LUCA D'AGOSTINO

La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al D.Lgs. 10 agosto 2018, n. 101

L'evoluzione normativa in materia di *privacy* ha fatto emergere nello scenario penalistico il dato personale quale oggetto di specifica tutela, che affonda le radici nel più ampio diritto alla riservatezza. Con il D. Lgs. 101/2018 il legislatore ha rivisitato l'apparato sanzionatorio del Codice della *privacy*, modificando le fattispecie previgenti, abrogandone altre, e introducendo due nuove ipotesi di reato. Il presente lavoro esamina in chiave critica il recente intervento riformatore, cercando di gettare luce su taluni profili problematici e soffermandosi in conclusione su possibili nuovi ambiti di intervento.

Regulatory developments in privacy laws led to the protection of personal data by means of criminal law, as an extension of right to private life. With the adoption il Legislative Decree 101/2018 Italian legislator amended the Privacy Act, by repealing and replacing some criminal offences and introducing two new incriminations. The article analyses critically the reforming Act, highliting some sensitive issues and focusing on possible new concerns.

1. Introduzione.

Il tema della protezione dei dati personali ha vissuto negli ultimi mesi una fase di estrema concitazione con l'approssimarsi del termine fissato dal Regolamento 2016//679/UE per la diretta applicabilità delle relative disposizioni[1]. La necessità di adeguare l'ordinamento nazionale alle disposizioni del GDPR, secondo quanto previsto dall'art. 13 della legge 25 ottobre 2017, n. 163 (c.d. legge di delegazione europea), è stata accompagnata da un'attenzione politica e mediatica sicuramente considerevole, anche tenuto conto dei contrapposti interessi delle categorie coinvolte. Dopo una prima bozza, che contemplava l'abrogazione *tout court* del Codice in materia di protezione dei dati persona-

[1] L'art. 99 del Regolamento prevede che, pur entrando in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale dell'Unione Europea, esso si applichi negli Stati membri a decorrere dal 25 maggio 2018.

li[2], il Governo ha mutato l'impostazione di fondo, elaborando un secondo schema di decreto legislativo[3], sottoposto all'esame del Parlamento per l'acquisizione del necessario parere delle Commissioni[4]. Con il nuovo testo il legislatore delegato ha preparato il tavolo per un intervento "chirurgico" sulle disposizioni del D. Lgs.196/2003, che fosse in grado di coordinare la normativa interna con le previsioni del Regolamento Generale senza eccessivi cambiamenti. A seguito del parere condizionato reso dalla competente Commissione parlamentare, il Consiglio dei Ministri ha definitivamente approvato il D. Lgs. 101/2018 di adeguamento del Testo Unico in materia di protezione dei dati personali alle disposizioni del GDPR[5].

In linea con i criteri direttivi contenuti nella delega[6], l'intervento riformatore ha avuto a oggetto anche l'appendice sanzionatoria del Codice della *privacy* (Titolo III), *ivi* comprese le fattispecie penali. La scelta del legislatore di mettere mano all'impianto sanzionatorio è una novità indubbiamente degna di nota.

Rivolgendo lo sguardo all'evoluzione storica della disciplina, emerge infatti un tendenziale immobilismo nella formulazione dei reati in materia di *privacy,* particolarmente evidente nel passaggio dalle disposizioni della legge 675/1996 al riordino effettuato con il D. Lgs. 196/2003[7]. Era infatti rimasta invariata

---

[2] La notizia, inizialmente diffusa da fonti giornalistiche, ha trovato conferma nel corso delle audizioni svolte in sede parlamentare. Si veda per approfondimenti l'articolo *Il Decreto di attuazione del regolamento Privacy: sconfessati i principi della prima bozza*, in *IlSole24Ore.com*.

[3] Il Consiglio dei ministri ha approvato, in esame preliminare, lo schema di decreto legislativo che è stato trasmesso alle Camere il 10 maggio 2018. Il successivo 23 maggio 2018 gli Uffici di Presidenza delle Commissioni speciali della Camera e del Senato, al fine di acquisire i necessari elementi istruttori per l'esame del provvedimento, hanno congiuntamente proceduto all'audizione di esperti e di rappresentanti della società civile, tra cui professionisti, operatori dei settori coinvolti e destinatari delle disposizioni in tema di *privacy*.

[4] Ai sensi dell'art. 31, co. 3, della legge 24 dicembre 2012 n. 234 la legge di delegazione europea prevede che sugli schemi dei decreti legislativi di recepimento sia acquisito il parere delle competenti Commissioni parlamentari della Camera dei deputati e del Senato della Repubblica, con la precisazione che, *«decorsi quaranta giorni dalla data di trasmissione, i decreti sono emanati anche in mancanza del parere»*.

[5] D. Lgs. 10 agosto 2018, n. 101 recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento 2016/679/UE 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», pubblicato in G.U. Serie Generale n. 205 del 04.09.2018.

[6] Si prevedeva espressamente che il Governo dovesse *«adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (UE) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse»* (art. 13, co. 3, lett. e).

[7] Con la riforma del 2003 non sono mutate le scelte di criminalizzazione e le tecniche di tutela penale

l'impostazione di fondo, caratterizzata dalla scelta di una penalizzazione 'a tappeto'[8] e da un ricorso forse troppo esteso[9] alla sanzione penale.
Il legislatore delegato si è inizialmente mosso in controtendenza, circoscrivendo l'ambito del penalmente rilevante alle sole condotte caratterizzate da maggiore offensività, in quanto animate dal fine di profitto[10]. Lo schema di decreto inizialmente licenziato dal Governo prevedeva infatti l'*abolitio* dei reati di omessa adozione di misure di sicurezza (art. 169 D. Lgs. 196/2003) e di inosservanza dei provvedimenti del Garante (art. 170), la configurazione dell'illecito trattamento di dati (art. 167) come reato di evento a dolo specifico di profitto, e l'introduzione di due nuove incriminazioni, la comunicazione e diffusione illecita di dati personali riferibili a un rilevante numero di persone (art. 167-*bis*) e l'acquisizione fraudolenta di dati personali (art. 167-*ter*)[11]. Le scelte di criminalizzazione sono tuttavia parzialmente mutate con l'approvazione del testo definitivo, nel quale ricompare il reato di inosservanza dei provvedimenti del Garante (art. 170 D. L.gs. 196/2003)[12] e si estende l'ambito applicativo dell'illecito trattamento di dati anche alle violazioni commesse al fine di arrecare danno ad altri. Trova invece conferma la scelta di depenalizzare il trattamento illecito effettuato senza il consenso dell'interessato[13].

---

del precedente impianto normativo, né si è posto rimedio alle disfunzioni e alle discrasie evidenziate dalla dottrina. In argomento, CORRIAS LUCENTE, *La nuova normativa penale a tutela dei dati personali,* in *Il codice dei dati personali. Temi e problemi*, Milano, 2004, 632; MANNA, *Il quadro sanzionatorio penale e amministrativo del codice sul trattamento dei dati personali*, in *Dir. inf.,* 2003, 2, 740; ID., *Prime osservazioni sul Testo Unico in materia di protezione dei dati personali: profili penalistici*, in *www.privacy.it*; VENEZIANI., *I beni giuridici tutelati dalle norme penali in materia di riservatezza informatica e disciplina dei dati personali,* in *Il diritto penale dell'informatica nell'epoca di internet*, a cura di Picotti, Padova, 2004 187

[8] L'espressione è di VENEZIANI, *Beni giuridici protetti e tecniche di tutela penale nella nuova legge sul trattamento dei dati personali,* in *Riv. trim. dir. pen. econ.* 1997, 1-2, 177

[9] SEMINARA, *Appunti in tema di sanzioni penali nella legge sulla privacy*, in *Resp. civ. e prev.,* 1998, 4-5, 919 parla di un uso "terroristico" della sanzione penale, criticando la scelta del legislatore di presidiare con la pena protezione dei dati personali *«per attribuire il massimo rilievo a precetti primari non ancora consolidati e di forzare così il loro impatto sulla società, accelerandone il processo di ricezione».*

[10] Sul tema, di recente, RESTA*, I reati in materia di protezione dei dati personali,* in *Cybercrime,* a cura di Cadoppi, Canestrari, Manna, Papa, Milano, 2019, 1019 ss.

[11] Veniva inoltre riformulato il delitto di cui all'art. 168 prevedendo la rilevanza penale, oltre del mendacio nelle comunicazioni, anche delle condotte di ostacolo all'esercizio delle funzioni (*Amplius* § 4.3 e 5).

[12] Nel citato parere sullo schema di decreto la Commissione aveva espresso il proprio disappunto circa l'abrogazione dell'art. 170 poiché in controtendenza rispetto alle scelte compiute quasi in sede di recepimento della direttiva 2016/680/UE sul trattamento dei dati personali nelle attività di contrasto.

[13] Il campo di operatività dell'incriminazione viene ridimensionato anche a causa dell'eliminazione del trattamento effettuato senza il consenso dell'interessato (art. 23) tra le violazioni presupposto dell'illecito trattamento di dati. Ciò ha prodotto una *abolitio criminis* parziale delle relative condotte, per le quali si

Si è altresì inciso sull'apparato sanzionatorio amministrativo del Testo Unico. Il novellato art. 166 del decreto prevede che per le violazioni di alcune disposizioni sul trattamento dei dati personali, individuate mediante la tecnica del rinvio alle norme di disciplina, si applichino le sanzioni comminate dall'art. 83, par. 4 e 5 del GDPR[14]. Nei primi due commi dell'art. 166 il legislatore ha selezionato soltanto alcune violazioni delle norme di disciplina sul trattamento dei dati, lasciando aperto il problema dell'applicabilità residuale, per tutte le altre, delle disposizioni del GDPR.

Si profilano inoltre questioni legate alla particolare afflittività delle sanzioni previste dal Regolamento Europeo[15], che, ad uno sguardo più attento, potrebbero apparire come delle vere e proprie pene nascoste[16] e sollevare dubbi di compatibilità convenzionale *ex* art. 4 prot. 7 CEDU, in caso di applicazione congiunta con le sanzioni penali.

L'obiettivo del presente lavoro è quello di procedere a una analisi critica dell'impianto normativo in questione, cercando di gettare luce su taluni profili problematici e soffermandosi in conclusione su possibili nuovi ambiti di intervento, con particolare riferimento al "grande assente" della riforma ovverosia l'ente[17]. Per far ciò è tuttavia prima necessario ripercorrere in sintesi l'evoluzione normativa nel settore in esame, caratterizzato dall'emersione,

---

applicheranno le sanzioni amministrative previste dal Regolamento (v. *infra*, 6.1).

[14] Per l'omissione di misure di sicurezza, l'inottemperanza ai provvedimenti dell'Autorità Garante e violazione dei diritti degli interessati, in violazione delle disposizioni richiamate al par. 5, è comminata la sanzione pecuniaria fino a 20.000.000 di euro e, per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. In caso di trattamento non conforme alle disposizioni del Regolamento e di lesione dei diritti degli interessati, in violazione delle disposizioni richiamate al par. 4, si prevedono sanzioni pecuniarie fino a 10.000.000 di euro, e, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. In argomento si veda, LABIANCA, *Il sistema delle tutele nel regolamento europeo n. 679/2016 sulla protezione dei dati personali*, in *Cybercrime,* Milano, 2019, 1000 ss.

[15] Alla stregua dei criteri elaborati dalla Corte di Strasburgo, l'applicazione congiunta delle sanzioni comminate dall'art. 83 GDPR e delle sanzioni penali potrebbe dar luogo a una duplicazione sanzionatoria per il medesimo fatto. Il timore di una possibile convergenza tra sanzioni qualificabili come "penali" emerge anche nelle osservazioni conclusive del citato parere parlamentare sullo schema di decreto delegato (pag. 21), ove si invita il Governo a considerare la possibilità *«di prevedere, compatibilmente con il rispetto dei principi e criteri direttivi della delega, il ricorso a sanzioni penali solo in presenza di violazioni gravi e rispetto a fattispecie che non siano già presidiate da sanzioni amministrative comminate ai sensi del Regolamento (UE) 2016/679».* Sul tema, di recente, D'AGOSTINO, *Cybersecurity, (auto)regolazione e governance del rischio. Quid de iure poenali?, in Luiss Law Review,* 2017, 1, p. 138

[16] Cfr. MAZZACUVA, *Le pene nascoste. Topografia delle sanzioni punitive e modulazione dello statuto garantistico*, Torino, 2017, p. 95 ss.

[17] La dottrina penalistica riteneva auspicabile l'introduzione di una forma di responsabilità diretta della persona giuridica per le violazioni della normativa sulla elaborazione e sul trattamento dei dati ancor prima che fosse emanato il D. Lgs. 231/2001. Cfr. MANNA, *La protezione dei dati personali nel diritto italiano,* in *Riv. trim. dir. pen. econ.,* 1993, 191.

nello scenario penalistico, del dato personale quale oggetto di specifica tutela.

2. *Habeas data*: dalla tutela della riservatezza alla protezione dei dati personali.

Il punto di partenza è dato dall'analisi del bene giuridico protetto, trattandosi di definire con precisione l'essenza della *privacy* nell'attuale contesto di disciplina[18]. Nel passato Maestri del diritto penale[19] si sono cimentati nell'individuare il fondamento normativo del diritto in questione in disposizioni di rango costituzionale sulla scia dell'esperienza giuridica statunitense. Dal confronto di opinioni in seno alla dottrina sono emerse diverse teorie intese a riconoscere al diritto alla riservatezza *de iure condito* rilievo costituzionale, facendo leva sui principi riconosciuti dalla Carta[20] o su previsioni del diritto sovranazionale[21].

Alcuni autori partono dal concetto di "vita privata" che, sebbene di estrema relatività semantica, si differenzierebbe nettamente dalla riservatezza *stricto sensu*[22]. Il diritto al rispetto della vita privata consiste infatti nell'impedire l'altrui attività diretta a conoscere le vicende private, laddove il diritto alla riservatezza difende la sfera privata dalla divulgazione di notizie legittimamente acquisite dal soggetto[23]. Ebbene, secondo questa linea di pensiero il primo diritto, sancito dagli artt. 8 della Convenzione EDU e 12 della Dichiarazione Universale dei diritti dell'uomo, avrebbe ancoraggio costituzionale grazie al

---

[18] Sul rapporto tra reati in materia di *privacy* e tutela della riservatezza, di recente v. MANNA, DI FLORIO, *Riservatezza e diritto alla privacy: in particolare la responsabilità per omissionem dell'internet provider*, in Cadoppi A., Canestrari S., Manna A., Papa M. (a cura di), *Cybercrime,* Milano, 2019, 892

[19] BRICOLA, *Prospettive e limiti della tutela penale della riservatezza*, in *Riv.it. dir. proc. pen.* 1967, p. 1079 ss.; MANTOVANI, *Diritto alla riservatezza e libertà di manifestazione del pensiero con riguardo alla pubblicità dei fatti criminosi*, in *Arch. giur.,* 1968, p. 61 ss.; PALAZZO, *Considerazioni in tema di tutela della riservatezza (a proposito del nuovo art. 615-bis c.p.),* in *Riv. it. dir. proc. pen.*, 1975, p. 126 ss.

[20] Vi era la tendenza a desumere il diritto alla riservatezza sulla base di disposizioni costituzionali che proclamano diritti affini o che costituiscono manifestazioni parziali della riservatezza (artt. 13, 14, 15, 27, 29 Cost.) ovvero a considerarla ricompresa tra i diritti inviolabili sanciti dall'art. 2 Cost.

[21] Il riferimento è ai diritti sanciti dall'art. 8 della Convenzione Europea dei diritti dell'uomo *(«Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge [...]»*) e dall'art. 12 della Dichiarazione Universale dei diritti dell'uomo (*«Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni»*).

[22] BRICOLA, *Prospettive e limiti della tutela penale della riservatezza,* cit. p. 1088

[23] Si afferma che nella violazione del diritto al rispetto della vita privata l'accento cade sul momento dell'interferenza, potendo la diffusione successiva della notizia così acquisita incidere soltanto sull'aggravamento della responsabilità. Nella violazione del diritto alla riservatezza, invece, il disvalore cade proprio sulla diffusione della notizia.

rinvio operato dall'art. 2 Cost. ai *diritti inviolabili dell'uomo*, mentre lo stesso non potrebbe dirsi per la riservatezza[24].

Altra parte della dottrina riconosce, al contrario, piena cittadinanza all'interno della Carte fondamentale al diritto alla riservatezza, ammettendo la possibilità di una sua costituzionalizzazione tanto originaria[25] quanto successiva[26]. Stante il carattere essenzialmente personalistico della nostra Costituzione *«non solo essa non contiene alcun limite al riconoscimento del diritto alla riservatezza»*, anzi *«un tale riconoscimento è, in via logica, in perfetta armonia col tipo di ordinamento da essa espresso»*[27]. Il presupposto di questa seconda teoria – che ci sembra sicuramente più al passo con le esigenze della modernità – è che la vita privata, da una parte, e la riservatezza, dall'altra, costituiscano un'endiadi, due momenti dell'unitario nucleo di tutela che connota il diritto alla *privacy.* Cosicché si cadrebbe nel formalismo[28] ritendendo che tale diritto non sia ricompreso nelle disposizioni di diritto sovranazionale sopra richiamate.

---

[24] L'argomentazione fa leva sul tenore testuale delle norme, poste a protezione dell'individuo dall'"ingerenza" e da "interferenze arbitrarie" nella propria vita privata. Le due locuzioni stanno ad indicare che la tutela è rivolta contro le attività che provengono dall'esterno e figurino come intromissioni illecite nella sfera intima del soggetto. Pertanto, nessuna delle due previsioni è idonea a includere in sé il diritto alla riservatezza, il quale prescinde da ogni ingerenza e presuppone l'acquisizione legittima delle notizie relative alla vita privata. Cfr. BRICOLA, *Prospettive e limiti della tutela penale della riservatezza,* cit., p. 1099

[25] La costituzionalizzazione originaria sarebbe ricavabile, *in via positiva diretta*, dall'art. 15 Cost. il quale, col garantire la inviolabilità della corrispondenza e di ogni altra forma di comunicazione, si riferirebbe *lato sensu* a tutte le informazioni e comunicazioni con contenuto privato o intimo; *in via positiva indiretta* per il tramite degli artt. 13, 14, 27, comma 2, e 29, comma 1, che tutelano manifestazioni ed estensioni estremamente rilevanti della riservatezza; *in via negativa* facendo leva sull'art. 21 Cost, che riconoscendo la libertà di manifestazione del pensiero, tutela anche l'aspetto negativo alla non manifestazione del pensiero, la cui essenza sarebbe frustrata se i terzi potessero liberamente disporre delle notizie e delle informazioni che il soggetto desidera rimangano riservate. In letteratura, BALDASSARRE, *Diritti della persona e valori costituzionali*, Torino, 1997, p. 57 ss.; ID., *Privacy e costituzione: l'esperienza statunitense*, Roma, 1974, p. 56 ss.; PIZZORUSSO, *Sul diritto alla riservatezza nella Costituzione italiana*, in *Prassi e teoria*, 1976, p. 29 ss. RODOTÀ., *Intervista su privacy e libertà*, Bari, 2005, p. 18 ss.

[26] La tesi è sostenuta sul presupposto della non tassatività dei diritti della personalità consacrati nell'art. 2 Cost., norma che funge da "clausola" aperta pronta a recepire nuovi interessi della personalità in prospettiva evolutiva. Cfr. MANTOVANI, *Diritto alla riservatezza e libertà di manifestazione del pensiero*, cit., p. 59; PALAZZO F., *Considerazioni in tema di tutela della riservatezza (a proposito del nuovo art. 615-bis c.p.),* in *Riv. it. dir. proc. pen.*, 1975, p. 135; BALDASSARRE, *Diritti della persona e valori costituzionali*, cit., p. 62

[27] MANTOVANI, *Diritto alla riservatezza e libertà di manifestazione del pensiero*, cit., p. 49

[28] È di quest'avviso PATRONO, voce *Privacy e vita privata (dir. pen.),* in *Enc. dir.*, vol. XXXV, Milano, 1986, p. 574, il quale ritiene la tesi formulata da Bricola eccessivamente formalistica, sostenendo viceversa che l'interesse alla non conoscibilità o diffusibilità delle notizie sia di per sé neutro e acquisti colore soltanto in quanto strumentale rispetto alla vita privata *«di cui costituisce solo un particolare contenuto».*

Non è questa la sede per affrontare *funditus* l'esteso dibattito circa il preciso fondamento normativo del diritto alla riservatezza[29], ai fini della nostra analisi appare sufficiente ribadirne la sua rilevanza à costituzionale.
Ciò posto, si rende necessario definire in positivo in cosa siffatto diritto si sostanzi, quale sia cioè il bene della vita a venire in rilievo e quali siano le facoltà giuridiche riconosciute al suo titolare. A tal riguardo ci sembra condivisibile, almeno in linea di prima approssimazione, l'affermazione tradizionale[30] secondo cui il diritto alla riservatezza consiste nell'interesse alla *non divulgazione* di dati, informazioni, e notizie che riguardano l'individuo, e che questi intende mantenere circoscritte alla sua sfera privata. La dottrina più attenta[31] ha tuttavia fatto rilevare come il concetto di "non divulgazione" debba essere inteso in modo consono alla dimensione oramai sociale dello scambio di informazioni personali. Un segnale inequivoco di questa necessità proviene anche dalla dottrina nordamericana, dove da tempo si è abbandonato il concetto di *privacy* come *right to be let alone*, intendendola piuttosto come *«the individual's ability to control the circulation of information relating to him – a power that often is essential to mantain social relationships and personal freedom»*[32]. Così, il diritto ad essere lasciato solo viene in rilievo non più come mero interesse alla "conoscenza esclusiva delle proprie vicende" – che è una forma di libertà negativa[33] – ma nella sua proiezione sociale, quale interesse diffuso a che i consociati conservino il controllo delle informazioni private che li riguardano[34]. Il significato minimale di *privacy* si arricchisce quindi di un contenuto ulteriore: non solo *ius excludendi alios* dalla conoscenza di informazioni private, ma altresì diritto positivo al controllo dei propri dati personali[35]. A ben vedere è questa seconda accezione quella su cui oggi si fo-

[29] La questione relativa alla costituzionalizzazione del diritto alla riservatezza ha oggi perduto di attualità con la modifica dell'art. 117 Cost. ad opera della l. cost. 18 ottobre 2001, n. 3. La previsione di cui al primo comma (*«la potestà legislativa è esercitata dallo Stato e dalle Regioni nel rispetto della Costituzione, nonché dei vincoli derivanti dall'ordinamento comunitario e dagli obblighi internazionali»*) fa sì che i diritti sanciti dalle Convenzioni internazionali assumano il valore di "norme parametro" di costituzionalità. Il diritto al rispetto della vita privata e familiare e alla protezione dei dati di carattere personale sono stati sanciti anche dalla Carta dei diritti fondamentali dell'Unione Europea (rispettivamente artt. 7 e 8).
[30] Cfr. PALAZZO, *Considerazioni in tema di tutela della riservatezza,* cit., p. 144; BRICOLA F., *Prospettive e limiti della tutela penale della riservatezza,* cit. p. 1088; MANTOVANI, *Diritto alla riservatezza e libertà di manifestazione del pensiero*, cit., p. 60.
[31] PATRONO, voce *Privacy e vita privata,* cit. p. 557
[32] L'espressione, di largo consumo nella dottrina americana, è riportata da MILLER, *The assault on privacy,* in *DePaul L. Rev,* 1971, p. 1062
[33] Depone in questo senso la dottrina costituzionale prevalente. Cfr. BALDASSARRE, *Diritti della persona e valori costituzionali*, cit. 45
[34] Sul punto, RODOTÀ, *Intervista su privacy e libertà*, cit. p. 18
[35] Nella dottrina penalistica, PATRONO, voce *Privacy e vita privata,* cit. p. 560; MUCCIARELLI, *Informati-*

calizza l'attenzione. Nella moderna società dell'informazione, infatti, il baricentro è collocato ben al di là della segretezza, assestandosi verso il controllo sulla corretta utilizzazione dei dati personali. Per garantire una effettiva tutela della riservatezza sarebbe anacronistico, oltre che inutile, imporre un divieto di ingerenza nella sfera privata: nella maggioranza dei casi le informazioni personali sono cedute spontaneamente dall'interessato per la fruizione di servizi legati alla società dell'informazione (*social network*, *mailing list*, *newsletter* etc.), divenendo successivamente oggetto di scambio sul mercato[36].

In tal senso, la nozione di *privacy* è invocata in un'accezione funzionale che va ben oltre la riservatezza intesa nel contenuto minimale sopra delineato. L'interesse alla *non divulgazione* delle informazioni di carattere privato è qualcosa di diverso dal diritto alla protezione dei dati, *rectius* al corretto trattamento dei dati personali. Nondimeno, ci sembra ragionevole ritenere che la latitudine semantica del termine "riservatezza" possa abbracciare anche queste nuove forme di manifestazione[37].

Nell'interpretare il concetto in chiave evolutiva, non ci si può esimere dal considerare come nella attuale società dell'informazione il trattamento auto-

---

ca e tutela penale della riservatezza, in Picotti L. (a cura di), *Il diritto penale dell'informatica nell'epoca di internet*, Padova, 2004 p. 176; TORRE, *La gestione del rischio nella disciplina del trattamento dei dati personali*, in Picotti L. (a cura di), *Il diritto penale dell'informatica nell'epoca di internet*, Padova, 2004 p. 239; LA MANUZZI, *Diritto penale e trattamento dei dati personali. I reati previsti dal Codice della privacy e la responsabilità amministrativa degli enti alla luce del regolamento 2016/679/UE*, in *JusOnline*, 2017, 1, p. 221.

[36] Si è detto, con metafora molto pertinente, che il dato personale è il petrolio del ventunesimo secolo per via delle enormi potenzialità di profitto inerenti alla sua utilizzabilità a scopo commerciale. La profilazione dei gusti, delle necessità e dei desideri riferibili ad un certo numero di persone, rende infatti possibile l'invio di offerte promozionali mirate per l'acquisto di beni o servizi.
Come evidenzia TORRE V., *La gestione del rischio nella disciplina del trattamento dei dati personali*, cit. p. 239, il mercato delle informazioni difficilmente giungerà a saturazione, poiché il prodotto che esso offre è per sua natura inesauribile; ciò rende evidenti il rischio di compressione della sfera privata degli utenti e il pericolo di un controllo totalizzante di aspettative, desideri, bisogni degli stessi.

[37] *Contra,* LA MANUZZI, *Diritto penale e trattamento dei dati personali. I reati previsti dal Codice della privacy e la responsabilità amministrativa degli enti alla luce del regolamento 2016/679/UE,* cit. p. 221, la quale ritiene preferibile mantenere distinte le nozioni di diritto alla *privacy* e di diritto alla protezione dei dati personali, inquadrando il primo come diritto ad avere uno spazio privato immune da ingerenze, mentre il secondo come diritto a un corretto trattamento dei propri dati personali. Quest'ultimo riflette l'interesse generale alla correttezza e liceità del trattamento dei dati e avrebbe duplice natura di diritto dell'individuo e interesse della collettività. L'autrice conclude nel senso che tra riservatezza e protezione dei dati personali intercorre un *rapporto di specialità bilaterale o reciproca*, in quanto la prima tutela la "vita privata" anche al di fuori del contesto del trattamento dei dati, la seconda tutela la correttezza del trattamento dei dati personali, anche a prescindere dalla sua incidenza sulla sfera privata dell'individuo. La tesi, sicuramente ben formulata, non ci pare tuttavia condivisibile. Riteniamo infatti che la riservatezza, intesa come rispetto della vita privata da atti di divulgazione altrui, e l'interesse al corretto trattamento dei dati personali siano manifestazioni dell'unitario interesse dell'individuo al rispetto delle proprie informazioni personali contro atti di indiscrezioni o divulgazioni non consentiti.

matizzato di dati su larga scala sia la prassi. Una prassi che induce la generalità dei consociati a rinunziare tacitamente alla propria riservatezza e a rilasciare le proprie informazioni personali per accedere ai servizi offerti. In un tale contesto il diritto alla riservatezza non può, chiaramente, essere circoscritto alla mera *non divulgazione* di informazioni, atteso che l'esigenza di tutelare la riservatezza dell'interessato sorge proprio a seguito della massiva *divulgazione* di dati personali a soggetti che, per lo più, trattano professionalmente siffatti dati. Ciò rende evidente che, essendo la divulgazione la regola, la riservatezza non può divenire l'eccezione! In altre parole, il diritto alla riservatezza ricomprende in sé non solo l'interesse alla non divulgazione, ma anche l'interesse alla *consapevole divulgazione e corretta gestione* delle informazioni riguardanti l'individuo. La consapevolezza della divulgazione guarda alla fase precedente alla costituzione del rapporto, in cui l'interessato riceve l'informativa sul trattamento. La correttezza nella gestione è invece rivolta alla successiva fase del trattamento, nella quale rimane vivo l'interesse al rispetto della riservatezza delle informazioni trattate. Nella sfera privata dell'individuo rientrano infatti non solo le informazioni che egli non intende divulgare a terzi, ma anche quelle divulgate a determinati fini o condizioni. Il dato personale non perde la connotazione di privatezza – per tale intendendosi la sua appartenenza alla sfera privata dell'interessato – per il solo fatto di essere stato comunicato a terzi; esso al contrario continua ad essere una informazione riservata e deve essere trattata entro i limiti del consenso prestato dall'interessato. Qualora detti limiti siano violati[38] oppure il trattamento sia effettuato in mancanza del consenso "informato" dell'interessato, si produce inevitabilmente una lesione o una messa in pericolo della riservatezza.

Non è di ostacolo alla tesi che qui si sostiene, la riconosciuta rilevanza pubblicistica delle norme sul trattamento dei dati personali[39]. Il riflesso pubblicistico, che emerge in modo inequivoco dall'inderogabilità delle disposizioni sul trattamento dei dati e dalla disciplina delle funzioni dell'Autorità Garante, evidenzia al contrario la volontà del legislatore di apprestare una tutela anticipata della riservatezza quale bene giuridico finale[40]. Risultano in tal modo rafforza-

[38] La violazione potrà consistere nella comunicazione a terzi dei dati personali per finalità commerciali, all'utilizzo degli stessi per scopi diversi da quelli per i quali fu prestato il consenso, oppure al trattamento con modalità non conformi alla legge (contrariamente a quanto dichiarato nell'informativa sul trattamento).

[39] Sul punto, LA MANUZZI, *Diritto penale e trattamento dei dati personali. I reati previsti dal Codice della privacy e la responsabilità amministrativa degli enti alla luce del regolamento 2016/679/UE,* cit. p. 223

[40] Sul rapporto tra beni finali e beni strumentali nel quadro della teoria del bene giuridico si veda FIORELLA, voce *Reato,* in *Enc. Dir.,* XXXVIII, Milano, 1987, 797 ss. In argomento anche MANNA, *Beni*

te le prerogative di protezione del bene individuale per mezzo della tutela dell'interesse superindividuale o collettivo[41].

Né sembra deporre in senso contrario la previsione in due distinti diritti[42] nella Carta dei diritti fondamentali dell'Unione Europea (art 7, Rispetto della vita privata e familiare; art. 8, Protezione dei dati di carattere personale). Sarebbe infatti riduttivo ritenere che la bipartizione sia sintomatica di una differente ontologia dei diritti ivi sanciti, come lo sarebbe – ad esempio – ritenere che la proibizione della tortura (art. 4) non rientri nel più generale diritto all'integrità fisica e psichica (art. 3).

Possiamo quindi affermare che l'oggettività giuridica protetta dalle norme sul trattamento dei dati personali si identifica nel diritto alla riservatezza, per tale intendendosi l'interesse, giuridicamente tutelato, alla non divulgazione, alla consapevole divulgazione e alla corretta gestione di informazioni che riguardano un individuo. Ciò porta a ritenere che le fattispecie che sanzionano l'inosservanza degli obblighi relativi al trattamento dei dati personali, siano rivolte a protezione del medesimo bene.

In conclusione, il comune cittadino che fruisce dei servizi della società dell'informazione è posto nell'impossibilità di non svelarsi nell'agire quotidiano. Egli rilascia continuamente dati personali che scompongono la sua identità sociale in un catalogo di informazioni, perdendo lentamente il controllo di sé. Per questo la *privacy*, comunemente intesa nell'accezione minimale di *right to be let alone*, deve – come si è detto – *«mutare il suo contenuto da diritto alla riservatezza a diritto all'autodeterminazione informativa»*[43]. I dati posseduti da terzi devono rientrare appieno nella sfera di signoria dell'interessato, che ne governa il flusso, e preserva un pieno controllo sulle proprie informazioni personali: *habeas data*[44].

Le forme di manifestazione tipiche degli *atti di indiscrezione* e *di divulgazione*[45] si realizzano oggi nel contesto digitale, nel cyberspazio, nel mondo dei

---

della personalità e limiti della protezione penale, Padova, 1989, 59 ss.

[41] La tesi trova conferma nelle scelte compiute dal legislatore in altri settori dell'ordinamento. Si pensi al sistema di prevenzione contro gli infortuni sul lavoro di cui al D. Lgs. 81/2008 nel quale si prevedono moltissime disposizioni, di curvatura pubblicistica, strumentali ad una tutela anticipata della vita e dell'incolumità personale. Sulle tecniche di tutela penale in materia di sicurezza sul lavoro, DE FALCO, *La repressione delle contravvenzioni e dei delitti in materia di sicurezza e igiene del lavoro,* Padova 2001 p.8 ss.; STELLA, *La costruzione giuridica della scienza: sicurezza e salute negli ambienti di lavoro,* in *Riv. it. dir. proc. pen.*, 2003 p. 55 ss.

[42] Cfr. RODOTÀ, *Intervista su privacy e libertà*, cit. p. 19

[43] Così TORRE, *La gestione del rischio nella disciplina del trattamento dei dati personali*, cit. p. 41

[44] L'espressione richiama la recente opera di FARIVAR, *Habeas Data: Privacy vs the Rise of Surveillance Tech*, Melville Publishing, 2018, un interessante libello sullo scandalo *Cambridge Analytica*.

[45] Si tratta di una distinzione molto diffusa in dottrina. Si veda BRICOLA, *Prospettive e limiti della tutela*

Big Data: a queste realtà occorre far riferimento per esprimere un fondato giudizio di valore sull'oggettività giuridica protetta dalle norme sul trattamento dei dati personali, che evidenziano chiari profili di continenza nel concetto di riservatezza, interpretato in chiave evolutiva rispetto alle esigenze della moderna società dell'informazione.

3. Il formante sovranazionale e l'evoluzione della disciplina interna.

L'attuale quadro di disciplina in tema di protezione dei dati personali è il risultato di un lungo e articolato percorso storico che si snoda lungo strade nazionali e sovranazionali. Per esaminare in modo più compiuto i contorni della tutela penale in materia, è utile ripercorrere le tappe principali dell'evoluzione normativa.

Il primo *input* fu fornito dall'apertura alla firma della Convenzione del Consiglio di Europa per la protezione dell'individuo in relazione al trattamento automatico di dati personali, approvata a Strasburgo il 28 gennaio 1981[46]. La Convenzione nacque dall'esigenza, evidenziatasi a partire dagli anni '60, di tutelare gli individui dal proliferare delle tecnologie dell'informazione. Le disposizioni sulle modalità e le finalità del trattamento riflettono principi considerati ancora oggi fondamentali e di estrema attualità[47]. Si prevede infatti che i dati debbano essere raccolti e trattati solo in base a determinate norme che ne permettano il trattamento automatizzato, per scopi specifici e legittimi, e che non debbano essere destinati a un uso incompatibile con la finalità di tratta-

penale della riservatezza, cit. p. 1095; MANTOVANI, *Diritto alla riservatezza e libertà di manifestazione del pensiero con riguardo alla pubblicità dei fatti criminosi*, cit. p. 52; RONCO, voce *Vita privata (interferenze illecite),* in *App. Noviss. Dig.*, vol. VII, Torino, 1987, p. 1162.

[46] Il legislatore nazionale diede esecuzione al trattato con la legge 21 febbraio 1989, n. 98. La Convenzione assume come scopo quello di assicurare a ciascun individuo il rispetto dei suoi diritti e delle sue libertà fondamentali e, in particolare, del diritto alla sua vita privata in relazione all'elaborazione automatica dei dati che lo riguardano. L'art. 1 della Convenzione, nel testo risultante dalla recentissima modifica, dispone che *«The purpose of this Convention is to protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy».*

[47] Di recente il Consiglio d'Europea ha provveduto ad aggiornare la Convenzione mediante l'adozione di un protocollo addizionale. Lo scorso 18 maggio del 2018 è stata approvata una modifica del testo della Convenzione, teso a modernizzarla per fornire un quadro giuridico più consono ad un'epoca nella quale le violazioni del diritto alla protezione dei dati sono divenute una importante preoccupazione. Il protocollo fornisce un quadro giuridico robusto e flessibile per facilitare il flusso dei dati attraverso le frontiere e fornire garanzie efficaci. Esso introduce innovazioni rilevanti come l'obbligo di comunicare le violazioni dei dati (*data breach*) e il rafforzamento del principio di minimizzazione dei dati, e di trasparenza dell'elaborazione. Richiede anche il rispetto del principio di *privacy by design*, introducendo ulteriori precauzioni nell'ambito dei trattamenti algoritmici, come il diritto di ottenere informazioni sulla logica alla base dell'elaborazione dei dati.

mento originaria (principio di pertinenza); che non possano essere conservati oltre il tempo necessario per raggiungere lo scopo prefissato (principio di non eccedenza); che le modalità e le finalità del trattamento siano trasparenti, chiare e accessibili agli interessati (principio di correttezza). Dal punto di vista sanzionatorio l'art. 10 si limitava a prevedere *«sanzioni e ricorsi adeguati relativi alle violazioni alle disposizioni del diritto interno di esecuzione dei principi fondamentali per la protezione dei dati»*[48].

Quello stesso anno fu approvata la legge n. 121/1981 recante il nuovo ordinamento dell'Amministrazione di pubblica sicurezza, che istituiva il Centro di elaborazione dati (CED) presso il Ministero dell'interno. Nel testo emergeva una particolare attenzione per la tutela dei dati ritenuti utili per il contrasto e la prevenzione della criminalità. Venivano disciplinate le finalità di raccolta dei dati e sanzionate penalmente la comunicazione o l'utilizzo indebito delle informazioni posti in essere dal pubblico ufficiale *«in violazione delle disposizioni della presente legge, o al di fuori dei fini previsti dalla stessa»* (art. 12). Si trattava, a detta della dottrina[49], dell'unica fattispecie di reato che si occupasse di punire condotte di abuso lesive della *privacy*.

Uno *step* successivo si ebbe con la Raccomandazione R (87) 15 del Comitato dei Ministri del Consiglio d'Europa, relativa alla disciplina dell'uso di dati personali nell'ambito della pubblica sicurezza, adottata dal Comitato dei Ministri il 17 settembre 1987. In essa si rappresentava la necessità che l'interesse della società alla prevenzione e alla repressione dei reati e al mantenimento dell'ordine pubblico fosse contemperato con il diritto al rispetto della vita privata dell'individuo. A tal fine si raccomandava l'istituzione di un'autorità di controllo indipendente ed esterna alla polizia, incaricata di vigilare sul rispetto dei principi del corretto trattamento dei dati, consentito soltanto per finalità di pubblica sicurezza e limitato a quanto necessario per la prevenzione di un pericolo concreto o per la repressione di uno specifico reato. La Raccomandazione non conteneva però alcuna indicazione circa la necessità di comminare sanzioni dissuasive per le violazioni delle modalità di trattamento.

Sul fronte interno si assisteva, nel frattempo, all'avvicendarsi di diversi progetti di legge[50] elaborati sulla spinta della Convenzione di Strasburgo del 1981. Il

---

[48] Anche nel testo risultante dalla riforma non si fa riferimento espresso a sanzioni di natura penale (*«Each Party undertakes to establish appropriate judicial and non-judicial sanctions and remedies for violations of the provisions of this Convention»*).

[49] MANNA, *La protezione dei dati personali nel diritto italiano,* in *Riv. trim. dir. pen. econ.,* 1993, p.181 il quale esprimeva una posizione decisamente critica per l'assenza di una disciplina generale sulla protezione dei dati personali.

[50] Per approfondimenti sul contenuto dei progetti elaborati a partire dal 1981, LOSANO, *I progetti di legge italiani sulla riservatezza dei dati personali*, in Alpa, Bessone (a cura di), *Banche dati telematica e*

più importante di essi fu il Progetto Mirabelli, del quale furono elaborate due versioni[51]. Tra i punti salienti del primo disegno di legge figurava la proposta di costruire una disciplina unitaria per i privati e gli enti pubblici che trattassero dati personali contenuti in una banca dati. Dal punto di vista sanzionatorio, il disegno di legge faceva massiccio ricorso allo strumento penale, tanto da incontrare aspre critiche in dottrina[52]. Ciò condusse all'elaborazione di un secondo Progetto Mirabelli[53] caratterizzato, per quel che qui rileva, da un deciso ridimensionamento dello spazio riservato al diritto penale. A seguire fu elaborato un terzo disegno di legge, con il quale si tornava a prediligere la via penale, anche rispetto a violazioni meramente formali della disciplina sulla elaborazione automatica dei dati personali[54].

Il fermento e la continua riedizione dei disegni di legge non produssero tuttavia alcun risultato finale; l'assetto normativo rimase invariato finché non si giunse a un nuovo, rilevante *input* sovranazionale.

Con la Direttiva del Parlamento europeo e del Consiglio 95/46/CE (c.d. Direttiva madre) la Comunità Europea delineava un complesso sistema di regole sui trattamenti, anche non automatizzati, di dati personali. L'esigenza di armonizzazione[55] nasceva dalla frammentarietà delle legislazioni vigenti nei diversi Stati membri, che determinava un indebolimento di tutela e alimentava discrasie e intollerabili disparità di trattamento. Il testo normativo fissava precisi limiti all'attività di raccolta e all'utilizzazione dei dati personali, chiedendo a ciascuno Stato membro di istituire un organismo nazionale indipendente incaricato della protezione degli stessi. L'obiettivo della Direttiva era

---

diritti della persona, Padova, 1984, p. 151 ss.; PERRI., *Privacy, diritto e sicurezza informatica,* Milano, 2007, p. 5 ss.

[51] DDL n. 1657 presentato alla Camera dei Deputati il 5 maggio 1984, rubricato *"Costituzione ed esercizio delle banche di dati personali ed elaborazione informatica".*

[52] Cfr. PECORELLA, *Profili penalistici della regolamentazione delle banche dati*, in Zeno- Zencovich V. (a cura di)., *Le banche dati in Italia. Realtà normativa e progetti di regolamentazione*, Napoli, 1985, p. 147 ss.; MANNA, *La protezione dei dati personali nel diritto italiano,* cit. p. 183

[53] Il 30 settembre 1989 il gruppo di lavoro presieduto dal Pres. Mirabelli consegnava al Ministro Vassalli lo schema di disegno di legge in materia di tutela della *privacy* che viene ricordato come "Mirabelli-*bis*". In argomento CIACCI, *Ettore Giannantonio e il principio di libertà informatica,* in *Informatica e diritto,* 2016, 1, p. 203

[54] Si tratta del DDL Martelli AC.152, presentato alla Camera dei Deputati in forma di Testo Unificato, anch'esso mai giunto ad approvazione definitiva. Tra le novità spiccava l'inserimento di un reato di accesso abusivo ai sistemi informatici, consistente nel prendere cognizione dei dati di un sistema informatico di elaborazione, contro la volontà espressa o tacita di chi ha diritto di escluderla, ipotesi di reato successivamente introdotta, sebbene con diversa formulazione, dall'art. 4 della legge 23 dicembre 1993 n. 547 che ha novellato il codice penale inserendovi l'art. 615-*ter.*

[55] Evidenziata da BUTTARELLI, *Verso un diritto della sicurezza informatica,* in *Sicurezza informatica*, 1995, 2, p. 25 ss; ID., *Privacy, sicurezza e nuove tecnologie al bivio di nuove scelte strategiche,* cit. p. 5

essenzialmente quello di contemperare la tutela dei diritti delle persone fisiche con l'esigenza della libera circolazione dei dati tra Stati membri, strumentale a sua volta all'esercizio delle libertà di circolazione delle persone dei beni e dei servizi all'interno della Comunità. Le disposizioni contenute nella direttiva 95/46/CE vincolavano gli Stati membri a conformarsi ad esse, lasciando ai legislatori nazionali significativi margini di adattamento, specie per quel che riguarda la previsione di deroghe in specifici settori.

L'emanazione della Direttiva condusse alla presentazione di un disegno di legge di iniziativa governativa[56], che giunse all'approvazione in tempi assai rapidi[57]. La legge 31 dicembre 1996 n. 675 introduceva finalmente nell'ordinamento italiano una disciplina generale sul trattamento dei dati personali, con o senza l'ausilio di dispositivi automatizzati, prevedendo precisi obblighi a carico del responsabile e del titolare del trattamento[58] e disciplinando in modo dettagliato il trasferimento dei dati medesimi. A corredo della disciplina sul trattamento dei dati personali, gli artt. 34-39 della legge prevedevano un articolato impianto sanzionatorio, facente leva principalmente su sanzioni di natura penale[59].

La legge 676 – promulgata contestualmente – conferiva delega al Governo per l'emanazione di successivi decreti delegati che completassero il quadro normativo di protezione dei dati personali in relazione ad alcuni aspetti tecnici. Per far fronte al ritardo del Governo nell'esercizio della delega, la legge 24 marzo 2001, n. 127 (*«Differimento del termine per l'esercizio della delega prevista dalla legge 31 dicembre 1996, n. 676, in materia di trattamento dei*

---

[56] DDL 1580-AC, presentato dal Ministro della Giustizia Flick il 20 giugno 1996 e approvato definitivamente in seconda lettura dalla Camera dei Deputati il 18 dicembre 1996. Il Ministro proponente, udito in sede parlamentare aveva ribadito che il disegno di legge costituiva *«l'inizio della tutela della personalità nell'ordinamento italiano, ristabilendo una serie di equilibri».* Cfr. Il *Resoconto della II Commissione permanente (Giustizia)* del 17 dicembre 1996, su www.camera.it

[57] VENEZIANI, *Beni giuridici protetti e tecniche di tutela penale nella nuova legge sul trattamento dei dati personali,* cit., p. 151 secondo cui complice della celerità nell'approvazione della legge fu l'intento di "adempimento internazionale" con cui fu presentata in Parlamento.

[58] Tra questi, in particolare, l'obbligo di fornire un'informativa al momento della raccolta, di adottare misure minime di sicurezza, e di assicurare l'esercizio dei diritti dell'interessato (artt. 10 ss.), sia per i dati comuni sia per quelli sensibili.

[59] Il Capo VIII della legge conteneva le seguenti ipotesi di reato: omessa o infedele notificazione (art. 34); trattamento illecito di dati personali (art. 35); omessa adozione di misure necessarie alla sicurezza dei dati (art. 36); inosservanza dei provvedimenti del Garante (art. 37). A chiusura del sistema erano previsti alcune sanzioni amministrative per l'inosservanza di alcune disposizioni secondarie sul trattamento dei dati (art. 39). Per un commento, SEMINARA, *Appunti in tema di sanzioni penali nella legge sulla privacy*, in *Resp. civ. e prev.,* 1998, 4-5, p. 915 ss. Per una disamina più approfondita dell'impianto sanzionatorio di rinvia al paragrafo seguente e all'analisi delle singole fattispecie di reato (*infra* § 3.1 e 4).

dati personali»), prorogava il termine in origine previsto, dettando criteri direttivi per l'emanazione di un Testo Unico al fine di assicurare un più armonico coordinamento e procedere a una migliore attuazione della delega[60]. Si giunse così all'emanazione del decreto legislativo 30 giugno 2003, n. 196 (di seguito, Codice della *privacy*), con il quale il legislatore ha riordinato le disposizioni vigenti in materia di trattamento dei dati personali e fissato una serie di principi, di ordine generale, validi per il trattamento di dati in tutti i settori. Il Codice non si limita a una risistemazione formale della disciplina, ma apporta modifiche di carattere sostanziale[61].

Per quel che qui rileva, la parte finale del testo legislativo è dedicata alla tutela amministrativa e giurisdizionale, e contiene una appendice sanzionatoria di carattere sia amministrativo che penale. Con riferimento alla prima il D. Lgs. 196/2003 ha previsto un generale inasprimento delle sanzioni pecuniarie e ampliato i casi in cui le sanzioni accessorie[62] possono essere irrogate. Sul fronte penale, pur rimanendo immutata l'architettura del sistema[63], si ebbero alcune novità di rilievo tra cui l'introduzione dell'elemento del "nocumento" nel delitto di illecito trattamento di dati (art. 167), l'ampiamento del raggio di azione del reato di inosservanza dei provvedimenti del Garante (art. 170), la previsione di una particolare modalità di estinzione del reato di omessa adozione delle misure di sicurezza (art. 169), l'abolizione dei reati di omessa o incompleta notificazione[64].

Tornando al fronte sovranazionale, il processo di integrazione europea non si arrestò con l'emanazione della Direttiva madre. Dopo alcuni anni, si tornò ad avvertire l'esigenza di provvedere a un'opera di maggiore coordinamento delle normative nazionali; l'esigenza si manifestò in modo particolare nelle attività di prevenzione e repressione dei reati, oggetto della decisione quadro

---

[60] Per approfondimenti sull'argomento si rinvia alla Relazione dell'Autorità Garante sullo *"Stato di attuazione della legge n. 675/1996"* del 17 luglio 2001, disponibile sul sito istituzionale del Garante.

[61] Oltre alle disposizioni di natura generale, il Codice prevede norme relative a specifici settori, disciplinando, tra l'altro, il trattamento dei dati in ambito giudiziario, sanitario ed in materia di lavoro e previdenza sociale. Per un primo commento, Zeno Zencovich, Cardarelli., Sica (a cura di), *Il codice dei dati personali. Temi e problemi*, Milano 2004, p. 15 ss.

[62] In base all'art. 165 il Giudice può disporre la pubblicazione dell'ordinanza-ingiunzione del Garante nelle ipotesi di illecito amministrativo. La pena accessoria della pubblicazione della sentenza di condanna (art. 172) è inoltre disposta inoltre per tutti i delitti previsti dal codice.

[63] Per un commento, CORRIAS LUCENTE, *La nuova normativa penale a tutela dei dati personali,* cit. p. 632 ss.; MANNA, *Il quadro sanzionatorio penale e amministrativo del codice sul trattamento dei dati personali*, cit. p. 727 ss. In chiave comparatistica, SHENKO WU, *La tutela penale della privacy nell'epoca di internet*, Napoli, 2012.

[64] Le novità risultanti dal riordino normativo saranno esaminate in modo più compiuto con riferimento alle singole fattispecie di reato (*infra*, § 4.1. ss).

2008/977/CEE. Con l'adozione di questo strumento normativo il Consiglio aveva stabilito principi e regole comuni in materia di protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, dettando una disciplina che completasse quella introdotta dalla direttiva 95/46/CE. Nella precedente struttura "a pilastri", la direttiva madre si applicava ai settori coperti dal diritto comunitario (I pilastro), con esclusione quindi dei trattamenti di dati svolti nei settori della cooperazione di polizia e giustizia e in quelli della cooperazione in materia di politica estera e di sicurezza degli Stati (II e III pilastro)[65].

All'indomani del Trattato di Lisbona si avvertì nuovamente, a livello eurounitario, la necessità di un ravvicinamento delle legislazioni nazionali di protezione dei dati personali. Secondo parte della dottrina[66], le ragioni del compimento di un ulteriore passo di armonizzazione possono essere ricondotte a tre esigenze di massima.

In primo luogo, quella di uniformazione delle normative nazionali, diversificate anche a causa degli ampi margini di discrezionalità riconosciuti agli Stati dalla Convenzione di Strasburgo del 1981, da cui derivava una marcata diversità di norme e di livelli di tutela. *In secundis,* quella derivante dall'incessante sviluppo di nuove tecnologie, che ha posto all'attenzione del legislatore nuovi fenomeni di trattamento e trasferimento illeciti di dati personali. Da ultimo l'esigenza di dare piena attuazione alle previsioni del Trattato di Lisbona relative alla protezione dei dati personali dei cittadini dell'Unione[67].

All'esito di un lungo *iter* legislativo, iniziato con l'istituzione di un tavolo di lavoro presso la Commissione nel 2012, è stato finalmente emanato il regolamento 2016/679/UE del Parlamento Europeo e del Consiglio *«relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati»* (di seguito, GDPR), che rappresenta il suggello dell'opera di armonizzazione delle discipline nazionali sulla protezione dei dati personali.

---

[65] Con l'entrata in vigore del Trattato di Lisbona fu abolita la struttura a pilastri. Nondimeno, la protezione dei dati personali nelle attività di contrasto resta disciplinata da un *corpus* normativo autonomo rispetto al Regolamento Generale di recente emanazione. Cfr. 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»* che abroga la decisione quadro 2008/977/GAI del Consiglio.

[66] In argomento, BUTTARELLI, *Privacy, sicurezza e nuove tecnologie al bivio di nuove scelte strategiche,* in *Federalismi.it*, editoriale del 14 gennaio 2015.

[67] Il Trattato e la Carta dei diritti fondamentali dell'Unione europea hanno elevato il diritto alla protezione dei dati al rango di autonomo diritto fondamentale (Cfr. Artt. 7 e 8 della Carta di Nizza; art. 16 TUE; artt. 16 e 39 TFUE).

Il regolamento introduce regole più chiare in materia di informativa e consenso, definisce i limiti del trattamento automatizzato dei dati[68], disciplina in modo più compiuto il trasferimento transfrontaliero degli stessi, impone nuovi obblighi di notificazione in caso di *data breach*[69], attribuisce rilievo all'autodisciplina e alla *compliance* aziendale[70].
Il sistema delineato dal nuovo Regolamento, in linea con la tradizione, si ispira ai principi di trasparenza[71], di pertinenza e di non eccedenza del trattamento[72]. Ai fini dell'oggetto del presente lavoro, risulta di particolare interesse il principio di *accountability* in virtù del quale i soggetti gravati dagli obblighi del GDPR dovranno autoresponsabilizzarsi e adottare precise strategie volte ad assicurare il pieno rispetto delle previsioni di legge[73]. In questa prospettiva, i principi della *privacy by design* e della *privacy by default*, secondo cui la protezione del dato personale deve essere assicurata *ab origine* come se fosse un'impostazione predefinita, sembrano prodromici ad una estensione totalizzante dell'autoresponsabilità in ogni fase della vita dell'impresa.[74] In breve, nel nuovo assetto normativo il titolare, il responsabile o l'incaricato del trattamento assumono un ruolo attivo nella protezione dei dati personali in questione, dovendo assumere tutte le misure tecniche e organizzative necessarie a pre-

[68] L'art. 22 del GDPR dispone che *«L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona».*
[69] Per garantire un elevato livello di sicurezza nella protezione dei dati personali, l'art. 33 del Regolamento impone al titolare e al responsabile del trattamento un obbligo di notificazione di ogni «violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati» (definizione dettata dall'art. 4 n. 12 GDPR).
[70] Per un commento sulle novità introdotte dal Regolamento, PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016.; BOLOGNINI,PELINO, BISTOLFI, *Il Regolamento privacy europeo*, Milano, 2016; LABIANCA, *Il sistema delle tutele nel regolamento europeo,* cit. 978 ss.
[71] È il principio in base al quale le informazioni relative all'identità del titolare del trattamento dei dati e le finalità del trattamento debbano essere facilmente accessibili e di facile comprensione per gli interessati.
[72] Secondo questo principio possono essere trattati soltanto i dati strettamente necessari alle finalità perseguite dal titolare, entro i limiti oggettivi e temporali dell'attività che giustifica la raccolta e/o il trattamento.
[73] L'art. 24 del GDPR a mente del quale «tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento» è considerato il cardine del principi di *accountability*. A tal riguardo, LA MANUZZI., *Diritto penale e trattamento dei dati personali. I reati previsti dal Codice della privacy e la responsabilità amministrativa degli enti alla luce del regolamento 2016/679/UE*, cit., p. 247
[74] BOLOGNINI, PELINO, BISTOLFI, *Il Regolamento privacy europeo*, cit., p. 324

venire il rischio di violazioni.
Contestualmente all'emanazione del regolamento è stata approvata la direttiva 2016/680/UE relativa al trattamento dei dati personali nello svolgimento delle attività di contrasto[75], la quale, sebbene non riguardi da vicino il tema oggetto di specifica analisi, completa il quadro normativo di protezione dei dati personali, disciplinando in modo organico il trattamento svolto a fini di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali[76].

4. L'apparato sanzionatorio-ammnistrativo del nuovo Regolamento Europeo e la disciplina nazionale di attuazione. Alcune brevi considerazioni critiche.
L'art. 13 della legge 25 ottobre 2017, n. 163 (legge c.d. di delegazione europea), ha conferito delega al Governo affinché adottasse, entro sei mesi, acquisiti i pareri delle competenti Commissioni parlamentari e del Garante per la protezione dei dati personali, uno o più decreti legislativi in modo da adeguare il quadro normativo nazionale alle disposizioni del regolamento 2016/679/UE. Seguendo la procedura prevista dall'art. 31 della legge 234/2012, il Consiglio dei ministri ha trasmesso alle Camere in data 10 mag-

[75] L'obiettivo della direttiva è quello di agevolare lo scambio e l'utilizzo dati giudiziari al fine di rendere maggiormente efficaci la prevenzione e gli strumenti di contrasto della criminalità e terrorismo, assicurando il rispetto dei diritti degli individui. Con D. Lgs. 18 maggio 2018, n. 51 il legislatore italiano ha dato attuazione alla direttiva sostituendo gran parte delle disposizioni del Codice della *privacy* aventi ad oggetto il trattamento dei dati personali effettuato in ambito penale. Quanto all'ambito di applicazione, si prevede che le disposizioni ivi contenute si applicano ai *«trattamenti interamente o parzialmente automatizzati di dati personali delle persone fisiche contenuti in un archivio o ad esso destinati, svolti dalle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica»* (art. 1). Circa i presupposti di liceità del trattamento il decreto dispone che i trattamenti dei dati in ambito penale possano essere previsti e disciplinati sia dalla legge che da un regolamento, purché in tal caso siano adeguatamente garantiti i diritti e le libertà dell'interessato. I trattamenti di tipo automatizzato, invece, debbono essere consentiti in modo espresso dalla legge poiché maggiormente rischiosi per l'interessato. Quanto ai diritti di quest'ultimo – tra cui la ricezione di informazioni, l'accesso, la rettifica, la cancellazione, e la limitazione del trattamento – il Decreto prevede che questi possano essere limitati, ritardati o esclusi solo qualora ciò sia strettamente necessario per non compromettere le attività svolte da parte dell'autorità giudiziaria in ambito penale, la sicurezza pubblica e nazionale, nonché i diritti e le libertà degli individui. Il decreto si chiude con due capi dedicati alle sanzioni amministrative e alle sanzioni penali per l'inosservanza delle disposizioni contenute nelle disposizioni sul trattamento dei dati. Nel dettaglio, l'art. 42 elenca una serie di violazioni punite con sanzioni che, nei casi più gravi, giungono a Euro 150.000; i successivi articoli da 43 a 45 introducono rispettivamente – in modo speculare rispetto alle fattispecie previste dal D. Lgs. 196/2003 – i reati di trattamento illecito di dati, di falsità in atti e dichiarazioni al Garante, e di inosservanza dei provvedimenti del Garante.
[76] Per approfondimenti sulle scelte di criminalizzazione compiute con il D. Lgs. 51/2018 si veda RESTA, *I reati in materia di protezione dei dati personali,* cit., 1024

gio 2018 uno schema di decreto per la riforma delle disposizioni del Codice della *privacy,* abbandonando l'idea di una abrogazione totale del *corpus* normativo, probabilmente dovuta alle possibili censure di illegittimità costituzionale che tale scelta avrebbe comportato. Costituita la Commissione speciale[77] e acquisito il parere dell'Autorità Garante[78], i lavori Parlamentari sono proseguiti con l'audizione di esperti, accademici e rappresentanti della società civile. All'esito dell'istruttoria, la Commissione incaricata ha reso un parere favorevole condizionato al recepimento di alcune modifiche, invitando il delegato a tener conto, in sede di deliberazione finale, anche di altre indicazioni non vincolanti [79]. Il Governo ha infine definitivamente approvato il D. Lgs. 101/2018 entrato in vigore in data 19 settembre 2018.

Ricostruito cursoriamente il cammino della riforma, possiamo ora esaminare da vicino le novità che interessano l'apparato sanzionatorio, rivolgendo lo sguardo dapprima a quello amministrativo e successivamente a quello penale.

La direttiva 95/46/CE prevedeva genericamente l'obbligo di stabilire sanzioni da applicare in caso di violazione delle disposizioni di attuazione della stessa (art. 24), lasciando ampia discrezionalità ai legislatori nazionali nell'individuare il contenuto degli illeciti e le relative sanzioni[80]. Nel passaggio

---

[77] Per consolidata prassi costituzionale, all'inizio della legislatura viene costituita una Commissione speciale, in entrambi i rami del Parlamento, per l'esame degli atti urgenti presentati dal Governo. Il presupposto giustificativo di questa scelta risiede nella necessità di esaminare gli atti in scadenza trasmessi dal Governo che non possono attendere i tempi di perfezionamento dell'avvio della legislatura (decreti-legge emanati e ancora da convertire, gli schemi di decreto legislativo trasmessi alle Camere per l'espressione dei pareri, etc.). Nella presente legislatura sono state costituite in seno al Senato della Repubblica (seduta di mercoledì 28 marzo 2018) e alla Camera dei deputati (seduta di martedì 10 aprile 2018) di due Commissioni speciali per l'esame degli atti del Governo che, alla data di stesura del presente contributo, continuano a svolgere la propria attività. Ha trovato così conferma la previsione (Cfr. LATTUCA, *La Commissione speciale per l'esame degli atti del Governo come strumento ordinario di avvio della legislatura*, in *Forum di Quaderni Costituzionali*, 17 aprile 2018) per cui l'attività della Commissione speciale avrebbe potuto essere prolungata, tenuto conto delle difficoltà riscontrate nella formazione del Governo e delle diverse situazioni d'urgenza da affrontare.

Con specifico riferimento allo Schema di decreto per l'adeguamento alle disposizioni del GDPR, il 23 maggio 2018 gli Uffici di presidenza, integrati dai rappresentanti dei gruppi, delle Commissioni speciali della Camera e del Senato, al fine di acquisire i necessari elementi istruttori per l'esame del provvedimento, hanno congiuntamente proceduto in modo tempestivo all'audizione di esperti, soggetti della società civile, professionisti, operatori dei settori coinvolti e destinatari delle disposizioni in tema di *privacy,* abbattendo così i tempi che sarebbero stati necessari per un esame disgiunto del suddetto schema.

[78] *Parere sullo schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679*, Registro dei provvedimenti n. 312 del 22 maggio 2018, su www.garanteprivacy.it, § 1.4

[79] *Bollettino delle Giunte e delle Commissioni parlamentari* di mercoledì 20 giugno 2018, XVIII legislatura.

[80] Come noto, il Trattato di Maastricht non attribuiva all'Unione (I pilastro) alcuna competenza in mate-

dal precedente all'attuale quadro normativo, la tecnica sanzionatoria ha subito un profondo *revirement*: il menzionato art. 83 del Regolamento[81] contiene

ria penale; il legislatore comunitario avrebbe pertanto potuto sanzionare soltanto in via amministrativa alcune condotte (in via diretta o indiretta a seconda dello strumento normativo utilizzato, se un regolamento o una direttiva). In un tale contesto si faceva largo consumo della clausola di adeguatezza delle sanzioni per la violazione delle disposizioni di armonizzazione.

[81] Il *paragrafo 4* della disposizione commina sanzioni amministrative pecuniarie fino a 10 milioni di Euro, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per la violazione:

a) degli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli artt. 8 (Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione), 11 (Disposizioni relative al trattamento che non richiede l'identificazione), da 25 a 39 (Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita; Previsioni in materia di contitolarità del trattamento; Obblighi dei rappresentanti di titolari del trattamento o dei responsabili del trattamento non stabiliti nell'Unione; Obblighi del responsabile del trattamento; Modalità del trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento; Tenuta dei registri delle attività di trattamento; Disposizioni sulla cooperazione con l'autorità di controllo; Disposizioni sulla sicurezza del trattamento; Obblighi di notifica di una violazione dei dati personali all'autorità di controllo; Obbligo di comunicazione di una violazione dei dati personali all'interessato; Valutazione d'impatto sulla protezione dei dati; Casi di consultazione preventiva; Designazione del responsabile della protezione dei dati, posizione e compiti di quest'ultimo), 42 (Obblighi del titolare e del responsabile inerenti la certificazione) e 43 (Disposizioni sugli organismi di certificazione);

b) gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;

c) gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4 (adozione di idonee misure in caso di violazione del codice di disciplina da parte di un titolare del trattamento o responsabile del trattamento).

Il *paragrafo 5* della disposizione commina sanzioni amministrative pecuniarie fino a 20 milioni di Euro, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per:

a) la violazione dei principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5 (Principi applicabili al trattamento), 6 (Liceità del trattamento), 7 (Condizioni per il consenso) e 9 (Disposizioni relative al trattamento di categorie particolari di dati personali);

b) la violazione dei diritti degli interessati a norma degli articoli da 12 a 22 (Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato; Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato; Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato; Diritto di accesso dell'interessato; Diritto di rettifica; Diritto alla cancellazione; Diritto di limitazione di trattamento; Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento; diritto alla portabilità dei dati; Diritto di opposizione; Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione);

c) la violazione della disciplina sui trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49 (Principio generale per il trasferimento; Trasferimento sulla base di una decisione di adeguatezza; Trasferimento soggetto a garanzie adeguate; Disposizioni sulle norme vincolanti d'impresa; Trasferimento o comunicazione non autorizzati dal diritto dell'Unione; Deroghe alle disposizioni precedenti in specifiche situazioni);

d) l'inosservanza di qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX (Disposizioni relative a specifiche situazioni di trattamento);

e) l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo, o il negato accesso in violazione delle prerogative dell'Autorità Garante.

una lunga lista di violazioni per le quali commina aspre sanzioni pecuniarie[82].
Il legislatore europeo sembra affidare a tale disposizione l'intera tenuta del sistema, prevedendo una ampissima forbice sanzionatoria, delimitata nel massimo ma non nel minimo, che accomuna svariate violazioni, a loro volta distinte in due categorie, a seconda della gravità.
La tecnica utilizzata desta perplessità sotto diversi profili. Al di là della eccessiva severità delle sanzioni, non si comprende secondo quale criterio il legislatore abbia raggruppato violazioni espressive di un disvalore profondamente disomogeneo. La violazione degli obblighi imposti al titolare e al responsabile del trattamento o l'omissione della tenuta del registro dei trattamenti soggiacciono, ad esempio, alla stessa sanzione prevista per le violazioni in materia di certificazione, nonostante nel primo caso la violazione riguardi misure obbligatorie della protezione dei dati, nel secondo un meccanismo soltanto eventuale. Così pure si pensi all'inosservanza dell'obbligo di notifica del *data breach,* sanzionato con gli stessi limiti edittali della mera omissione di consultazione preventiva del Garante.
Inoltre, la ricostruzione del precetto è resa assai farraginosa dal rinvio alle norme di disciplina, effettuato in modo tutt'altro che puntuale. Anziché richiamare un preciso dovere o divieto sancito dal Regolamento, con indicazione esatta del relativo paragrafo, si effettua un rinvio puro e semplice a interi articoli che, al loro interno, contengono più norme magari rivolte a destinatari diversi. È il caso dell'art. 38 che tratta della posizione del responsabile della protezione dei dati, ma prevede anche obblighi a carico del titolare e del responsabile del trattamento. In altri casi il richiamo integrale è ad articoli che contengono norme di carattere dispositivo, dalle quali non sembrerebbe potersi trarre l'imposizione di un obbligo o la fissazione di un divieto. Un esempio è dato dall'art. 42 che disciplina la certificazione della protezione dei dati senza dettare alcuna specifica norma imperativa, stante la volontarietà della relativa procedura.
Nel delineare il quadro sanzionatorio amministrativo il legislatore europeo sembra aver calcato la mano solo nella definizione dei massimi edittali, dimostrandosi piuttosto noncurante – forse volutamente – nella graduazione del trattamento sanzionatorio e nella precisa individuazione della violazione. La genericità della formula utilizzata non rende affatto chiaro quale sia il margine di manovra lasciato agli Stati membri. L'elasticità della cornice edittale – descritta con la locuzione "fino a" – sembrerebbe *prima facie* consentire ai legislatori nazionali la possibilità di differenziare la risposta sanzionatoria in base

[82] Di recente, LABIANCA, *Il sistema delle tutele nel regolamento europeo,* cit., 1000

alla gravità delle violazioni; ma non è escluso che essi prediligano una lettura "minimalista", richiamando *sic et simpliciter* le disposizioni del Regolamento per non incorrere in procedure di infrazione.
A quest'ultima lettura sembra essersi ispirato il legislatore delegato nel riformare l'apparato sanzionatorio-amministrativo del D. Lgs. 196/2003. Il novellato art. 166 seleziona una lunga lista di violazioni, prevedendo che, per esse, si applichino a seconda dei casi le sanzioni di cui ai paragrafi 4 e 5 del GDPR[83], senza ulteriori specificazioni.

[83] Il primo comma dell'art. 166 prevede che siano soggette alla sanzione amministrativa di cui all'articolo 83, paragrafo 4, del Regolamento « le violazioni delle disposizioni di cui agli articoli 2-*quinquies*, comma 2 (Informativa sul consenso del minore in relazione ai servizi della società dell'informazione), 2-*quinquiesdecies* (Trattamento che presenta rischi elevati per l'esecuzione di un compito di interesse pubblico), 92comma 1 (Disciplina relative alla tenuta delle cartelle cliniche), 93, comma 1 (Disposizioni sul certificato di assistenza al parto), 123, comma 4 (Informativa da parte del fornitore di servizi di comunicazione elettronica sul trattamento dei dati relativi al traffico), 128 (Disciplina del trasferimento automatico della chiamata), 129, comma 2 (Inclusione del contraente negli elenchi telefonici), e 132-*ter* (Sicurezza del trattamento svolto da fornitori di servizi di comunicazione elettronica). Alla medesima sanzione amministrativa è soggetto colui che non effettua la valutazione di impatto di cui all'articolo 110, comma 1, primo periodo, ovvero non sottopone il programma di ricerca a consultazione preventiva del Garante a norma del terzo periodo del predetto comma».
Il secondo comma prevede che soggiacciano alla sanzione amministrativa di cui all'articolo 83, paragrafo 5, del Regolamento « le violazioni delle disposizioni di cui agli articoli 2-*ter* (Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri), 2-*quinquies*, comma 1(disciplina del consenso del minore in relazione ai servizi della società dell'informazione), 2-*sexies* (Trattamento di categorie particolari di dati personali necessari per motivi di interesse pubblico rilevante), 2-*septies*, comma 7 (Misure di garanzia per il trattamento di alcuni dati genetici e biometrici), 2-*octies* (Principi relativi al trattamento di dati relativi a condanne penali e reati), 2-*terdecies*, commi 1, 2, 3 e 4 (Diritti riguardanti le persone decedute) 52, commi 4 e 5 (Diffusione di sentenze recanti i dati identificativi delle parti), 75 (Specifiche condizioni del trattamento in ambito sanitario), 78 (Informativa fornita dal medico), 79 (Informativa fornita dalle strutture sanitarie), 80 (Informativa da parte di altri soggetti), 82 (Disciplina relativa alle emergenze e alla tutela della salute e dell'incolumità fisica), 92, comma 2, (disciplina dell'accesso alle cartelle cliniche), 93, commi 2 e 3 (sicurezza del trattamento dei dati relativi al parto), 96 (Trattamento di dati relativi a studenti da parte di istituzioni o enti di ricerca), 99 (Durata del trattamento dei dati raccolti per finalità di interesse pubblico o di analisi statistica), 100, commi 1, 2 e 4, (Dati relativi ad attività di studio e di ricerca), 101 e 105 commi 1, 2 e 4 (Modalità del trattamento), 110-*bis*, commi 2 e 3 (Trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici) 111 (Regole deontologiche per trattamenti nell'ambito del rapporto di lavoro), 111-*bis* (Informazioni in caso di ricezione di *curriculum*), 116, comma 1, (Accesso ai dati del fruitore di servizi di patronato e assistenza sociale) 120, comma 2 (Trattamento dei dati relativi a sinistri da parte di società di assicurazione) 122 (Accesso alle informazioni raccolte nei riguardi dell'utente di servizi di comunicazione elettronica), 123, commi 1, 2, 3 e 5 (Disciplina dei dati relativi al traffico), 124 (Regole sulla fatturazione), 125 (Identificazione della linea chiamante), 126 (Dati relativi all'ubicazione), 130, commi da 1 a 5 (Disciplina delle comunicazioni indesiderati), 131 (Informazioni ai contraenti sui rischi di captazione illecita dei dati) 132 (Conservazione dei dati di traffico per altre finalità), 132-*bis*, comma 2, (Procedure per garantire all'utente l'accesso ai propri dati), 132-*quater* (Informazioni sui rischi), 157 (Richiesta del Garante di informazioni e di esibizione di documenti), nonché delle misure di garanzia, delle regole deontologiche di cui rispettivamente agli articoli 2-*septies* e 2-*quater*».

A tal riguardo, nel parere della Commissione parlamentare si rinveniva una condivisibile proposta di emendamento per l'introduzione di un comma 8-*bis* all'art. 166, in base a quale *«nell'adozione dei provvedimenti sanzionatori, il Garante ha riguardo alla gravità della violazione, all'opera svolta dall'agente per l'eliminazione o attenuazione delle conseguenze della violazione [...] nonché alla personalità dello stesso, alle sue condizioni economiche ovvero alla dimensione dell'impresa con particolare riguardo alle micro, piccole e medie imprese»*[84]. La raccomandazione non ha tuttavia trovato seguito nella stesura del testo definitivo.

La Commissione parlamentare invitava inoltre a valutare l'opportunità di prevedere un minimo edittale per le sanzioni previste dal nuovo Regolamento, che, oltre a delimitare l'ampissima forbice sanzionatoria, avrebbe consentito l'accesso al pagamento in misura ridotta[85]. In base ai principi generali in tema di illecito amministrativo, questo rilievo espresso dalla Commissione non ci sembra però cogliere nel segno. Invero, l'art. 16 della legge 689/1981 prevede che sia possibile il pagamento in misura ridotta di una somma *«pari alla terza parte del massimo della sanzione prevista per la violazione commessa»* ovvero, ma soltanto se più favorevole, *«qualora sia stabilito il minimo della sanzione edittale, pari al doppio del relativo importo»*. Ne deriva che, pur in assenza di definizione di un limite edittale minimo, l'accesso al beneficio rimane certamente possibile, seppure la previsione di un minimo edittale avrebbe reso certamente più agevolmente percorribile questa soluzione in ragione dell'importo verosimilmente più ridotto da corrispondere.

Esaminando con attenzione il novellato art. 166, ci si rende subito conto che, nel coordinamento tra la disciplina del Testo Unico e quella del Regolamento Europeo, il legislatore ha selezionato soltanto alcune delle violazioni previste dall'art. 83 GDPR, riconducibili ad attività di trattamento di dati particolarmente sensibili (come quelli relativi alla salute o alle condanne penali) oppure ad attività di trattamento svolte da alcuni soggetti (fornitori di servizi di comunicazione elettronica, istituti di formazione, istituti di elaborazione statistica, strutture sanitarie). La norma non chiarisce quale sia il rapporto tra le violazioni contemplate dei primi due commi e quelle previste dall'art. 83 GDPR.

La previsione di una nutrita lista di violazioni della normativa nazionale potrebbe essere indicativa della volontà del legislatore nazionale di circoscrivere i confini dell'apparato sanzionatorio amministrativo, attuando solo in parte le previsioni del Regolamento. D'altra parte, si potrebbe ritenere che le viola-

[84] *Bollettino delle Giunte e delle Commissioni parlamentari* del 20 giugno 2018, cit. p. 21

[85] *Bollettino delle Giunte e delle Commissioni parlamentari, ibidem.*

zioni *de quibus* siano state inserite allo scopo di differenziare il trattamento sanzionatorio per alcune specifiche ipotesi, ferma la diretta applicabilità delle sanzioni comminate dall'art. 83 per i casi non contemplati dal medesimo art. 166. In quest'ultimo senso sembrerebbe deporre il terzo comma della disposizione che, indicando il Garante come l'organo competente a conoscere degli illeciti amministrativi, fa riferimento alle sanzioni «di cui all'articolo 83 del medesimo Regolamento e di cui ai commi 1 e 2», lasciando in tal modo intendere che le sanzioni amministrative previste dal GDPR siano direttamente applicabili e non necessitino di alcuna disposizione nazionale di attuazione. Tale lettura trova conforto anche nel mancato inserimento, nel testo dell'art. 166, delle violazioni dei principi basilari sulla liceità del trattamento[86] che, diversamente opinando, resterebbero prive di sanzione.
Dal combinato disposto di questo comma con i primi due, sembra potersi ricavare che la lunga elencazione di violazioni assolve a una *funzione integrativa* per quelle violazioni non direttamente previste dal Regolamento (ad esempio quelle previste per il trattamento di dati effettuato dai fornitori di servizi di patronato o assistenza sociale; oppure per l'oscuramento dei dati relativi al numero nelle chiamate in entrata), e a una *funzione di disciplina* per quelle violazioni *borderline* che potrebbero essere sanzionate ai sensi dei paragrafi 4 e 5 del Regolamento (come nel caso della violazione dei principi sull'informativa e sul consenso del caso di fruizione da parte dei minori di servizi della società dell'informazione). Comunque sia, la scelta legislatore della riforma non brilla per chiarezza. La predetta norma di coordinamento tra i testi legislativi rischia, all'opposto, di diventare l'ennesimo fattore di complicazione di un quadro normativo già di per sé di difficile lettura.
Ne deriva un sistema sanzionatorio amministrativo "integrato", in cui l'individuazione del precetto e della sanzione sarà rimessa all'abilità dell'interprete di collazionare segmenti di norme di disciplina, rinvenibili qua e là nei testi normativi, mentre la graduazione del trattamento sanzionatorio – prerogativa cui ha abdicato tanto il legislatore italiano quanto quello europeo – spetterà in ultima istanza all'Autorità competente ad irrogare le sanzioni amministrative.

5. La delega per la riforma del sistema sanzionatorio penale in materia di trattamento dei dati personali. Profili di illegittimità costituzionale.

[86] Prima ricompresi nel titolo II e III del Codice della privacy, abrogati dal D. Lgs. 101/2018. Cfr. Art. 6 e ss. GDPR.

Nel preambolo al GDPR si rinvengono espresse indicazioni circa la possibilità di prevedere un presidio penale. In particolare il *considerandum* n. 149 dispone che *«gli Stati membri dovrebbero poter stabilire disposizioni relative a sanzioni penali per violazioni del presente regolamento, comprese violazioni di norme nazionali adottate in virtù ed entro i limiti del presente regolamento»*, fermo restando che l'imposizione di sanzioni penali per violazioni di tali norme nazionali e di sanzioni amministrative *«non dovrebbe essere in contrasto con il principio del ne bis in idem quale interpretato dalla Corte di giustizia»*.

La disposizione va letta in combinato disposto[87] con l'art. 84 che impone agli Stati membri di prevedere sanzioni effettive proporzionate e dissuasive per le violazioni non soggette alle sanzioni amministrative pecuniarie di cui all'art. 83.

Al fine di dare attuazione a tali principi, la legge 25 ottobre 2017, n. 163 stabiliva espressamente che il Governo dovesse adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196, anche il sistema sanzionatorio penale, *«con previsione di sanzioni efficaci, dissuasive e proporzionate»* (art. 13, comma 3, lett. e), senza dettare alcun principio o criterio direttivo per il legislatore[88].

A ben vedere, la latitudine della delega solleva dubbi di violazione dell'art. 76 della Costituzione, avuto riguardo al potere di riformare il sistema sanzionatorio penale[89]. Con riferimento a quest'ultimo l'esercizio della delega sembra

---

[87] In dottrina si è parlato, a proposito del *considerandum* n. 149, della natura di "quasi direttiva" del Regolamento, nella parte in cui prescrive agli Stati membri di adottare sanzioni penali non solo per le violazioni del regolamento ma anche per la violazione delle norme nazionali da adottarsi in virtù del regolamento. A tal riguardo si precisa che, essendo la competenza in materia penale limitata alla fissazione di regole minime in settori tassativamente indicati o già oggetto di misure di armonizzazione (art. 83 TFUE), l'Unione non potrebbe introdurre direttamente norme incriminatrici. Cfr. LA MANUZZI., *Diritto penale e trattamento dei dati personali. I reati previsti dal Codice della privacy e la responsabilità amministrativa degli enti alla luce del regolamento 2016/679/UE*, cit., p. 253 la quale ritiene che la previsione di cui al citato *considerandum* potrebbe essere considerata come un esercizio atipico della competenza in materia penale attraverso lo strumento del regolamento in luogo della direttiva. Ciò non frustrerebbe tuttavia la *ratio* dell'art. 83 TFUE, poiché molte disposizioni del Regolamento in esame richiedono una normativa nazionale di recepimento.

[88] L'art. 13, comma 3, della legge 163/2017 dispone che *«Nell'esercizio della delega [...] il Governo è tenuto a seguire, oltre ai principi e criteri direttivi generali di cui all'articolo 32 della legge 24 dicembre 2012, n. 234, anche i seguenti principi e criteri direttivi specifici: [...] e) adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (UE) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse»*.

[89] In argomento gli studi di CUPELLI*., La legalità delegate. Crisi e attualità della riserva di legge nel diritto penale*, Napoli, 2012, p. 22 ss.; ID., *Il parlamento europeo e i limiti di una codecisione. Tra modelli di*

del tutto svincolato da criteri e principi direttivi, i quali neppure potrebbero essere enucleati facendo riferimento al Regolamento europeo, che non contiene alcuna indicazione sulle previsioni penali.
Invero, la determinazione dei principi e criteri della delega, per consolidata giurisprudenza costituzionale, ben può avvenire *per relationem*, con riferimento ad altri atti normativi, purché sufficientemente specifici[90]. L'indicazione dei principi e dei criteri direttivi di cui all'art. 76 Cost. non è infatti finalizzata a eliminare ogni discrezionalità nell'esercizio della delega ma soltanto a circoscriverla, in modo che resti pur sempre salvo il potere di valutare le specifiche e complesse situazioni da disciplinare. Le norme deleganti non possono però limitarsi a disposizioni *«talmente generiche da essere riferibili indistintamente a materie vastissime ed eterogene e, né possono esaurirsi in mere enunciazioni di finalità, ma debbono essere idonee ad indirizzare concretamente ed efficacemente l'attività normativa del Governo»*[91]. Nel caso in esame l'insufficienza della delega per la riforma del sistema sanzionatorio penale del D. Lgs. 196/2003 emerge con chiarezza dal confronto con quello amministrativo, per il quale il GDPR fornisce indicazioni di dettaglio sulle singole violazioni e sulla relativa cornice edittale. Solo in questo secondo caso appaiono soddisfatti i requisiti dettati dal Giudice delle leggi per la determinazione indiretta dei principi e dei criteri direttivi.
Alla assoluta mancanza di principi e criteri direttivi non sembra poter supplire il disposto dell'art. 32 della legge 234/2012[92], che non contiene alcun criterio direttivo generale che faccia venir meno il dubbio di illegittimità costituzionale dell'art. 13, comma 3, lett. e) della legge delega n. 163/2017[93].

---

democrazia e crisi della riserva di legge, in *Criminalia*, 2012, p. 545 ss.; ID., *Riserva di legge e carenza di delega legislativa nella tormentata vicenda dell'associazione militare con scopi politici: i nuovi spazi di sindacabilità del vizio procedurale*, in *Riv. it. dir. proc. pen.,* 2014, 2, p. 977 ss. Sugli strumenti di trasposizione interna degli obblighi di fonte UE e sulla legge di delegazione europea si veda anche GULLO, *Deflazione e obblighi di penalizzazione di fonte UE*, in *Dir. Pen. Cont.,* 10 febbraio 2016; GRANDI, *Le «qualità» della norma penale correlate al procedimento formativo nazionale e quello europeo*, in Grasso G., Picotti L., Sicurella R. (a cura di), *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011, p. 371 ss.

[90] Corte Cost. sent. n. 87/1989; n. 126/1996; n. 383/1998; n. 200/1999. Sul punto BELLOCCI, *La delega legislativa,* § 3.1 in *Quaderni di studio della Corte Costituzionale*, www.cortecostituzionale.it

[91] Così, Corte Cost. sent. n. 156/1987, § 4. Sui vizi della delega legislativa nella prospettiva del diritto costituzionale di rinvia a DE FIORES, *Trasformazioni della delega legislativa e crisi delle categorie normative,* Padova, 2001; CERVATI, *La delega legislativa*, Milano,1972.

[92] La norma enumera una serie di principi e criteri direttivi generali di delega per l'attuazione del diritto dell'Unione europea, che si aggiungono *ope legis* a quelli contenuti nella legge di delegazione e nelle direttive da attuare

[93] Dalla declaratoria di illegittimità costituzionale della delega deriverebbe la decadenza delle disposizioni di attuazione, e precisamente dell'intero art. 15, comma 1, del D. Lgs. 101/2018, fatta eccezione per

Il criterio di cui alla lettera d) attribuisce infatti al delegato la facoltà di prevedere sanzioni penali *«per le infrazioni alle disposizioni dei decreti»* laddove ciò sia *«necessario per assicurare l'osservanza delle disposizioni contenute nei decreti legislativi»* e *«solo nei casi in cui le infrazioni ledano o espongano a pericolo interessi costituzionalmente protetti»*, ma stabilendo un limite ben preciso: potranno essere introdotti per questa via soltanto contravvenzioni punite, in via alternativa o congiunta, con l'ammenda fino a Euro 150.000 e con l'arresto fino a tre anni.

Ciò è sufficiente a far ritenere prive di copertura le due nuove figure di illecito di cui agli artt. 167-*bis* e 167-*ter* del Codice della *privacy*, che, oltre ad essere configurati come delitti, sono puniti con pena detentiva che, nel massimo, supera quella consentita per l'arresto. Non rinvenendosi alcun altro principio e criterio generale che potesse giustificare, nel silenzio del regolamento europeo e del legislatore delegante, l'introduzione di tali fattispecie, vi è motivo di ritenere che esse siano costituzionalmente illegittime per violazione dell'art. 76 Cost.

Rimane da chiedersi se era nei poteri del legislatore delegato la riforma delle fattispecie di reato preesistenti (artt. 167-170 D. Lgs. 196/2003) e, quindi, se vi fossero principi direttivi generali in grado di supplire su questo fronte al difetto di delega.

A tal fine non soccorre il criterio direttivo sopra richiamato, che disciplina l'introduzione di sanzioni penali per le infrazioni dei decreti delegati *«al di fuori dei casi previsti delle norme penali vigenti»*.

Né, d'altro canto, poteva farsi riferimento al criterio di cui alla lettera e)[94] relativo alla rivisitazione di una materia già oggetto di misure di armonizzazione. Sebbene il Regolamento abbia disciplinato *ex novo* una materia pregressa, in nessun atto legislativo precedente si rinvengono norme relative all'adozione di fattispecie di reato per le violazioni della disciplina sul trattamento dei dati personali. Se ne deduce che, nel modificare le disposizioni del Codice della *privacy*, il legislatore non avrebbe potuto revisionare anche l'apparato sanzionatorio penale.

---

la sola lett. a), nella parte in cui modifica l'apparato sanzionatorio amministrativo. In relazione a quest'ultimo, infatti, non si ravvisano profili di illegittimità costituzionale, tenuto conto della possibilità di ricavare i criteri direttivi dalle disposizioni sanzionatorie del GDPR.

[94] Si tratta del criterio generale secondo cui al recepimento di direttive o all'attuazione di altri atti dell'Unione europea che modificano precedenti direttive o atti già attuati con legge o con decreto legislativo *«si procede, se la modificazione non comporta ampliamento della materia regolata, apportando le corrispondenti modificazioni alla legge o al decreto legislativo di attuazione della direttiva o di altro atto modificato»*.

Altrettanto inconferente è il richiamo al successivo art. 33[95] della legge del 2012 che, nel disciplinare il conferimento della delega per le violazioni di atti normativi dell'Unione, invita il legislatore ad adottare sanzioni penali per le infrazioni di obblighi contenuti in direttive europee *«al fine di assicurare la piena integrazione delle norme dell'Unione europea nell'ordinamento nazionale».* Si tratta di una disposizione di natura soltanto programmatica, avente come destinatario il legislatore delegante.

Quand'anche se ne volesse affermare l'efficacia immediatamente precettiva, quale fondamento di una facoltà generalizzata di rivisitazione delle disposizioni sanzionatorie penali nel recepimento di atti normativi dell'Unione, si dovrebbe comunque riconoscere che l'inciso finale *«per i quali non sono già previste sanzioni penali o amministrative»* ponga un limite insuperabile nell'esercizio della delega. Si deve pertanto escludere che, nell'attuazione del Regolamento 679/2016/UE, il legislatore avesse il potere di riformare *ad libitum* una disciplina sanzionatoria penale già esistente.

Nessun criterio direttivo utile sembra potersi ricavare dal secondo comma della disposizione, che si limita a prevedere che i decreti legislativi debbano informarsi *«oltre che ai principi criteri direttivi di cui all'articolo 32, comma 1, lettera d), della presente legge, a quelli specifici contenuti nella legge di delegazione europea, qualora indicati».*

Dal combinato disposto delle disposizioni sopra richiamate, si può trarre la conclusione che la delega legislativa in esame era limitata al mero adeguamento del sistema sanzionatorio ai nuovi obblighi previsti dal Regolamento[96], da cui non può dedursi la facoltà per il delegato di rivisitare gli elementi costitutivi e il trattamento sanzionatorio delle fattispecie di reato esistenti, né tantomeno quella di introdurre nuove incriminazioni.

6. I reati in materia di *privacy*: uno sguardo d'insieme.

[95] Il primo comma della disposizione esprime il principio secondo cui *«la legge di delegazione europea delega il Governo ad adottare, entro la data dalla stessa fissata, disposizioni recanti sanzioni penali o amministrative per le violazioni di obblighi contenuti in direttive europee [...] o in regolamenti dell'Unione europea pubblicati alla data dell'entrata in vigore della stessa legge di delegazione europea, per i quali non sono già previste sanzioni penali o amministrative».*

[96] Inquadrata la questione in questi termini, si ritiene che rientrasse nella facoltà del delegato la riforma delle fattispecie vigenti soltanto nella misura in cui ciò fosse necessario per reprimere le violazioni di obblighi previsti dal GDPR. *Nulla quaestio*, dunque, se il legislatore si fosse limitato ad aggiornare l'elenco delle violazioni presupposto della responsabilità per illecito trattamento di dati (art. 167), o a indicare nuovi riferimenti normativi per l'individuazione delle ipotesi in cui è punita la falsità delle comunicazioni al Garante (art. 168).

Mettendo ora da parte i rilievi sopra espressi in punto di violazione dell'art. 76 Cost., passiamo ad esaminare nel dettaglio le diverse modifiche apportate al tessuto penalistico che, come si è prima ricordato, era rimasto pressoché inalterato rispetto all'impianto risalente alla l n. 675/1996.

L'immobilismo del sistema è stato oggetto di aspre critiche in dottrina, specie per quel che riguarda la tendenza alla "panpenalizzazione"[97] e all'impiego di sanzioni penali per la tutela di beni strumentali rispetto alla riservatezza. Le censure sollevate avevano ad oggetto le scelte di criminalizzazione e, più in generale, la tecnica di redazione delle fattispecie di reato.

Si criticava in particolare la carenza di offensività di alcune ipotesi, legate alla mera inosservanza degli obblighi sul trattamento dei dati o costruite sull'ostacolo alle prerogative dell'Autorità di settore. Così nel caso di omessa adozione di misure di sicurezza o di inosservanza dei provvedimenti del Garante, il legislatore avrebbe dovuto assegnare un ruolo predominante alla sanzione amministrativa o, tuttalpiù, a fattispecie contravvenzionali[98]. Il sistema sanzionatorio delineato dal D. Lgs. 196/2003 *ante* riforma sembrava invece ispirarsi all'opposto principio della criminalizzazione di condotte di mera omissione, in cui era marginale il ruolo attribuito alla sanzione amministrativa. Si delineava così un "sistema bipolare"[99] nel quale appariva piuttosto sfumata la funzione di *extrema ratio* dell'intervento penale e confusa la demarcazione delle sfere di tutela tra sanzioni penali e violazioni amministrative[100].

---

[97] Cfr. VENEZIANI., *I beni giuridici tutelati dalle norme penali in materia di riservatezza informatica e disciplina dei dati personali,* cit., p. 187; ID., *Beni giuridici protetti e tecniche di tutela penale nella nuova legge sul trattamento dei dati personali,* cit., p. 177. In proposito appare opportuno richiamare le Raccomandazioni espresse all'esito del XV Congresso Internazionale di diritto penale, tenutosi a Rio De Janeiro dal 4 al 10 settembre 1994, il cui testo è pubblicato sulla *Rivista trimestrale di diritto penale dell'economia*, 1994, 3, p. 1286 ss., in cui l'AIDP ribadisce la necessità di orientare l'intervento penale alla luce dei criteri di sussidiarietà ed *extrema ratio*. In particolare, che *«le previsioni penali nel settore della privacy siano [...] usate solo in casi gravi in specie quelli relativi a dati altamente sensibili o concernenti informazioni confidenziali».*

[98] Nei contesti nei quali il legislatore voglia favorire l'adozione di misure idonee a garantire la migliore tutela dell'interesse protetto, disincentivando la creazione di una situazione di pericolo, il ricorso a sanzioni amministrative appare certamente la scelta più rispettosa dei principi di offensività e di *extrema ratio* del diritto penale. Per approfondimenti, PALIERO, *La sanzione amministrativa come moderno strumento di lotta alla criminalità economica*, in *Riv. trim. dir. pen. ec.,* 1993, pp. 1021 ss.; ID., *Le alternative alla tutela penale: l'illecito amministrativo*, in Aa Vv., *Il sistema sanzionatorio penale e le alternative di tutela*, Milano, 1998, p. 12 ss. Di recente, MAZZACUVA, *Le pene nascoste*, cit., p. 125 ss.

[99] L'espressione è di MANNA, *Il quadro sanzionatorio penale e amministrativo del codice sul trattamento dei dati personali*, cit., p. 740

[100] Nel sistema previgente, erano sanzionate come illecito amministrativo le violazioni seguenti: omessa o inidonea informativa all'interessato (art. 161); sanzioni in materia di conservazione dei dati di traffico (art. 162-*bis*); sanzioni nei confronti di fornitori di servizi di comunicazione elettronica accessibili al pubblico (art. 162-*ter*); omessa o incompleta notificazione (art. 163); omessa informazione o esibizione

Nel sistema previgente, vi erano perfino dei casi in cui le due sfere di tutela convergevano fino alla sovrapposizione, dando luogo all'applicazione cumulativa[101] della pena e della sanzione pecuniaria[102].
Un secondo rilievo di fondo mosso all'impianto sanzionatorio del Codice ha riguardato la formulazione delle fattispecie penali in funzione meramente sanzionatoria della disciplina sul trattamento dei dati personali. La tecnica c.d. del rinvio suscita non poche perplessità sul piano della intellegibilità del precetto che, per sua natura, dovrebbe essere chiaro e immediatamente comprensibile ai consociati[103]. Le sanzioni penali del D. Lgs. 196/2003 sembrano apposte «a mo' di appendice»[104] per il caso di inosservanza di tutta una serie di disposizioni che oltre ad essere connotate da una crescente complessità – dovuta alla sofisticazione del sistema – sono formulate tenendo conto degli schemi e delle esigenze proprie della disciplina sostanziale di settore[105].
Date queste premesse, vediamo quale sono state le direttrici seguite dal legislatore in sede di riforma.

---

al Garante (art. 164); altre fattispecie (art. 162). Il D. Lgs. 101/2018 ha abrogato tutte le disposizioni ora elencate, includendone alcune nel novellato art. 166 ed espungendone altre.

[101] Di recente sulla tecnica sanzionatoria del doppio binario nella manualistica BENAZZI, *Sanzioni amministrative per violazioni ritenute penalmente rilevanti,* in Cadoppi A. Canestrari S. Manna A. Papa M. (diretto da), *Diritto penale dell'economia,* Tomo I, Torino, 2017, p. 1295; TRIPODI., *Ne bis in idem e reati tributari*, in Cadoppi Canestrari Manna Papa (diretto da), *Diritto penale dell'economia*, cit., p. 684 ss. In rapporto con il divieto di *bis in idem* si veda D'ALESSANDRO, *Tutela dei mercati finanziari e rispetto dei diritti umani fondamentali*, in *Dir. pen. proc.,* 2014, p. 614; TRIPODI, *Uno più uno (a Strasburgo) fa due. L'Italia condannata per violazione del ne bis in idem in tema di manipolazione del mercato*, in *Dir. pen. cont.*; VIGANÒ, Una nuova sentenza di Strasburgo su ne bis in idem e reati tributari, in Dir. pen. cont., 2017, 5, p. 392 ss.; FIMIANI, *Market abuse e doppio binario sanzionatorio dopo la sentenza della Corte E.D.U., Grande Camera, 15 novembre 2016, A e B c. Norvegia*, in *Dir. pen. cont.,* 2017, 2, p. 5 ss.; BASILE, *Una nuova occasione (mancata) per riformare il comparto penalistico degli abusi di mercato?,* in *Dir. pen. cont.,* 2017, 5, p. 271 ss.;

[102] Quando il trattamento di dati personali era effettuato in violazione delle misure minime di sicurezza o delle disposizioni elencate nell'art 167 si applicava in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma di denaro (art. 162, comma 2-*bis*); lo stesso accadeva in caso di inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieto di cui, rispettivamente, all´articolo 154, comma 1, lettere c) e d), in cui si applicava altresì la sanzione amministrativa pecuniaria (art. 162, comma 2-*ter*).

[103] La chiarezza del precetto penale è servente alla sua conoscibilità. A tal fine il diritto penale si fonda sul principio generale di tassatività. Cfr. MANTOVANI, *Principi di diritto penale*, Padova, 2002, p. 20; PALAZZO, *Introduzione ai principi del diritto penale,* Torino, 1999, p. 254.

[104] In questo senso VENEZIANI, *Beni giuridici protetti e tecniche di tutela penale nella nuova legge sul trattamento dei dati personali,* cit., p. 143

[105] Secondo SEMINARA, *Appunti in tema di sanzioni penali nella legge sulla privacy*, in *Resp. civ. e prev.,* 1998, 4-5, p. 915 ss. l'imputazione penalistica presenta caratteristiche autonome, la cui valorizzazione è preclusa dal richiamo integrale di norme il cui contenuto risponde a diverse esigenze.

6.1. L'illecito trattamento di dati.

L'illecito trattamento di dati (art. 167) è la fattispecie di reato centrale dell'impianto sanzionatorio del D. Lgs. 196/2003[106]

Secondo la nuova formulazione[107], la condotta incriminata consiste nel fatto di chi al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 (dati relativi al traffico, all'ubicazione e disciplina delle comunicazioni indesiderate) o dal provvedimento di cui all'articolo 129 (inserimento e utilizzo degli elenchi dei contraenti), arreca nocumento all'interessato. Il rinvio alle norme di disciplina è riferito ai dati personali (diversi da quelli sensibili e giudiziari) trattati in violazione delle citate disposizioni in materia di servizi di comunicazione elettronica. Non è stato tuttavia riproposto il riferimento all'art. 23 (abrogato), che attribuiva rilevanza all'illecito trattamento di dati effettuato senza il consenso degli interessati. Deve pertanto ritenersi che nel passaggio dalla precedente alla attuale formulazione vi sia stata una *abolitio criminis* parziale e che la violazione dei principi sul consenso costituirà unicamente illecito amministrativo ai sensi dell'art. 83, par. 5, lett a) GDPR. Così facendo il legislatore ha mutato profondamente l'ontologia del reato, che sarà applicato ad un numero piuttosto circoscritto di violazioni.

Il secondo comma punisce con pena più severa (reclusione da uno a tre anni) il medesimo fatto, commesso procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-*sexies* e 2-*octies*, (trattamento di categorie particolari di dati personali necessari per motivi di interesse pubblico rilevante o relativi a condanne penali e reati), o delle misure di garanzia di cui all'articolo 2-*septies* (misure relative al trattamento dei dati genetici, biometrici e relativi alla salute) ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-*quinquiesdecies* (misure relative ai trattamenti che presentano rischi elevati per l'esecuzione di un compito di interesse pubblico)[108].

---

[106] Per un commento ANTONINI, *Il trattamento illecito di dati personali nel codice della privacy: i nuovi confini della tutela penale,* in *Dir. pen. proc.*, 2005, 3, 338 ss.; CORRIAS LUCENTE, *La nuova normativa penale a tutela dei dati personali,* cit. p. 632; LOTIERZO, *Del nocumento nell'illecito trattamento dei dati personali ovvero dell'esigenza di ascendere alle origini di una incriminazione,* in *Cass. pen.,* 2013, p. 1589 ss.; MANNA, *Prime osservazioni sul Testo Unico in materia di protezione dei dati personali: profili penalistici*, in *www.privacy.it.*

[107] L'art. 15, comma 1, lett. b) del D. Lgs. 101/2018 ha sostituito interamente il testo dell'art. 167. La precedente formulazione puniva chi, *«al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130 se dal fatto deriva nocumento».*

[108] Si richiamano le regole in materia di trattamenti che presentano rischi specifici, tra cui i principi applicabili al trattamento dei dati giudiziari, sanitari, e, in genere, quelli sensibili.

La stessa pena si applica anche a chi, ai medesimi fini, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti dagli articoli 45, 46 o 49 del Regolamento, arrechi nocumento all'interessato (art. 167, comma 3).
Pur presentando forti similitudini con quelle descritte dalla norma previgente[109], le condotte incriminate sono ora configurate come reati di evento. Nella precedente formulazione l'illecito trattamento di dati era punito *«se dal fatto deriva[va] nocumento»*, inciso che aveva acceso un intenso dibattito sulla natura giuridica di tale elemento. Il nocumento[110] si inseriva, infatti, nel corpo di una fattispecie caratterizzata dal dolo specifico di trarre profitto per sé o per altri o di recare ad altri un danno. Ciò dava luogo a una incongruità notevole: il nocumento, che doveva verificarsi ai fini della integrazione/punibilità del reato, coincideva con una parte del dolo specifico. In dottrina era prevalsa la tesi secondo cui il requisito del nocumento dovesse essere ricondotto alla controversa figura delle condizioni obiettive di punibilità intrinseche[111]. Si ar-

[109] Il testo dell'art. 167 riprendeva pressoché totalmente la formulazione dell'art. 35 della legge 675/1996, dalla quale aveva ereditato non solo la struttura in due commi differenziati in base alla natura dei dati oggetto del trattamento, ma anche la tecnica del rinvio alla normativa extrapenale e la punibilità a titolo di dolo specifico. Sulla conformazione della fattispecie previgente SEMINARA, *Appunti in tema di sanzioni penali nella legge sulla privacy,* cit. p. 914.
La modifica più rilevante introdotta dal Testo Unico fu l'inserimento nella fattispecie base dell'inciso "se dal fatto deriva nocumento", che prima era previsto come circostanza aggravante dal terzo comma dell'art. 35. Con l'aggiunta di questo elemento sembra che il legislatore abbia voluto sopire le critiche formulate sulla inoffensività di alcune violazioni della disciplina di settore.
[110] Dal punto di vista semantico il "nocumento" è un *minus* rispetto al danno in senso giuridico. La presenza di questo elemento all'interno di una fattispecie di pericolo, offre un appiglio per poter sostenere la natura di pericolo concreto del reato. È di questo avviso la giurisprudenza di legittimità secondo cui la riforma del 2003 ha segnato il passaggio da una figura di reato di pericolo astratto a una figura di reato di pericolo concreto. Cfr. Cass. Pen. Sez. III, 9 luglio 2004 n. 30134, in *Dir. pen. proc.*, 2005, 3, 338 ss.; Cass. Pen, Sez. III, 26 marzo 2004, n. 26680 in *Cass. Pen.*, 2006, 7-8, pp. 2564 ss.; Cass. Pen., Sez. III, 15 giugno 2012, n. 23789, in *Cass. Pen.*, 2013, 4, p. 1578 ss.; Cass. Pen. Sez. III, 17 dicembre 2013, n. 5107, in *Cass. Pen.* 2014, 6, p. 2057.
[111] In questo senso MANNA, *Il quadro sanzionatorio penale e amministrativo del codice sul trattamento dei dati personali*, cit., p. 747; Id., *Prime osservazioni sul Testo Unico in materia di protezione dei dati personali: profili penalistici,* cit. p. 4; MANNA, DI FLORIO, *Riservatezza e diritto alla privacy: in particolare la responsabilità per omissionem dell'internet provider*, cit., 897; ANTONINI, *Il trattamento illecito di dati personali nel codice della privacy: i nuovi confini della tutela penale,* cit. p. 342. *Contra* CORRIAS LUCENTE., *La nuova normativa penale a tutela dei dati personali,* cit. p. 644.
Sul tema, in generale, BRICOLA, *Punibilità (condizioni obiettive di),* in *Noviss. Dig.,* XIV, Torino, 1967, p. 588 ss.; ANGIONI, *Condizioni di punibilità e principio di colpevolezza,* in *Riv. it. dir. proc. pen,* 1989, 144; NEPPI MODONA, *Concezione realistica del reato e condizioni obiettive di punibilità*, in *Riv. it. dir. proc. pen.*, 1971, 1-2, p. 184. Di recente, in materia penale fallimentare ZANCHETTI, *Incostituzionali le fattispecie di bancarotta? Vecchi quesiti e nuove risposte (o magari viceversa), alla luce della giurisprudenza di legittimità sul ruolo del fallimento nella bancarotta fraudolenta prefallimentare*, in *Riv. trim. pen. ec.*, 2014, 120; MASULLO, *La sentenza dichiarativa di fallimento è condizione obiettiva di punibili-*

gomentava che, sebbene l'inclusione tra gli elementi costitutivi del reato potesse contare sul rilievo che il nocumento concorresse a definire l'interesse giuridicamente protetto[112], a sostegno dell'inquadramento tra le condizioni obiettive di punibilità deponesse la previsione del dolo specifico. Sarebbe stato infatti irragionevole[113] prevedere quale evento del reato una finalità che, come noto, non è necessario si realizzi ai fini della integrazione del reato. La stessa dottrina rinveniva un rapporto sinergico tra condizione obiettiva di punibilità e dolo specifico, nel senso che la prima avrebbe assolto alla funzione di criterio selettivo della meritevolezza di pena sul piano oggettivo, mentre il secondo avrebbe operato sul piano soggettivo. In tal senso, sarebbero state meritevoli di sanzione penale soltanto quelle condotte tali da attualizzare una effettiva e tangibile lesione del diritto alla riservatezza, inteso nella sua ampia accezione di interesse dell'individuo alla consapevole divulgazione e alla corretta gestione dei dati personali che lo riguardano. Così, ad esempio, l'indebita comunicazione a terzi dei dati personali al fine di un loro utilizzo a scopo commerciale, sarebbe stato punito a condizione che si determinasse un reale nocumento per l'interessato (costretto, ad esempio a tollerare il continuo invio di messaggi promozionali[114]).

Parimenti si discuteva circa l'inquadramento dogmatico della seconda parte del primo comma nel quale si prevedeva una pena maggiore *«se il fatto consiste[va] nella comunicazione o diffusione».* La tesi più convincente[115] era nel senso di ritenere che si trattasse di una condotta autonoma e più grave rispetto a quella descritta nella prima parte della disposizione.

---

tà: quando affermare la verità non costa nulla, in *Riv. it. dir. proc. pen.*, 2017, p. 1151.

[112] Tale lettura avrebbe il pregio di soddisfare appieno le esigenze derivanti dal principio di colpevolezza e di personalità della responsabilità penale, ma si scontra con argomenti testuali e logici apparentemente insuperabili.

[113] MANNA, *Il quadro sanzionatorio penale e amministrativo del codice sul trattamento dei dati personali*, cit., p. 748

[114] Cfr. Cass. Pen., Sez. III, 15 giugno 2012, n. 23789, nel quale la Corte ha affermato che anche il reiterato invio di massaggi per finalità di *marketing* è idoneo ad arrecare un nocumento all'interessato, in termini di perdita di tempo

[115] Proposta da CORRIAS LUCENTE, *La nuova normativa penale a tutela dei dati personali,* cit. p. 646. La tesi faceva leva, anzitutto, sulla natura meramente specializzante della comunicazione e della diffusione, che, non differenziandosi dall'attività di trattamento dei dati, rappresentava un segmento eventuale dello stesso; *in secundis* sulla maggiore offensività per il bene giuridico, giacché le due condotte evidenziavano il massimo grado di offesa alla riservatezza dell'individuo. Contra MANNA, *Il quadro sanzionatorio penale e amministrativo del codice sul trattamento dei dati personali*, cit., p. 747 secondo cui l'inciso, adempiendo alla funzione di restringere l'area della punibilità a quelle condotte particolarmente offensive dell'oggettività giuridica protetta dalla norma, e facendo emergere il bisogno di una pena maggiore rispetto alla verificazione del nocumento per l'interessato, descriveva anche qui una condizione obiettiva di punibilità.

Con la riscrittura dell'art. 167, la causazione del nocumento è stata inserita, come detto, tra gli elementi costitutivi del reato. L'illecito trattamento di dati è ora configurato secondo lo schema tradizionale dei reati ad evento naturalistico: il legislatore ha in tal modo conseguito l'auspicabile risultato di far rientrare il nocumento all'interessato a pieno titolo nell'oggetto del dolo, evitando di scomodare la controversa figura dogmatica delle condizioni obiettive intrinseche di punibilità.

Per quel che riguarda il dolo specifico, nulla è mutato rispetto alla formulazione precedente. Lo schema di decreto prevedeva inizialmente la scomparsa della finalità *«di recare ad altri un danno»*, giustificata dalla diversa funzione attribuita al nocumento. Tale soluzione avrebbe però potuto determinare un restringimento dell'ambito operativo della norma, tagliando fuori le condotte di illecita diffusione di dati o immagini personali per finalità di carattere non economico; si pensi al fenomeno del *revenge porn* o dello *slut shaming*, che non sarebbero più rientrati nell'alveo di questa disposizione. Accogliendo i rilievi formulati in sede consultiva[116], il legislatore delegato è così tornato sui suoi passi, mantenendo il dolo specifico alternativo che caratterizza la disposizione fin dalla sua prima introduzione.

Non si può tuttavia fare a meno di notare che la reintroduzione della finalità di danno si inserisce – diversamente dal passato – in una fattispecie in cui è presente un evento naturalistico. Si viene così a creare un particolarissimo binomio (dolo specifico e evento) polarizzato su requisiti molto simili: il soggetto dovrà agire al fine di arrecare danno all'interessato, proposito che, almeno in parte, è necessario che si realizzi (*sub specie* di nocumento) per l'integrazione del reato. Il dolo specifico di danno potrà dunque dispiegare una reale funzione selettiva delle condotte penalmente rilevanti soltanto nei

---

[116] La Commissione parlamentare per l'esame lo schema di decreto di attuazione del GDPR aveva espresso preoccupazione per l'eliminazione del riferimento alla finalità di danno nel testo dell'art. 167. Nel *Bollettino delle Giunte e delle Commissioni parlamentari* del 20 giugno 2018, cit., p. 19 si invitava il Governo *«a valutare la possibilità di prevedere, oltre alla finalità del profitto per sé o per altri, anche quella del danno all'interessato, al fine di evitare di affievolire la tutela contro fatti incresciosi come il 'revenge porn' o lo 'slut shaming', che dovrebbero al contrario essere oggetto di attenta tutela».* In argomento, RESTA, *I reati in materia di protezione dei dati personali,* cit. 1035

Anche il Parere reso dall'Autorità Garante era nel senso di considerare, quale oggetto alternativo del dolo specifico anche il nocumento *«in ragione dell'esigenza di presidiare con la sanzione penale condotte connotate da un simile disvalore, anche quando sorrette dal dolo di danno e non solo da quello di profitto. Tale modifica consentirebbe inoltre di assicurare una maggiore continuità normativa con la fattispecie vigente e di evitare gli effetti (anche sui processi in corso) dell'abolitio criminis che si dovesse ravvisare, in parte qua, per effetto della novellazione proposta».* Cfr. *Parere sullo schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679*, cit., § 1.4

rari casi in cui il trattamento illecito cagioni un semplice senso di frustrazione, noia o fastidio all'interessato (sussumibili nel concetto di nocumento, ma non in quello di danno): per la configurabilità del reato sarà in questo caso necessario che il reo abbia agito per uno scopo ulteriore e più profondo rispetto al semplice "dare fastidio", cioè al fine di provocare *stricto sensu* un danno (inteso quale lesione di un diritto dell'interessato).

La nuova formulazione dell'art. 167 non sembra poter "intaccare" lo stato dell'arte sulla responsabilità omissiva dell'*internet provider* per illecito trattamento di dati. Sebbene il primo comma della disposizione preveda alcune violazioni-presupposto ascrivibili ai fornitori di servizi digitali (in particolare quelle relative ai dati di traffico e di ubicazione; alla disciplina delle comunicazioni indesiderate; o all'utilizzo degli elenchi dei contraenti), che in astratto potrebbero essere commesse anche attraverso un *non facere* antigiuridico[117], resta il fatto che la definizione legislativa di trattamento[118] include condotte di tipo necessariamente commissivo[119].

Esclusa dunque la possibilità di configurare un trattamento illecito in forma puramente omissiva, rimane da chiedersi se nel riformato quadro legislativo vi sia spazio per una responsabilità omissiva impropria del *provider ex* artt. 167 D. Lgs. 196/2003 e 40, comma 2, c.p. per omesso impedimento del reato commesso dai terzi fruitori del servizio. La fattispecie è ora strutturata come un reato di evento, elemento che fa venir meno una delle principali obiezioni a sostegno della tesi della inapplicabilità della clausola di equivalenza[120].

---

[117] Ad esempio, omettendo di anonimizzare i dati relativi all'ubicazione oppure di fornire adeguata informativa agli utenti.

[118] L'art. 4, comma 2 GDPR definisce trattamento *«qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione».*

[119] Una diversa interpretazione rischierebbe infatti di collidere con il principio di legalità. Di questo avviso MANNA, DI FLORIO, *Riservatezza e diritto alla privacy,* cit., 904; MANNA, *I soggetti in posizione di garanzia*, in *Dir. Inf.,* 2010, 6, 786. Come noto, nella prassi giudiziaria più recente si registra un solo precedente favorevole alla configurabilità dell'illecito trattamento di dati in forma omissiva (Trib. Milano, 12.4.2010 n. 1972, caso *Google* vs *Vividown*), oggetto di aspre critiche in dottrina. Per approfondimenti di rinvia a INGRASSIA, *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine?,* in Lupària L. (a cura di), *Internet provider e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale,* Milano, 2012, 15 ss.

[120] Cfr. MANNA, *I soggetti in posizione di garanzia*, cit., 786. In giurisprudenza esclude la contestazione in forma omissiva al *provider* dell'illecito trattamento di dati in quanto reato di mera condotta App. Milano, 22 dicembre 2012, n. 8611, in *Diritto Penale Contemporaneo*, 04 marzo 2013, con nota di INGRASSIA, *La Corte d'Appello assolve i manager di Google anche dall'accusa di illecito trattamento dei dati personali.*

Cionondimeno, sebbene non siano mancate decisioni di segno contrario[121], resta il dato incontestabile della mancanza di una norma a fondamento del generale obbligo di sorveglianza degli utenti della rete, affiancato dall'ovvia considerazione che l'obbligo di rimozione dei contenuti illeciti sorge quando il reato si è già consumato[122]. Rimane quindi ferma, a nostro modo di vedere, l'impossibilità di ricorrere al paradigma della responsabilità omissiva impropria per sanzionare l'omesso impedimento da parte dell'ISP dell'illecito trattamento commesso da terzi.

6.2. La falsità nelle dichiarazioni e notificazioni al Garante.

L'art. 168 del Codice è considerato un reato ostacolo, volto a tutelare le prerogative e le funzioni dell'Autorità Garante. La disposizione non era inizialmente presente nel testo della legge 675/1996, nella quale si faceva menzione della sola omessa e incompleta notificazione (art. 34). Successivamente, l'art. 16 del D. Lgs. 28 dicembre 2001, n. 467, introdusse l'art. 37-*bis* confluito in misura pressoché integrale nel nuovo Codice della *privacy*[123]. Il Legislatore del 2003 non aveva infine riproposto[124] nel Codice il reato di omessa o incompleta notificazione, degradato a illecito amministrativo (art. 163)[125].

---

[121] Il riferimento è alla recente pronuncia Cass. Pen., Sez. V, 27 dicembre 2016, n. 59496 in cui la Corte, pronunciandosi al termine di una vicenda in cui il gestore di un sito Internet era stato tratto in giudizio per concorso (omissivo) in diffamazione, ha ritenuto immune da vizi a sentenza d'appello. I giudici di legittimità hanno affermato che il gestore del sito può essere ritenuto responsabile a titolo omissivo per avere consapevolmente mantenuto *online* il contenuto diffamatorio, con ciò postulando la natura di reato permanente della diffamazione. Viene così avvalorata la tesi – invero piuttosto audace – di una sostanziale equivalenza tra *permanenza del reato* e per *permanenza degli effetti* del reato, tale per cui l'omesso impedimento della ritrasmissione del file (e dunque l'approfondimento dell'offesa all'altrui reputazione) assumerebbe rilievo *ex* art. 40, capoverso. In dottrina a favore dell'estensione della responsabilità per omesso impedimento degli effetti MANNA, DI FLORIO, *Riservatezza e diritto alla privacy,* cit., 912; *contra*, PANATTONI., *Il sistema di controllo successivo: obbligo di rimozione dell'ISP e meccanismi di notice and take down,* in *Dir. Pen. Cont. – Riv. Trim*, 2018, 5, 250; CARBONE, *Responsabilità del* blogger*: parziale* revirement *della Cassazione?*, in *Cass. Pen.*, 2017, 7-8, 2782 ss.

[122] Sono queste soltanto alcune delle obiezioni che la dottrina prevalente ha sollevato contro il paradigma di responsabilità omissiva impropria dell'*internet provider*. Per gli opportuni approfondimenti si rinvia al lavoro di INGRASSIA, *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine?,* cit., 12 ss

[123] Per un commento, MANNA, *Il quadro sanzionatorio penale e amministrativo del codice sul trattamento dei dati personali*, cit. p. 757; CORRIAS LUCENTE, *La nuova normativa penale a tutela dei dati personali,* cit. p. 647.

[124] L'art. 34 della legge 675/1996 nella formulazione iniziale puniva con la reclusione da tre mesi a due anni chi *«essendovi tenuto, non provvede alle notificazioni prescritte [...], ovvero indica in esse notizie incomplete o non rispondenti al vero».*

[125] La scelta di riservare la sanzione penale alle sole condotte connotate da mendacio era in armonia con le opzioni politico criminali effettuate in altri rami dell'ordinamento Artt. 2621, 2622, 2638 cc.; Artt.

La condotta era descritta come il fatto di chi *«nelle comunicazioni di cui all'articolo 32-bis, commi 1 e 8, nella notificazione di cui all'articolo 37 o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi»*[126].

L'intervento riformatore ha apportato significative novità, modificando la rubrica della norma in *«Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante»,* includendovi due distinte ipotesi di reato.

La prima ipotesi punisce, salvo che il fatto costituisca più grave reato, *«chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi».* La nuova formulazione risulta più chiara e meno ridondante, ma taglia fuori alcune ipotesi di falsità. Non viene infatti riproposto il riferimento alle comunicazioni del *provider* in caso di violazione dei dati e le notificazioni relative al trattamento di dati sensibili, la cui falsità, salvo che sia commessa nel corso di un procedimento o di un accertamento, ha perso rilevanza penale con conseguente applicazione del regime di cui all'art. 2, comma 2, c.p.[127].

La seconda ipotesi punisce con la reclusione sino ad un anno *«chiunque intenzionalmente cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti».* I fatti descritti dalla norma non rientrano tra quelli precedentemente puniti; si tratta dunque di una nuova incriminazione, introdotta "a chiusura" del sistema di modo da sanzionare tutte quelle condotte che, pur non risolvendosi in un mendacio, ostano alla speditezza dei procedimenti e degli accertamenti svolti

---

139, comma 2 e 140, comma 2, D. Lgs. 385/1993. Oggi l'omessa e incompleta notificazione del *data breach* all'autorità di controllo è sanzionata ai sensi degli artt. 33 e 83, par. 4., GDPR. Non vi è dubbio che l'omissione *tout court* nelle informazioni costituisca illeciti amministrativo, dando luogo alla violazione del disposto dell'art. 33. Rimane dubbia la configurabilità dell'illecito quando la notifica non presenti tutti i requisiti contenuti al par. 3 dell'art. 33 e risulti, quindi, incompleta. L'art. 83, par. 4, fa infatti riferimento alla violazione dell'art. 33, senza specificare il paragrafo di riferimento, con ciò lasciando intendere che qualsiasi violazione della norma di disciplina – dunque anche la mancanza di uno dei requisiti ivi previsti – costituisce illecito amministrativo. Sulla scarsa precisione nella formulazione del precetto si rinvia ai rilievi che abbiamo effettuato *supra* (§ 4).

[126] I veicoli informativi che venivano in rilievo erano le comunicazioni che il fornitore di servizi di comunicazione elettronica deve fare al Garante in caso di *data breach*; le notificazioni relative al trattamento di dati sensibili; ogni comunicazione, atto, documento o dichiarazione reso nel corso di un procedimento dinanzi al Garante o nel corso di accertamenti. La condotta consisteva, a seconda dei casi, in una falsità dichiarativa o documentale.

[127] L'inosservanza delle disposizioni sulla notificazione al Garante in caso di *data breach* soggiace alle sanzioni previste dall'art. 83, par. 4, GDPR, richiamata dalla clausola contenuta al terzo comma dell'art. 166 del Codice.

dal Garante.

La decisione del legislatore di presidiare penalmente l'esercizio delle funzioni dell'Autorità di settore appare condivisibile, oltre che in linea con le scelte di criminalizzazione compiute in altri rami dell'ordinamento (Art. 170-*bis* D. Lgs. 58/1998; art. 2638 c.c.).

La fattispecie è costruita secondo lo schema dei reati a forma libera; l'evento è descritto facendo leva su elementi più precisi rispetto all'indeterminato concetto di "ostacolo"[128] proprio delle disposizioni da ultimo richiamate. La previsione di un dolo particolarmente intenso supplisce alla scarsa selettività delle modalità di offesa sul piano oggettivo, limitando l'ambito operativo della fattispecie alle sole condotte intenzionali, dotate dunque di maggior disvalore. Ciò nonostante, questa fattispecie di chiusura sembra destinata ad avere un ambito applicativo assai esteso, ricomprendendo anche le mere omissioni informative commesse nell'ambito di un procedimento o nel corso di un accertamento, a prescindere dalla concreta idoneità della condotta a ledere il bene giuridico finale.

6.3. L'omessa adozione di misure di sicurezza.

L'art. 169, rubricato genericamente «Misure di sicurezza», comminava l'arresto fino a due anni per chi *«essendovi tenuto, omette[va,* ndr*] di adottare le misure minime previste dall'articolo 33»*[129]. Si trattava di una fattispecie di reato già prevista dall'art. 36 della legge 675/1996, riproposta dal legislatore del 2003 con significative differenze. Nel testo originario, l'omissione era riferita alle misure previste dalle fonti regolamentari ivi richiamate; con l'emanazione del D. Lgs. 196/2003 le misure minime di sicurezza richiamavano quelle indicate dall'art. 33 del Codice, che a sua volta rinviava alle previsioni del Capo II, e agli artt. 31 e 58, comma 3. Dal combinato disposto

[128] Secondo ALESSANDRI, *Diritto penale e attività economiche*, Bologna, 2010, p. 272, ostacolare significa nella lingua corrente *«rendere più difficile o più arduo, fino al limite dell'impedimento totale [...]: un limite che s'intuisce non è certamente necessario raggiungere per avere la consumazione del fatto di ostacolo».* Invero, sul piano etimologico l'ostacolo è qualcosa che intralcia, un impedimento, una barriera; dunque ostacolare vuol dire intralciare in modo da rallentare, rendere più complesso o impedire il raggiungimento di qualcosa. In argomento anche SEMINARA, *False comunicazioni sociali, falso in prospetto e nella revisione contabile e ostacolo alle funzioni delle autorità di vigilanza*, in *Dir. pen. proc.*, 2002, 692 ss.; CORNACCHIA, Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza, in Giur. comm., 2017, 1, 89.

[129] In dottrina, TORRE, *La gestione del rischio nella disciplina del trattamento dei dati personali*, in Picotti L. (a cura di), *Il diritto penale dell'informatica nell'epoca di internet*, Padova, 2004 p. 237 ss.; MANNA, *Il quadro sanzionatorio penale e amministrativo del codice sul trattamento dei dati personali*, cit. p. 760; CORRIAS LUCENTE, *La nuova normativa penale a tutela dei dati personali,* cit. p. 649.

emergeva che i soggetti titolari e responsabili del trattamento dovessero adottare, per non incorrere nella contravvenzione in commento, le seguenti misure: per i trattamenti con strumenti elettronici, quelle prescritte dall'art. 34; per i trattamenti senza l'ausilio di strumenti elettronici, quelle previste dall'art. 35; per i trattamenti effettuati dai Servizi d'informazione e di sicurezza, quelle individuate con decreto presidenziale.

Rimaneva peraltro fermo il dovere di custodia e controllo dei dati personali in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento *«in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta»* (art. 31). Inoltre, il richiamo integrale alle disposizioni del Capo II portava a includere tra le misure di necessaria adozione anche il disciplinare tecnico di cui all'allegato B), *«relativo alle misure minime di cui al presente capo aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie e il Ministro per la semplificazione normativa, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore»* (art. 36).

La struttura del reato era stata oggetto di critica sotto diversi profili[130]. Si è evidenziato come il rinvio alle norme di disciplina non valesse sempre a identificare in modo puntuale la misura da adottare; alcune di esse erano descritte soltanto attraverso riferimenti funzionali alla natura dei dati trattati, al progresso della tecnica e alla riduzione al minimo del rischio. Infine, l'integrazione del precetto da parte di fonti sublegislative (nelle ipotesi di cui agli art. 36 e 58, comma 3) sollevava dubbi sul rispetto del principio della riserva di legge[131].

Al secondo comma dell'art. 169 si prevedeva che il Garante, nell'ambito della propria attività ispettiva, potesse impartire una prescrizione all'autore della violazione, fissando un termine per la regolarizzazione. In caso di ottemperanza, l'autore del reato era ammesso dal Garante a pagare una somma pari al quarto del massimo della sanzione stabilita per la violazione amministrativa, con la conseguente estinzione del reato[132]. I rinvii recettizi a norme di carattere

---

[130] CORRIAS LUCENTE, *La nuova normativa penale a tutela dei dati personali,* cit. p. 650

[131] Cfr. MANNA, *Il quadro sanzionatorio penale e amministrativo del codice sul trattamento dei dati personali,* cit. p. 762 secondo cui il mero rinvio operato dalla norma in esame alla fonte regolamentare non rispettava i requisiti richiesti dalla giurisprudenza costituzionale, dal momento che il contenuto delle fonti sub-legislative appariva svincolato da ogni tipo di determinazione legislativa a monte.
Contra con riferimento alla fattispecie di cui all'art. 36 della legge 675/1996 VENEZIANI, *Beni giuridici protetti e tecniche di tutela penale nella nuova legge sul trattamento dei dati personali,* cit. p. 175.

[132] La norma prevede una ipotesi speciale di c.d. ingiunzione estintiva, disciplinata in via generale dagli

valutativo o di rango sub-legislativo da lato, e l'individuazione di una procedura amministrativa finalizzata all'estinzione del reato dall'altra, facevano ben propendere per l'inopportunità di continuare a prevedere la sanzione penale per l'omessa adozione di misure di sicurezza[133].
La strada della depenalizzazione è quella percorsa dal legislatore delegato che ha previsto, condivisibilmente, l'abrogazione dell'art. 169. Nel quadro attuale, il presidio sanzionatorio per l'omessa adozione delle misure di sicurezza è affidato, da un lato all'art. 166 pocanzi esaminato, il cui primo comma richiama, per le violazioni commesse dai fornitori di servizi di comunicazione elettronica, l'art. 132-*ter* del decreto il quale, a sua volta, rinvia alle misure di sicurezza di cui all'art. 32 del GDPR; per tutte le altre violazioni il referente sanzionatorio è l'art. 83, par. 4, lett. a) GDPR, che richiama la disciplina dettata dall'art. 32 del medesimo Regolamento sulla sicurezza del trattamento.

6.4. L'inosservanza dei provvedimenti del Garante.

L'art. 170 del Codice punisce con la reclusione da tre mesi a due anni chiunque, essendovi tenuto, *«non osserva il provvedimento adottato dal Garante ai sensi degli articoli 58, paragrafo 2, lettera f) del Regolamento, dell'articolo 2-septies, comma 1, nonché i provvedimenti generali di cui all'articolo 21, comma 1, del decreto legislativo di attuazione dell'articolo 13 della legge 25 ottobre 2017, n. 163»*[134].

---

artt. 20 ss. del D. Lgs. 19 dicembre 1994 n. 758. Allo scopo di eliminare la contravvenzione accertata, l'organo di vigilanza, nell'esercizio delle funzioni di polizia giudiziaria di cui all'art. 55 del codice di procedura penale, impartisce al contravventore un'apposita prescrizione, fissando per la regolarizzazione un termine non eccedente il periodo di tempo tecnicamente necessario (art. 20. Quando risulta l'adempimento alla prescrizione, l'organo di vigilanza ammette il contravventore a pagare in sede amministrativa, nel termine di trenta giorni, una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione commessa (art. 21, comma 2). La contravvenzione si estingue se il contravventore adempie alla prescrizione impartita dall'organo di vigilanza nel termine ivi fissato e provvede al pagamento nei termini previsti. Tale disciplina è stata espressamente richiamata dal legislatore del Testo Unico della sicurezza sul lavoro che, all'art. 301, prevede espressamente che *«alle contravvenzioni in materia di igiene, salute e sicurezza sul lavoro previste dal presente decreto nonché da altre disposizioni aventi forza di legge [...] si applicano le disposizioni in materia di prescrizione ed estinzione del reato di cui agli articoli 20, e seguenti, del decreto legislativo 19 dicembre 1994, n. 758».* Più di recente l'art. 1, comma 9, della legge 22 maggio 2015 n. 68 ha introdotto una parte VI-*bis* nel Testo Unico dell'ambiente (D. Lgs. 03 aprile 2006 n. 152) in cui è contenuta una disciplina specifica sull'estinzione delle contravvenzioni in materia ambientale (artt. 318-*bis* ss.) che presenta fortissime similitudini con quella dettata in generale dal D. Lgs. 758/1994.

[133] MANNA, *Il quadro sanzionatorio penale e amministrativo del codice sul trattamento dei dati personali*, cit. p. 765 richiama i lavori della Commissione Nordio, ricordando come nell'art. 18 del Progetto di depenalizzazione si fosse prevista la depenalizzazione dell'art. 36 della legge 675/1996.

[134] Nella versione precedente alla riforma la disposizione puniva chiunque, essendovi tenuto *«non osser-*

La disposizione incrimina l'inosservanza dei provvedimenti del Garante relativi alle autorizzazioni al trattamento di dati biometrici, genetici, o relativi alla salute; dei provvedimenti con cui l'Autorità impone una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento; delle autorizzazioni generali del Garante per la protezione dei dati personali relative a categorie particolari di dati personali (art. 21 del D. Lgs. 101/2018).
La *ratio* di tutela risiede nella particolare importanza che assumono le decisioni del Garante nei procedimenti di cui si tratta, tali da dover essere presidiate con la sanzione penale. Secondo una opinione dottrinale[135], lo scopo dell'incriminazione non varrebbe a giustificare l'utilizzo da parte del legislatore di un precetto così scarsamente definito, che richiama alla memoria quello di cui all'art. 650 c.p. A tale tesi è stato opposto[136], condivisibilmente, che tutti i provvedimenti presi in considerazione dalla norma sono atti che raggiungono un destinatario determinato, il quale è posto in condizione di conoscerli e rispettarli. Di tal guisa, la similitudine più appropriata è con il reato di cui all'art. 388 c.p. che presidia l'autorità delle decisioni giudiziarie rese in particolari contesti; la previsione della sanzione penale trova quindi giustificazione nella necessità di presidiare la corretta e pronta esecuzione dei provvedimenti del Garante resi in settori particolarmente sensibili.
Nello schema di decreto inizialmente approvato si prevedeva l'abolizione dell'art. 170, scelta rispetto alla quale sia l'Autorità Garante, sia la Commissione Speciale, hanno espresso parere negativo[137]. L'*abolitio* dell'incriminazione era considerata in controtendenza rispetto alle scelte compiute nell'atto di recepimento della direttiva 2016/680/UE sulla protezione dei dati personali delle attività di contrasto e alla previsione, essendosi provveduto in quella sede a introdurre una norma volta a incriminare l'inosservanza dei provvedimenti del Garante[138], del tutto analoga all'attuale art. 170. Qualora la norma fosse stata abrogata si sarebbe determinato il pa-

---

va il provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lettera c)».

[135] MANNA, *Il quadro sanzionatorio penale e amministrativo del codice sul trattamento dei dati personali*, cit. p. 767. In senso contrario si veda VENEZIANI, *Beni giuridici protetti e tecniche di tutela penale nella nuova legge sul trattamento dei dati personali,* cit. p. 175.

[136] CORRIAS LUCENTE, *La nuova normativa penale a tutela dei dati personali,* cit. p. 654

[137] Cfr. *Parere sullo schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679*, cit., § 1.4; *Bollettino delle Giunte e delle Commissioni parlamentari* del 20 giugno 2018, cit., p. 19

[138] L'art. 45 del D. Lgs, 18 maggio 2018 n. 51 commina la pena della reclusione da tre mesi a due anni per chi *«essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi dell'articolo 143, comma 1, lettera c), del Codice, in un procedimento riguardante il trattamento dei dati di cui all'articolo 1, comma 2».*

radosso per cui l'inadempimento del medesimo provvedimento del Garante avrebbe avuto rilevanza penale se imputabile ad organi incaricati di funzioni di accertamento, prevenzione, repressione dei reati; mentre sarebbe andata esente da pena se commesso da qualsiasi altro soggetto[139].
Senza entrare nel merito della questione, ci si limita ad osservare che la relativa condotta sembra trovare un presidio sufficiente nelle sanzioni amministrative comminate dall'art. 83 del Regolamento[140]. Da questo punto di vista, il legislatore delegato avrebbe forse dovuto valutare più attentamente la scelta di reintrodurre l'art. 170 per assecondare i rilievi espressi in sede parlamentare.
Infine, l'intervento riformatore ha ritoccato, senza sostanziali novità, l'art. 171 del Codice della *privacy* che, per le violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori prevede che si applichino le sanzioni di cui all'articolo 38 della legge 20 maggio 1970, n. 300.

7. Le nuove fattispecie introdotte dal D. Lgs. 101/2018.

La mano chirurgica del legislatore della riforma non si è limitata a un intervento meramente ortopedico delle fattispecie previgenti, ma ha innestato due nuove "protesi" nell'apparato sanzionatorio del D. Lgs. 196/2003.
Fuor di metafora, il riferimento è ai nuovi articoli 167-*bis* e 167-*ter,* che puniscono, rispettivamente, la «Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala» e la «Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala»[141].
La prima disposizione punisce con la reclusione da uno a sei anni chiunque, al fine di trarre profitto per sé o altri:
1) *«comunica o diffonde [...] un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2-ter, 2-sexies e 2-octies»* (comma 1);

---

[139] Che comunque ne risponderebbe a titolo di illecito amministrativo ai sensi dell'art. 83, par. 5, lett. e) GDPR. Sul punto l'Autorità Garante, nel citato parere, ha evidenziato una disparità di trattamento poiché *«alla medesima condotta, lesiva dello stesso bene giuridico [...] si applicherebbero due regimi sanzionatori estremamente diversi, solo in ragione della natura soggettiva del titolare e del contesto in cui sia realizzato il trattamento (attività di polizia o giustizia penale, ovvero ogni altro ambito). Elementi, questi, inidonei a giustificare, di per sé soli, tale differente regime sanzionatorio».*
[140] Alla lett. e) del paragrafo 4, si punisce l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.
[141] La rubrica delle norme è stata modificata con l'approvazione del testo definitivo. Nello schema di decreto sottoposto all'esame della Commissione parlamentare i delitti punivano la «Comunicazione e diffusione illecita di dati personali riferibili a un rilevante numero di persone» e la «Acquisizione fraudolenta di dati personali».

2) *«comunica o diffonde [...] senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala [...]»* quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione (comma 2). Le condotte esecutive assumevano (e assumerebbero tuttora) rilevanza penale come illecito trattamento di dati *ex* art. 167, ma presentano elementi specializzanti che denotano una particolare carica offensiva, tale da aver reso necessaria la creazione di una fattispecie autonoma di reato.

Il bene giuridico tutelato dalla disposizione è indubbiamente la riservatezza, intesa come interesse al controllo e alla corretta gestione dei dati personali di un individuo[142].

I casi previsti dal primo comma riguardano il trattamento di dati effettuati per finalità comunque connesse all'esercizio di pubblici poteri, e quelli concernenti il trattamento dei dati giudiziari penali[143]. La disposizione sembra rivolta a reprimere la diffusione abusiva di dati personali raccolti da soggetti che, in virtù dei compiti istituzionali affidati, trattano dati riferibili a un vasto numero di soggetti[144]. Nel testo inizialmente approvato erano individuati quali soggetti attivi, il titolare, il responsabile e l'incaricato del trattamento; con l'approvazione del testo definitivo il legislatore della riforma ha rimodellato la fattispecie configurandola come reato comune[145].

La previsione del secondo comma ha invece portata più ampia e trova applicazione in tutti quei casi in cui la comunicazione o la diffusione sia avvenuta senza il consenso dell'interessato, la cui previa acquisizione rappresenta, com'è noto, il principio generale della disciplina sulla protezione dei dati personali. Anche in questo caso occorre che la condotta abbia ad oggetto un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala. L'obiettivo del legislatore delegato sembra essere quello di punire più severamente quelle condotte di cessione a scopo di lucro di rilevanti quantità di dati personali senza la previa acquisizione del consenso degli interessati. La previsione di una cornice edittale che nel

---

[142] *Supra,* § 2.

[143] Più precisamente è richiamata la violazione delle norme sul trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico, di categorie particolari di dati personali necessario per motivi di interesse pubblico, ovvero dei principi sul trattamento dei dati relativi a condanne penali e reati

[144] Cfr. RESTA*., I reati in materia di protezione dei dati personali,* cit., 1037

[145] Nel citato parere sullo schema di decreto la Commissione parlamentare aveva invitato il Governo a valutare l'opportunità di definire il novero dei soggetti attivi – analogamente a quanto disposto per le altre fattispecie – con il termine «chiunque». Cfr. *Bollettino delle Giunte e delle Commissioni parlamentari* del 20 giugno 2018, cit., p. 19

massimo giunge a sei anni di reclusione consentirà, sul piano processuale, l'impiego di tutti gli strumenti investigativi e coercitivi previsti dal codice di procedura penale[146].

Con l'approvazione del testo definitivo del decreto il legislatore della riforma ha modificato l'oggetto materiale della condotta, sostituendo l'inciso «dati personali riferibili a numero rilevante di persone» con «un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala». Il legislatore ha così inteso evitare che la determinazione del numero rilevante di persone fosse rimessa alla discrezionalità del giudice al caso concreto.

La nuova formulazione presta tuttavia il fianco a diverse critiche.

Il concetto di trattamento "su larga scala" non è meno indefinito del precedente, dal momento che, sebbene sia utilizzato in numerose disposizioni del Regolamento[147], nessuna ne precisa il significato. Inoltre, l'identificazione dell'oggetto materiale della condotta nell'archivio automatizzato sembra incidere in misura significativa sul campo di applicazione della norma, accentuando la componente 'patrimonialistica' di tutela a scapito della riservatezza degli interessati[148]. Il riferimento apre infatti le porte a possibili lacune di tutela nel caso in cui un soggetto, anziché comunicare o diffondere una parte dell'archivio, si limiti a comunicare o diffondere per finalità commerciali le informazioni che riguardano un numero rilevante di interessati senza però avvicinarsi a una soglia tale da configurare una comunicazione o diffusione dell'intero archivio o una parte sostanziale di esso. Né il Regolamento né il Codice della *privacy* definiscono esattamente la nozione di «archivio automatizzato». L'art. 4, par. 1 n. 6 GDPR dispone soltanto che per «archivio» debba intendersi *«qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico»*. L'attributo "automatico" e il participio "automatizzato" compaiono in altre disposizioni come sinonimo di "informatico" o, più in generale, di "elettronico"[149] per di-

[146] La previsione di un massimo edittale superiore, nel massimo, a cinque anni di reclusione consente l'applicazione della custodia cautelare in carcere in caso di pericolo di reiterazione (art. 274, comma 1, lett. c) e la possibilità di utilizzare le intercettazioni (art. 266, comma 1, lett. a).

[147] Si vedano, con riferimento agli obblighi del titolare del trattamento e degli altri soggetti, gli artt. 27, par. 2, 35, par. 3, 37, par. 1 GDPR.

[148] V. *infra*.

[149] In tal senso si veda l'art. 20 che, nel sancire il diritto alla portabilità dei dati, prevede che *«l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano»,* e il successivo art. 22 secondo cui *«l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato [...]».* La locuzione

stinguere il trattamento effettuato con strumenti digitali dal trattamento analogico. Nel formulare la nuova ipotesi di reato il legislatore delegato sembra aver tratto ispirazione dal registro linguistico utilizzato nel Regolamento, anziché affidarsi a un vocabolario già sperimentato in passato[150] che, probabilmente, avrebbe reso più chiaro il significato della disposizione. Ad ogni modo, ci sembra che il criterio della rilevanza – recepito nello schema di decreto trasmesso alle Camere – fosse preferibile, oltre che maggiormente in linea con la tecnica utilizzata in altri settori dell'ordinamento[151].

Le condotte alternative di comunicazione o diffusione si pongono in linea con la tecnica descrittiva utilizzata per alcuni delitti contro la personalità dello Stato[152] e contro la persona[153], o in alcune leggi complementari[154]. La previsione di due distinte condotte, ciascuna idonea ad integrare il reato, si spiega in virtù della differenza semantica che vi è tra la comunicazione e la diffusione: se la prima presuppone che l'agente instauri un rapporto comunicativo con un terzo soggetto determinato (o terzi soggetti), perché si abbia la seconda è sufficiente una *disclosure* dell'informazione che renda possibile a un numero indeterminato di soggetti di venirne a conoscenza.

Non è semplice stabilire se condotte di comunicazione e diffusione, descritte mediante predicati di uso comune, vogliano in realtà operare un tacito rinvio

---

"automatizzato" compare nella stessa accezione anche al *considerandum* n. 15 secondo cui *«al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate. La protezione delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati personali sono contenuti o destinati a essere contenuti in un archivio».*

[150] Avrebbe ad esempio potuto indicare "archivio informatico", locuzione utilizzata in alcune disposizioni del Codice dell'Amministrazione Digitale (Cfr. art. 42 ss. D. Lgs. 82/2005), oppure "banca di dati informatica" (art. 4, comma 1, lett. p D. Lgs. 196/2003 che definiva tale *«qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti»,* oggi abrogato).

[151] Il criterio della rilevanza si rinviene, ad esempio, nelle riformate fattispecie di false comunicazioni sociali (artt. 2621 e 2622 cc.). Era di diverso avviso la Commissione parlamentare che, nel parere sullo schema di decreto aveva sollecita l'attenzione del delegato a sostituire il riferimento al «rilevante numero di persone» con altra formulazione che possa salvaguardare maggiormente la tassatività della disposizione. Cfr. *Bollettino delle Giunte e delle Commissioni parlamentari del 20 giugno 2018*, cit., p. 20

[152] Il riferimento è alle fattispecie di disfattismo politico (art. 265) e di attività antinazionale del cittadino (art. 269).

[153] Cfr. La fattispecie di interferenze illecite nella vita privata (art. 615-*bis*) che al secondo comma punisce le condotte di diffusione e rivelazione delle immagini attinenti alla vita privata; il reato di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater) e quello di diffusione di apparecchiature dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico (art. 615-*quinquies*).

[154] Le condotte di comunicazione o diffusione figurano, ad esempio, tra quelle inserite nella lunga lista dell'art. 171-*ter* della legge 633/1941 sul diritto d'autore, e nei reati di diffusione di notizie riservate (art. 73) e di divulgazione di notizie false sull'ordine pubblico o su altre cose di pubblico interesse (art. 77) del R.D. 20 febbraio 1941, n. 303 (Codici penali militari di pace e di guerra).

alle definizioni contenute all'art. 2-*ter*, comma 4, del D. Lgs. 196/2003. Da una parte potrebbe darsi che il legislatore abbia voluto costruire il precetto utilizzando un elemento normativo della fattispecie, dotato di un significato 'tecnico' ben preciso[155]; dall'altra risulta piuttosto incerta la possibilità di attribuire alle definizioni una valenza generalizzata[156]. Non essendovi indicazioni di segno contrario, deve ritenersi che la fattispecie trovi applicazione tanto nelle ipotesi di trattamento lecito di dati, quanto in quelle di trattamento effettuato in violazione delle norme di disciplina[157].

Quanto al rapporto con altre fattispecie, non sembra potersi escludere il concorso formale con il reato di interferenze illecite nella vita privata (art. 615-*bis*, comma 1), nel caso in cui l'archivio automatizzato di dati personali archiviati, oggetto di comunicazione o diffusione, sia stato "autoprodotto" dal soggetto attivo mediante l'acquisizione di immagini su larga scala, nei luoghi di privata dimora (es. videocamere di sicurezza, riprese effettuati tramite dispositivi satellitari o droni). La clausola di riserva *«salvo che il fatto costituisca più grave reato»* presente nel secondo comma dell'art. 615-*bis* c.p., impedisce invece l'applicazione cumulativa delle fattispecie. Pertanto, se l'agente ha soltanto comunicato o diffuso l'archivio automatizzato (formato legittimamente), risponderà del solo delitto di cui all'art. 167-*bis*.

Va parimenti escluso il concorso con l'illecito trattamento di dati, nel caso in cui il soggetto comunichi o diffonda dati personali già trattati in violazione delle norme di disciplina del D. Lgs. 196/2003. Depone in questo senso non solo la clausola presente in apertura dei primi tre commi dell'art. 167, ma anche il riferimento, rispettivamente nel primo e nel secondo comma dell'art. 167-*bis*, alle violazioni degli artt. 2-*ter*, 2-*sexies* e 2-*octies* e all'assenza del consenso, dai quali si ricava che l'illiceità del trattamento è un presupposto della

---

[155] Per *comunicazione* si intende *«il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione»* (lett. a); per diffusione *«il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione»* (lett. b).

[156] L'art. 2-*ter* disciplina la base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. La collocazione sistematica della definizione lascia dunque supporre che la condotta di comunicazione e diffusione di cui all'art. 167-*bis* possa assumere significato 'normativo' soltanto con riferimento all'illecito trattamento di dati effettuato in violazione dell'art. 2-*ter*, giusto il rinvio ad esso operato dalla disposizione incriminatrice.

[157] Risponderà del reato anche il soggetto che effettui il trattamento in modo illecito (violando ad esempio l'art. 126 sui dati relativi all'ubicazione) e quello che abbia acquisito fraudolentemente l'archivio di dati (v. *infra*).

condotta.
Il successivo art. 167-*ter* punisce con la reclusione da uno a quattro anni, salvo che il fatto costituisca più grave reato, chiunque[158] *«al fine trarne profitto per sé o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala».* Le condotta ivi descritta assumeva rilevanza penale già prima dell'intervento riformatore, potendo, a seconda dei casi, ricadere sotto diversi titoli di reato (es. appropriazione indebita, peculato, truffa)[159].
L'illecito è configurato come reato commissivo a dolo specifico alternativo, posto a tutela della riservatezza dell'individuo, nella accezione testé richiamata, e dell'interesse patrimoniale del legittimo possessore dell'archivio automatizzato. Tra i soggetti passivi del reato, oltre ai singoli interessati, rientra – a nostro avviso – anche chi possieda legittimamente l'archivio automatizzato e tratti i dati in modo conforme alla legge. Depone in tal senso il riferimento all'*archivio automatizzato* di dati che costituisce un bene economicamente apprezzabile che può essere oggetto di indebita appropriazione[160]. Vi è pertanto motivo di credere che si tratti di un reato plurioffensivo, che, oltre alla riservatezza degli interessati, lede anche il patrimonio del legittimo titolare del trattamento.
Anche questa fattispecie presenta il difetto di una eccessiva indeterminatezza nella definizione dell'oggetto materiale della condotta. In sede di approvazione del testo definitivo il legislatore della riforma ha anche qui cancellato la locuzione «dati personali riferibili a numero rilevante di persone» che, per le ragioni pocanzi esposte, si lasciava preferire a quella attuale.

---

[158] La fisionomia della fattispecie come reato comune ha fatto sorgere la necessità di non restringere il novero dei soggetti attivi dell'art. 167-*bis.* La condotta punisce infatti l'acquisizione fraudolenta di dati da parte di chiunque, ma non la loro successiva diffusione; mentre l'art. 167-*bis* nella sua formulazione originaria limitava la punibilità della comunicazione e della diffusione illecita di dati personali al solo responsabile, titolare o incaricato del trattamento. Si veniva così a creare un vuoto di tutela, nel caso in cui un soggetto che non fosse in possesso della qualifica richiesta dalla norma avesse comunicato o diffuso un archivio automatizzato o una parte sostanziale di esso.
[159] Si deve comunque precisare che, adottando il criterio della continuità strutturale nel tipo di illecito proposto da parte minoritaria ma autorevole della dottrina (ROMANO., *Commentario sistematico del codice penale*, I, Milano, 2004, 58 ss.) si dovrebbe concludere per la natura di nuova incriminazione della fattispecie in commento. Risulta infatti evidente come il legislatore abbia individuato una nuova oggettività giuridica meritevole di tutela (l'archivio automatizzato di dati personali, non contemplato in precedenza) e selezionato una specifica modalità di aggressione (l'acquisizione fraudolenta, non ricompresa tra quelle rilevanti *ex* art. 167 *ante* riforma).
[160] Cfr., Cass. Pen., Sez. VI, 09 maggio 2018, n. 33031 secondo cui, in tema di peculato, rientrano nella categoria dei beni mobili suscettibili di appropriazione da parte del pubblico agente anche i beni immateriali, a condizione che gli stessi abbiano un diretto ed intrinseco valore economicamente apprezzabile.

La norma punisce chi *«acquisisce»,* locuzione che, in verità, è piuttosto inusuale nella descrizione della condotta vietata. Dando uno sguardo alle fattispecie del codice penale si può notare come il legislatore sia solito descrivere azioni analoghe mediante l'utilizzo di altri predicati[161]. Soltanto in tempi recenti, con la trasposizione del reato di indebito utilizzo e falsificazione di carte di credito e di pagamento (art. 493-*ter*) il verbo acquisire è stato impiegato con questa funzione nell'impianto del codice[162]. Pur risultando abbastanza evidente la volontà del legislatore di includere nell'alveo del penalmente rilevante qualsiasi attività con cui l'agente riesca a procurarsi la disponibilità di un archivio automatizzato o una parte sostanziale di esso, rimane il dubbio sulla riconducibilità a questa fattispecie dell'ipotesi di "autoproduzione" illecita di un archivio automatizzato di dati personali, allorché l'agente acquisiti senza diritto, in violazione della normativa sul trattamento dei dati e sui diritti degli interessati, un rilevante numero di dati personali, li organizzi in un archivio informatico[163]. Ci si chiede, in buona, sostanza, se l'acquisizione fraudolenta debba riguardare necessariamente un archivio già formato in modo legittimo ad opera di un terzo, ovvero possa includere anche i dati raccolti in modo fraudolento dal reo e poi organizzati in archivio. Interpretando fedelmente il testo della disposizione sembrerebbe doversi concludere nel senso che l'art. 167-*ter* possa essere applicato soltanto nei casi in cui l'archivio di dati sia sottratto (*rectius*, acquisito) in modo fraudolento dal legittimo titolare: depone in questo senso la descrizione dell'oggetto materiale della condotta (riferita direttamente al bene-archivio, e non ai dati personali oggetto di trattamento). Questo esito interpretativo presenta tuttavia il difetto – di certo non superabile per via interpretativa – di lasciare impunita l'autoproduzione fraudolenta di un archivio di dati personali che, stante la nuova e più ristretta formulazione dell'art. 167, non può essere considerata un illecito trattamento di dati[164]. Il

[161] Quali, ad esempio, «si procura» (art. 256, 257, 547 abr., 600-*quater* c.p.), «si appropria» (art. 646, 647 c.p.), «ottiene» (art. 366 c.p.),

[162] L'art. 4, comma 1, lett. a) del D. Lgs. 1 marzo 2018, n. 21 (*Disposizioni di attuazione del principio di delega della riserva di codice nella materia penale*) ha introdotto nel codice penale l'art. 493-*ter* che, al secondo periodo punisce chi *«acquisisce tali carte [di credito o di pagamento] o documenti di provenienza illecita o comunque falsificati o alterati».* La fattispecie di indebito utilizzo e falsificazione di carte di credito o di pagamento è la trasposizione letterale del reato originariamente collocato all'art. 55, comma 9, del D. Lgs. 21 novembre 2007, n. 231.

[163] Si pensi al caso del soggetto che, consegnata l'informativa sul trattamento dei dati personali, riesca a carpire con dolo (formulario redatto in modo confuso, difficilmente intellegibile o incompleto) l'autorizzazione all'utilizzo per finalità commerciali da parte di un grande numero di consumatori.

[164] Se il soggetto acquisisce in modo fraudolento i dati personali degli interessati realizza, tecnicamente, un trattamento senza consenso che ne fa venir meno la liceità (art. 6 GDPR). Si detto in precedenza (v. *supra* § 6.1) che la scomparsa del rinvio alla norma generale sulla liceità del trattamento (art. 23 abr. D.

reato di consuma con la effettiva acquisizione dei dati[165].
L'elemento della fraudolenza è verosimilmente riferito a qualsiasi forma di inganno o espediente idoneo al conseguimento dello scopo, quali artifici, raggiri, simulazioni falsi pretesti e persino le semplici menzogne, purché abbiano una propria idoneità ingannatoria. Non potrebbero pertanto ritenersi sufficienti le mere allegazioni, sia pur non veritiere, di circostanze che siano facilmente verificabili e non possano, perciò, in alcun modo trarre in inganno chi abbia la disponibilità dell'archivio contenente i dati personali. Il mezzo fraudolento può essere riferito sia all'impiego di accorgimenti idonei a eludere la possibilità di percezione del fatto illecito da parte degli interessati (o di soggetti che trattano dati personali), quanto all'utilizzo di artifici o raggiri[166].
Per quel che riguarda, infine, il rapporto con il reato di cui all'art. 167-*bis*, ci si chiede se possa ricorrere una ipotesi di concorso (materiale) di reati nella condotta di chi, dopo aver acquisito in modo fraudolento un archivio o parte di esso, lo diffonda o lo comunichi a terzi al fine di trarre profitto. Se da un lato si potrebbe argomentare nel senso che la seconda condotta sia un *post factum* non punibile, dall'altro va considerato come essa presenti un più alto grado di offensività per la riservatezza degli individui rispetto alla prima (ed è infatti punita più severamente). Diversamente opinando si addiverrebbe alla irragionevole conclusione di mandare esente da pena la diffusione di un archivio fraudolentemente sottratto, condotta che avrebbe invece rilevanza penale nel caso in cui la detenzione dell'archivio fosse *ab origine* lecita; la rigidità della risposta sanzionatoria dipenderebbe, in buona sostanza, dalla precedente attività delittuosa compiuta dal reo, lasciando esposti gli interessati a condotte (impunite) di diffusione e comunicazione dei propri dati personali. Sembra dunque da preferire la soluzione secondo cui, in ipotesi di questo tipo, l'agente debba rispondere di ambedue i reati.
Deve invece essere escluso il concorso (formale) con il reato di appropriazione indebita e con quello di peculato. Nel primo caso troverà applicazione in virtù del principio di specialità il solo art. 167-*ter;* nel secondo caso, in forza della clausola di contenuta in apertura della disposizione in commento, si applicherà il solo delitto contro la pubblica amministrazione, punito con pena

---

Lgs. 196/2003) ha determinato una *abolitio criminis* parziale dell'illecito trattamento di dati effettuato senza il consenso degli interessati (oggi sanzionabile *ex* art. 83, par. 5 lett. a GDPR).
[165] Cfr. FIANDACA, MUSCO, *Diritto Penale – Parte speciale*, Bologna, 2012, 357; ANTOLISEI, *Manuale di diritto penale – Parte speciale*, vol. II, Milano, 2008, 498, a proposito del reato di esenzione fraudolenta dall'obbligo di prestare l'ufficio (art. 366, fattispecie descritta in termini analoghi a quella in commento).
[166] Sull'elemento della fraudolenza a proposito del nuovo art. 617-*septies* c.p. GULLO, *Il delitto di riprese e registrazione fraudolente ex art. 617-septies c.p.,* in Mazza O. (a cura di), *Le nuove intercettazioni*, Torino, 2018, p. 191

più severa sia nel minimo che nel massimo edittale. Non vi è invece luogo a sovrapposizione alcuna con il reato di cui all'art. 171-*bis*, comma 1, della legge 633/1941, poiché l'archivio automatizzato di dati personali oggetto di trattamento su larga non rientra nel concetto di banca di dati rilevante ai fini della legge sul diritto d'autore[167], mancando il requisito della creazione intellettuale da parte del titolare del trattamento.

8. La responsabilità delle persone giuridiche per i delitti in materia di *privacy.*

Il tema della responsabilità dell'ente per i delitti in materia di *privacy* è ormai risalente.

Un primo tentativo volto ad introdurla, in epoca antecedente all'entrata in vigore del D. Lgs. 231/2001, si deve al Progetto Violante[168], presentato alla Camera dei Deputati il 12 gennaio 1993, con il quale, nell'ambito di un più generale quadro di ripartizioni tra sanzioni penali e amministrative, si delineavano alcune sanzioni applicabili direttamente alla persona giuridica per illeciti riguardanti l'omessa nomina del responsabile per la protezione dei dati personali o per la lacunosa notifica della tenuta di una banca di dati. Non mancavano peraltro voci inclini [169]ad attribuire la competenza per l'inflizione di dette sanzioni al giudice penale. Si sarebbe così ottenuto un doppio beneficio: una maggiore efficacia general-preventiva della sanzione, dotata dello stigma penale; un rispetto rigoroso delle garanzie procedurali per l'ente-imputato.

Come è noto la scelta 'minimalista' in sede di introduzione nel nostro ordinamento di una responsabilità diretta dell'ente di chiara matrice punitiva, ha fatto sì che le ipotesi criminose in materia di trattamento dei dati non figurassero tra i reati presupposto.

Successivamente, la legge 18 marzo 2008, n. 48 di ratifica della Convenzione di Budapest (art. 7) ha inserito l'art. 24-*bis*, rubricato *«Delitti informatici e trattamento illecito di dati».* A dispetto però della rubrica, la disposizione non

[167] La legge 633/1941, come modificata dal D. Lgs. 6 maggio 1999, n. 169 di attuazione della direttiva 96/9/CE, definisce la banca di dati come la raccolta «di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo» (art. 2, n. 8) a condizione che «che per la scelta o la disposizione del materiale costituisca «una creazione intellettuale dell'autore» (art. 1, comma 2).

[168] Il richiamo è alla proposta di legge AC- 2097. Lo ricorda MANNA, *La protezione dei dati personali nel diritto italiano,* in *Riv. trim. dir. pen. econ.,* 1993, p.185

[169] MANNA, *La protezione dei dati personali nel diritto italiano*, cit., p. 185;

fa menzione dei reati in tema di *privacy* che, nell'ultima fase dell'*iter* parlamentare, sono scomparsi dal contenuto della disposizione[170].
L'obiettivo dell'estensione della responsabilità della persona giuridica ai delitti in materia di *privacy* sembrava raggiunto con il decreto legge 14 agosto 2013, n. 93, recante *«Disposizioni urgenti in materia di sicurezza e per il contrasto della violenza di genere, nonché in tema di protezione civile e di commissariamento delle province»,* il cui art. 9 aveva modificato l'art. 24-*bis*, richiamando anche i seguenti reati: art. 640-*ter* c.p. (frode informatica); art. 55, comma 9, del d.lgs. 21 novembre 2007, n. 231 (utilizzo indebito e falsificazione di carte di credito); artt. 167, 168 e 170 del D. Lgs. 196/2003 (illecito trattamento di dati, falsità nelle dichiarazioni e notificazioni al Garante, e inosservanza di provvedimenti del Garante). L'auspicabile meta raggiunta dal Governo non ha trovato però coronamento in sede di conversione del decreto; la legge 15 ottobre 2013 n. 119 ha infatti soppresso il secondo comma dell'art. 9 del decreto legge.
La ragione va probabilmente ricercata[171] nel fatto che l'introduzione nel catalogo dei reati-presupposto dei delitti in materia di *privacy* era destinata a comportare importanti riflessi sul piano operativo per le imprese, soprattutto in relazione alla responsabilità amministrativa derivante dall'illecito trattamento dei dati; novità queste troppo rilevanti per poter essere introdotte con decretazione d'urgenza.
Il D. Lgs. 101/2018 di riforma del Codice della *privacy* non ha previsto alcuna disposizione sul punto. Il legislatore delegato ha così perduto l'ennesima occasione per introdurre una tale forma di responsabilità con le positive ricadute in punto di predisposizione ad opera degli enti di modelli organizzativi di prevenzione del rischio-reato in questo settore.

8.1. Principio di autoresponsabilità, obblighi di *compliance* e modello 231: verso un sistema integrato?

Nel delineare il quadro sanzionatorio per le violazioni in materia di *privacy*, il legislatore dell'Unione ha dimostrato però una netta preferenza per forme di

[170] In argomento, SARZANA DI S. IPPOLITO, *La legge di ratifica della Convenzione di Budapest: una "gatta" legislativa frettolosa,* in *Dir. pen. proc.,* 2008, 12, p. 1572 ss; CORASANITI, CORRIAS LUCENTE, *Cybercrime, responsabilità degli enti, prova digitale*, Padova, 2009, p. 156 ss.; BELTRANI S., *Reati informatici e d.lgs. 231/2001 alla luce della legge di attuazione della Convenzione di Budapest,* in *La responsabilità amministrativa delle società e degli enti*, 2008, 4, p. 24 ss.
[171] Sul punto LA MANUZZI, *Diritto penale e trattamento dei dati personali. I reati previsti dal Codice della privacy e la responsabilità amministrativa degli enti alla luce del regolamento 2016/679/UE*, cit., p. 257

responsabilità che si indirizzano verso la persona giuridica. Il nuovo Regolamento prevede numerose disposizioni indicative della volontà di imporre gli obblighi di corretta gestione dei dati direttamente in capo alle società, *rectius* alle imprese. Le sanzioni pecuniarie di cui all'art. 83 GDPR sono state concepite avendo a mente la capacità economica delle grandi imprese; altrimenti non si potrebbe giustificare la previsione di un limite edittale così elevato nel massimo.

Indicazioni univoche si rinvengono anche dalla lettura delle norme di disciplina del Capo IV del GDPR, impositive di obblighi gestionali e organizzativi attuabili soltanto all'interno di enti collettivi. Un esempio è dato dalla figura del responsabile per la protezione dei dati (art. 38), al quale sono attribuiti compiti di vigilanza sul rispetto della legge, consulenza, intermediazione, oltre che di sensibilizzazione e la formazione del personale.

La disciplina dettata dal Regolamento sembra plasmata sul modello dei grandi attori economici. Non a caso la normativa in materia di codici di condotta prevede che questi siano destinati a contribuire alla corretta applicazione del Regolamento *«in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese»* (art. 40, par. 1); quella relativa alla procedura di certificazione, invita a prendere in considerazione *«le esigenze specifiche delle micro, piccole e medie imprese»* (art. 42, par. 1).

Dalla morfologia delle disposizioni sanzionatorie e dalle norme di disciplina sembra potersi quindi ricavare che i destinatari principali degli obblighi imposti dal GDPR siano le imprese di rilevanti dimensioni. Ebbene, la tradizione giuridica statunitense[172] ci insegna che sono proprio queste le imprese rispetto alle quali le strategie di *compliance* dispiegano al massimo la propria efficacia. Tale circostanza è tenuta in primaria considerazione al legislatore dell'Unione, che ispira il nuovo Regolamento al principio c.d. dell'*accountability*, da cui deriva l'obbligo generalizzato per i titolari del trattamento di attuare da sé le misure organizzative idonee alla protezione dei dati personali. Il sistema è congegnato in chiave funzionale seguendo una architettura di tipo flessibile. Il responsabile del trattamento dovrà, per impostazione predefinita, mettere in atto misure tecniche e organizzative adeguate *«tenuto conto [...] dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche»* (artt. 24 e 25); il livello di sicurezza e misure di protezione non è predeterminato *ex ante*, dovendo piuttosto essere *«adeguato*

[172] DI GIOVINE, *Lineamenti sostanziali del nuovo illecito punitivo*, in LATTANZI (a cura di), *Reati e responsabilità degli enti*, 2ªed., Milano, 2010, p. 87

al rischio» (art. 32, par. 1). Il titolare è inoltre tenuto a effettuare una valutazione di impatto sulla protezione dei dati tutte le volte in cui il trattamento *«prevedendo in particolare l'uso di nuove tecnologie [...] può presentare un rischio elevato»*. Il sistema di protezione dei dati personali sembra dunque ruotare attorno al concetto di rischio, per far fronte al quale l'impresa sarà tenuta ad implementare idonee misure di prevenzione[173]. La responsabilizzazione dei titolari del trattamento – l'*accountability* che dir si voglia – sembra rivolta a creare uno schermo contro le violazioni della disciplina di settore.

Osservando il sistema di protezione dei dati personali da questa prospettiva, è possibile cogliere forti similitudini rispetto ai principi posti alla base della responsabilità degli enti *ex* d.lgs. n. 231 del 2001. Come noto, la persona giuridica sarà chiamata a rispondere dell'illecito commesso nel suo interesse o a suo vantaggio qualora non abbia adottato e implementato una serie di misure organizzative volte a contenere il rischio di commissione del reato; per non incorrere in responsabilità sarà tenuta ad elaborare un modello organizzativo idoneo *ex* art. 6 del D. Lgs. 231/2001. In estrema sintesi, l'efficacia esimente riconosciuta all'adozione di misure di prevenzione del rischio è un fattore comune tra i due sistemi in esame[174].

Disponiamo ora degli strumenti per comprendere le reali opportunità che l'estensione della responsabilità dell'ente ai delitti in materia di *privacy* offrirebbe.

Da un punto di vista tecnico-normativo, la struttura delle fattispecie criminose a protezione dei dati personali sembra conciliarsi perfettamente con l'inserimento nel novero dei reati presupposto. La punibilità a titolo di dolo specifico di profitto, che accomuna l'illecito trattamento di dati alle fattispecie previste dagli artt. 167-*bis* e 167-*ter*, si giustifica sulla base dell'evidenza statistica che, nella realtà odierna, il dato personale è un bene prezioso da sfruttare a fini di lucro. Le violazioni in materia di *privacy* assumono spesso la veste di reati tipicamente economici, che, in quanto tali, possono risultare espres-

[173] La violazione degli obblighi di *compliance* è sanzionata dall'art. 83, par. 1, lett. a) GDPR che si riferisce *inter cetera* agli obblighi del titolare e del responsabile del trattamento a norma del Capo IV (artt. 25-39).

[174] DI GIOVINE, *Lineamenti sostanziali del nuovo illecito punitivo,* cit., 91; PALIERO, *La responsabilità degli enti: profili di diritto sostanziale*, in Aa. Vv., *Impresa e giustizia penale: tra passato e futuro,* Milano, 2009, 277 ss. Sulla prevenzione del rischio nell'ambito della sicurezza sul lavoro si vedano ALDROVRANDI, *La responsabilità amministrativa degli enti per i reati in materia di salute e sicurezza sui luoghi di lavoro alla luce del d.lgs. 9 aprile 2008, n. 81*, in *Indice Pen.*, 2009, 495 ss.; AMARELLI., *La responsabilità penale degli enti per gli infortuni sul lavoro*, in De Vita A., Esposito M. (a cura di), *La sicurezza sui luoghi di lavoro*, Napoli, 2009; CASTRONUOVO, *La responsabilità degli enti collettivi per omicidio e lesioni alla luce del d. lgs. n. 81 del 2008,* in Aa. Vv., *La prevenzione dei rischi e la tutela della salute in azienda*, Milano, 2008, 178 ss.

sione di una politica d'impresa.
Last but not least, l'illecito trattamento di dati è costruito intorno alla previa violazione della disciplina di settore, quella stessa disciplina che il responsabile del trattamento è tenuto ad osservare, adottando le misure più idonee (art. 24 GDPR). In altre parole, l'attività di *compliance* per la protezione dei dati è rivolta (anche) a contenere il rischio di reato.
Il complesso delle ragioni che abbiamo illustrato ci porta a concludere nel senso della piena opportunità politico-criminale di inserire i delitti in materia di *privacy* tra i reati presupposto della responsabilità delle persone giuridiche ai sensi del D. Lgs. 231/2001. Si verrebbe in tal modo a creare un sincretismo tra misure tecnico-organizzative funzionali alla legalità nella gestione dell'impresa, secondo quanto già accaduto in materia di prevenzione degli infortuni sul lavoro[175].
Un coordinamento tra i due sistemi – quello di protezione dei dati personali e quello di prevenzione del rischio di reato – è reso possibile dall'esistenza di numerosi punti di contatto. Così, ad esempio, la valutazione d'impatto sulla protezione dei dati potrebbe essere ricompresa nella fase di *risk assessment* prodromica alla costruzione del modello; i codici di condotta di cui all'art. 40 GDPR potrebbero disciplinare anche i requisiti di idoneità del modello ai sensi dell'art. 6, comma 3 del D. Lgs. 231/2001; il responsabile della protezione dei dati potrebbe essere nominato membro dell'Organismo di Vigilanza o comunque suo interlocutore privilegiato.
Dal punto di vista sanzionatorio, l'illecito dell'ente per le violazioni in materia di *privacy* dovrebbe essere punito con misure anche di tipo interdittivo[176] che garantiscano, secondo la logica del *carrot-stick* alla base degli artt. 13 e 17 del D. Lgs. 231/2001, una rapida eliminazione della carenza organizzativa.
Ad ogni modo, l'introduzione della responsabilità da reato dell'ente richiederebbe, a monte, una efficace opera di coordinamento tra i testi legislativi per evitare il pericolo di una duplicazione sanzionatoria. Sarebbe sufficiente, a tal fine, prevedere l'inapplicabilità delle sanzioni amministrative di cui agli artt. 166 del Codice e 83 GDPR per i fatti costituenti reato, affidando al giudice penale il compito di irrogare la sanzione pecuniaria nel processo penale a ca-

[175] Sul tema, GUERRINI, *Le modifiche al D. Lgs. 08 giugno 2001 n. 231*, in GIUNTA, MICHELETTI, *Il nuovo diritto penale della sicurezza nei luoghi di lavoro,* Milano, 2010, p. 132 ss.; PIERGALLINI, *I reati presupposto della responsabilità dell'ente e l'apparato sanzionatorio*, in Lattanzi G. (a cura di), *Reati e responsabilità degli enti*, cit., p. 216; VITARELLI, *Infortuni sul lavoro e responsabilità degli enti: un difficile equilibrio normativo*, in *Riv. it. dir. proc. pen.* 2009, 2, p. 695 ss.
[176] Tenuto conto del rigoroso quadro sanzionatorio delineato dall'art. 83 GDPR non sembra invece opportuno far leva su sanzioni di tipo pecuniario.

rico dell'ente[177].

9. Rilievi conclusivi.

Le norme sul trattamento dei dati personali tutelano la riservatezza dell'individuo da nuove forme di aggressione. Il concetto di riservatezza, interpretato in chiave evolutiva rispetto alle esigenze della moderna società dell'informazione, evidenzia un contenuto più ampio rispetto al mero interesse alla non divulgazione delle informazioni relative alla sfera privata. Il diritto alla corretta gestione dei dati personali e alla consapevole divulgazione degli stessi è oggi la forma di manifestazione più rilevante della riservatezza[178].
L'intervento del diritto penale a presidio delle norme in materia di trattamento dei dati personali appare auspicabile e in linea con la rilevanza costituzionale del bene ad esse sotteso.
L'emanazione del Regolamento 2016/679/UE, e il successivo decreto delegato di adeguamento della disciplina interna, hanno mutato la morfologia del quadro sanzionatorio penale e amministrativo in materia di trattamento dei dati personali.
Sul versante amministrativo, il timore di un uso "terroristico"[179] delle sanzioni amministrative – al fine di incentivare una rapida assimilazione dei principi posti alla base del Regolamento, forzandone così l'ingresso nel tessuto sociale – non appare del tutto destituito di fondamento. Depone in questa direzione, anzitutto, l'afflittività delle sanzioni comminate dal GDPR, indeterminate nel minimo e di applicazione generalizzata, che danno luogo a carico sanzionatorio francamente eccessivo.
Da altro punto di vista, desta perplessità sia la tecnica utilizzata per l'individuazione della violazione, imperniata sul rinvio a intere norme di disciplina dal contenuto variegato, sia la scelta di sottoporre al medesimo trattamento sanzionatorio violazioni espressive di un disvalore decisamente non omogeneo[180].
A tali discrasie non ha posto rimedio il legislatore della riforma. Il nuovo art. 166 del Codice *privacy* anziché dettare criteri più precisi per l'individuazione

[177] Il meccanismo delle 'quote' previsto dal D. Lgs. 231/2001 permetterebbe di adeguare la sanzione pecuniaria alla capacità economica della persona giuridica (sia pur con un massimo edittale di gran lunga inferiore rispetto a quello comminato dagli artt. 83, parr. 4 e 5 GDPR).
[178] V. *Supra*, § 2.
[179] Si richiama la brillante metafora di SEMINARA, *Appunti in tema di sanzioni penali nella legge sulla privacy*, cit., p. 919
[180] V. *Supra,* § 4.

delle violazioni e per la scelta delle sanzioni, complica ulteriormente il quadro. I primi due commi della disposizione individuano una lunga serie di violazioni delle norme di disciplina, che soggiacciono, a seconda dei casi, alle sanzioni di cui ai paragrafi 4 e 5 dell'art. 83 GDPR. Dalla lettura del terzo comma si evince che, per le violazioni non previste dai primi due commi, l'Autorità dovrà irrogare le sanzioni previste dal Regolamento. Ne deriva un sistema sanzionatorio che abbiamo definito "integrato", nel quale alcune violazioni sono individuate dal D. Lgs. 196/2003 e altre, in via residuale, direttamente dal Regolamento. Un sistema complesso e farraginoso, caratterizzato dalla estrema genericità nella individuazione delle violazioni e nella graduazione del trattamento sanzionatorio.

Sul versante penale, emergono anzitutto seri dubbi di legittimità costituzionale dell'intervento riformatore per violazione dell'art. 76 Cost. a causa dell'assenza di principi e criteri di delega che consentissero al legislatore l'articolato intervento di riforma posto in essere[181].

Volendo esprimere un giudizio nel merito della riforma, riteniamo che il legislatore delegato abbia compiuto scelte condivisibili sul piano della politica criminale, sebbene tradotte in fattispecie non proprio brillanti per chiarezza e precisione.

Una nota di merito va riconosciuta alla depenalizzazione dell'omessa adozione di misure di sicurezza (art. 169) e alla revisione della struttura dell'illecito trattamento di dati (art. 167), configurato come reato di evento. La tecnica di redazione delle fattispecie lascia tuttavia aperto il problema della chiarezza e della conoscibilità del precetto, che l'interprete è costretto a ricostruire sciogliendo il reticolo del rinvio alle norme di disciplina. Inoltre, la previsione di un dolo specifico di danno polarizzato su un requisito parzialmente sovrapponibile all'evento del reato ne riduce sensibilmente l'efficacia selettiva, relegandola a ipotesi piuttosto marginali[182]. Desta non poche perplessità la depenalizzazione del trattamento illecito di dati effettuato senza consenso, la cui repressione è stata affidata alle sole disposizioni sanzionatorie del Regolamento. Sarebbe stato più coerente con la scelta di configurare il reato come di evento che anche la violazione dei principi basilari del trattamento potesse assumere rilievo penale laddove produttivo di un nocumento per l'interessato.

L'introduzione dei delitti di «Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala» (art. 167-*bis*) e di «Acquisizione

[181] V. *Supra*, § 5.
[182] V. *Supra*, § 6.1.

fraudolenta di dati personali oggetto di trattamento su larga scala» (art. 167-*ter*) risulta condivisibile ma anche qui si scontano i lamentati problemi in punto di precisione della norma[183].

Non mancano tuttavia note più spiccatamente critiche.

La prima riguarda il rapporto tra sanzioni pecuniarie amministrative previste dal Regolamento e sanzioni penali. Il "coordinamento" effettuato dal nuovo art. 166 non scongiura il rischio di una duplicazione sanzionatoria nel caso in cui la violazione della disciplina sia commessa al fine di conseguire un profitto e arrechi nocumento all'interessato. In questo caso l'autore sarebbe colpito dalle sanzioni "draconiane" di cui agli artt. 166 del Codice e dell'art. 83 GDPR, e dalle pene previste dagli artt. 167 e seguenti. L'ultimo comma dell'art. 167 prevede infatti la sola riduzione di pena *«quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa»*[184], postulando in tal modo l'applicazione congiunta delle due sanzioni[185].

Il ricorso alla pena dovrebbe giustificarsi soltanto in presenza di violazioni gravi, che non siano già adeguatamente presidiate da sanzioni amministrative pecuniarie. Il legislatore delegato non ha tuttavia previsto alcun meccanismo per evitare la duplicazione sanzionatoria per il medesimo fatto. La "via mediana" della circostanza attenuante per effetto del pagamento della sanzione

---

[183] V. *Supra*, § 7.

[184] La riduzione di pena conseguente all'esazione della sanzione pecuniaria amministrativa è applicabile, in forza del richiamo contenuto degli artt. 167-*bis* e 167-*ter*, anche alle fattispecie di comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala e di acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala.

[185] Sul punto, la Commissione parlamentare, nel rendere il parere sullo schema di decreto, aveva espresso un preciso *caveat* di valutare la possibilità di prevedere, compatibilmente con il rispetto dei principi e criteri direttivi della delega, *«il ricorso a sanzioni penali solo in presenza di violazioni gravi e rispetto a fattispecie che non siano già presidiate da sanzioni amministrative comminate ai sensi del Regolamento (UE) 2016/679»*. Cfr. *Bollettino delle Giunte e delle Commissioni parlamentari* di mercoledì 20 giugno 2018, XVIII legislatura. Non è sicuramente agevole individuare l'espediente tecnico più funzionale ad evitare l'applicazione congiunta di sanzione penale e amministrativa. Da un lato, l'introduzione di una clausola di salvaguardia *"salvo che il fatto costituisca reato"* in apertura dei due commi che compongono il nuovo testo dell'art. 166 rimetterebbe all'Autorità amministrativa la cognizione incidentale sull'integrazione del reato, il che non eliminerebbe la possibilità che per il medesimo fatto si apra un procedimento penale; dall'altro, la previsione di una clausola di salvaguardia in apertura degli art. 167 e seguenti non sarebbe possibile dal momento che il precetto è descritto mediante il rinvio alle medesime disposizioni poste a fondamento dell'illecito amministrativo. Rimarrebbe aperta la strada di un sindacato *ex post* del giudice penale sull'opportunità di irrogare la pena per un fatto già gravemente sanzionato in sede amministrativa, scelta che sconterebbe l'evidente difetto di rimettere alla discrezionalità giudiziaria la decisione sulla meritevolezza di pena al caso concreto, con evidente usurpazione delle scelte di incriminazione rimesse al legislatore.

amministrativa – secondo una formula già sperimentata, pur con le dovute differenze, in ambito penale tributario[186] – non pare lo strumento migliore per risolvere il delicato problema dell'applicazione congiunta di sanzioni penali e amministrative per il medesimo fatto. Rimane così aperta la problematica questione della convergenza di sanzioni dotate di particolare afflittività, che solleva non pochi dubbi sul rispetto del divieto di *bis in idem* secondo l'interpretazione fornita dalla Corte di Strasburgo; aspetto su cui – non a caso – il Regolamento aveva richiamato l'attenzione del legislatore interno[187]. Il timore di una duplicazione sanzionatoria non viene di certo meno per effetto della circostanza – contingente e comunque soltanto eventuale – che le due sanzioni siano dirette a destinatari diversi (la persona fisica da una parte, e l'organizzazione complessa dall'altra). Sul punto non può che osservarsi che anche nel caso in cui le conseguenze economiche della sanzione amministrativa fossero sopportate dall'impresa, ciò non varrebbe a escludere l'esposizione patrimoniale diretta della persona fisica autrice del reato (socio amministratore, società di persone, associazioni prive di personalità giuridica) o indiretta (azione di responsabilità nei confronti degli amministratori).
La seconda concerne l'inserimento dei delitti in materia di *privacy* tra i reati presupposto della responsabilità dell'ente, che colpevolmente non ha, per l'ennesima volta, visto la luce. Il coordinamento tra i due sottosistemi normativi, reso possibile dall'esistenza di numerosi punti di contatto, darebbe infatti luogo a un sincretismo di misure tecnico-organizzative funzionali alla legalità nella gestione dell'impresa[188].

[186] Cfr. Art. 13-*bis* D. Lgs. n. 74/2000.
[187] V *Supra,* §§ 1 e 5.
[188] V. *Supra,* § 8.1