Per una riflessione su una delle prime sentenze di merito successive alla declaratoria di invalidità, cfr. R. FLOR, *Data retention ed art. 132 Cod. privacy: vexata quaestio (?)*, in questa *Rivista*, fasc. 3/2017, p. 356 ss.; F. RUGGIERI, *Data retention e giudice di merito penale. Una discutibile pronuncia,* in *Cass. pen.*, 2017, p. 2483 ss. Sul tema del bilanciamento tra esigenze securitarie e *privacy* si veda anche *C. Giust., Grande Sezione, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, Tele2 Sverige AB c. Post- och telestyrelsen e a.*.

[19] Non sfugge, peraltro, il rischio di possibili abusi, come ha dimostrato il noto caso dei «tabulati Telecom». In tema, si vedano le osservazioni di R. ORLANDI, *Questioni attuali in tema di processo penale e informatica*, in *Riv. dir. proc.*, 2009, p. 130.

[20] Si può ricordare come, nel processo per l'omicidio D'Antona, assunsero valore probatorio dati acquisiti secondo tempistiche di conservazione al tempo lecite, ma che attualmente esonderebbero rispetto a quelle previste dall'art. 132 codice *privacy*. In argomento, vedi V. RIZZI – N. GALLO – A. MAROTTA, *L'impronta telefonica. La ricostruzione di un attentato terroristico attraverso l'analisi dei contatti telefonici*, in M. Andretta – D. Fondaroli – G. Gruppioni (a cura di), *Dai «casi freddi» ai «casi caldi». Le indagini storico e forensi fra saperi*

giuridici e investigazioni scientifiche, Wolters Kluver Cedam, Padova, 2014, p. 171 ss.