LUISS Guido Carli
LIBERA UNIVERSITA' INTERNAZIONALE DEGLI STUDI SOCIALI

Dipartimento di Giurisprudenza

Cattedra di Diritto Penale, Parte Speciale

LA TUTELA PENALE DEL DATO PERSONALE

RELATORE:

Chiar.mo Prof. Antonino Gullo

CANDIDATO: Maria Cristina Misaggi

MATRICOLA: 133363

CORRELATORE:

Chiar.mo Prof. Maurizio Bellacosa

Anno Accademico 2017/2018

LA TUTELA PENALE DEL DATO PERSONALE

CAPITOLO II

IL QUADRO SANZIONATORIO PRECEDENTE LA RIFORMA

CAPITOLO III

LE NOVITA' INTRODOTTE DAL D.LGS. 101/2018 E I PROFILI CRITICI DELLA DISCIPLINA

INTRODUZIONE

La protezione dei dati personali è una tematica che, soprattutto negli ultimi anni, ha assunto una rilevanza centrale nel panorama giuridico italiano, ma prima ancora, europeo.

Se, di certo, è lecito sostenere che la protezione dei dati personali sia funzionale alla protezione della *privacy*, i due concetti non sono sovrapponibili.

«Nella società dell'informazione tendono a prevalere definizioni funzionali della *privacy* che, in diversi modi, fanno riferimento alla possibilità di un soggetto di conoscere, controllare, indirizzare, interrompere il flusso delle informazioni che lo riguardano. La *privacy*, quindi, può essere più precisamente definita, in una prima approssimazione, come il diritto di mantenere il controllo sulle proprie informazioni»[1].

Nell'odierna società dell'informazione, inaugurata dall'avvento del processo di globalizzazione e dominata dall'incessante evoluzione e diffusione dei mezzi tecnologici, il concetto di *privacy*, nonostante sia un concetto molto diffuso, non ha un'uniforme definizione.

La proposta di mantenere inalterato tale vocabolo, senza tentarne una meccanica traduzione, sembra la più corretta, dal momento che gli equivalenti lemmi italiani non ne descrivono che singoli, circoscritti aspetti, che non evocano la complessità di situazioni di riferimento.

L'identificazione del diritto alla *privacy* con il diritto alla protezione dei dati personali[2] è il punto di approdo di una lunga evoluzione concettuale che, nelle sue varie tappe, ha arricchito di implicazioni e significati nuovi e ulteriori un concetto – quello della *privacy* – che si è caratterizzato e si caratterizza ancora oggi per la sua incessante mutevolezza contenutistica e per la sua valenza polisemantica.

La natura poliedrica del concetto risulta ancor più evidente ripercorrendone l'evoluzione storica, dalle origini sino agli ultimi interventi legislativi.

---

[1] RODOTÀ S., *Tecnologie e diritti*, Bologna 1995.

[2] NIGER S., *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006.

Il presente lavoro si propone di analizzare la disciplina relativa alla tutela penale dei dati personali e nel tentativo di soffermarsi sui profili di maggiore criticità, con particolare attenzione al Regolamento europeo 2016/679, il suddetto elaborato si articola in tre capitoli.

Il primo capitolo «La protezione dei dati personali nell'ordinamento italiano» si concentrerà, preliminarmente, sulla genesi e sul fondamento – costituzionale – del diritto alla *privacy*, procedendo poi con l'analisi del rapporto intercorrente tra la *privacy*, *stricto sensu* intesa, e altri beni giuridici, quali l'identità personale e la riservatezza; la prima, non più confinabile in una dimensione statica, ma strettamente connessa al processo evolutivo che ruota attorno al concetto di *privacy*, e la seconda rappresentante, invece, il bene giuridico intorno al quale si costituisce e si articola il c.d. "diritto alla *privacy".*

Successivamente, ed è questo il *fulcrum* del presente capitolo, ci si soffermerà sul diritto alla protezione dei dati personali, che nonostante sia stato considerato diritto fondamentale dell'individuo (articolo 8 della Carta di Nizza), non è stato oggetto di un'elaborazione dottrinaria e giurisprudenziale, ma è stato introdotto *per tabulas* dal legislatore italiano, proprio con l'emanazione del codice *privacy*.

Dopo aver analizzato il fondamentale passaggio dall'*habeas corpus* all'*habeas data*[3] o più specificamente all'«*habeas corpus* in chiave digitale» – riportando un'espressione del Professor Rodotà –, si procederà con lo studio del dato personale, con particolare attenzione alle varie categorie e alle modalità di trattamento lecito.

Il presente capitolo si concluderà con un'attenta analisi del quadro normativo di riferimento, partendo dai pilastri sui quali si fonda la normativa italiana, Convenzione di Strasburgo 108/1981 e Direttiva 95/46/CE, sino ad arrivare all'analisi dell'*iter* legislativo che ha condotto all'emanazione del decreto 101/2018, il quale ha adeguato ed armonizzato la normativa italiana a quella europea del *General Data Protection Regulation*.

[3] RODOTÀ S., *Il mondo nella rete.* Quali i diritti, quali i vincoli, Roma – Bari, 2014

Essendo il presente elaborato dedicato all'approfondimento della tutela penale del dato personale, il secondo capitolo si porrà come obiettivo quello di analizzare il quadro sanzionatorio vigente in Italia fino al Codice *privacy*, D.lgs. 196/2003, con attento approfondimento esegetico di ogni singola fattispecie incriminatrice, posta a tutela della protezione del dato personale.
Ci si soffermerà in particolar modo sull'articolo 167, che punisce il trattamento illecito di dati personali e nello specifico sull'emblematico caso *Google Vividown,* il quale si pone al centro di un dibattito che coinvolge i diritti del mondo digitale.

Il terzo capitolo ha ad oggetto l'attuale disciplina relativa alla protezione penale del dato personale, esaminando le novità introdotte dalla riforma 101/2018, e tutti i profili critici ad essa connessi. Si occuperà di approfondire il quadro sanzionatorio penale, ma prima ancora quello amministrativo, ampiamente definito e disciplinato dal *GDPR*. L'arsenale sanzionatorio penale-amministrativo insieme, ispirato da un meccanismo cumulativo è stato da tempo additato dalla dottrina come difficilmente compatibile con il principio *dell'extrema ratio* che dovrebbe guidare il ricorso al diritto criminale; oltre che poco coerente rispetto ai fondamentali canoni della proporzionalità e ragionevolezza dell'intervento penale, ma soprattutto risulta lesivo del diritto a un equo processo e del principio cristallizzato nel brocardo del "*ne bis in idem*". Il presente capitolo si occuperà infatti di analizzare e ripercorrerne tutte le tappe. Da ultimo si avrà modo di analizzare le fattispecie incriminatrici, tanto quelle rimaste e modificate dal *GDPR*, quale ad esempio l'articolo 167, quanto quelle di nuovo conio, quali l'articolo 167-bis, e 167-ter.
Sarà infine svolta una breve analisi sulla tutela del dato personale e la responsabilità degli enti *ex* decreto legislativo 231/2001.

CAPITOLO I
LA PROTEZIONE DEI DATI PERSONALI NELL'ORDINAMENTO ITALIANO

SOMMARIO**:** *-1. La nascita del diritto alla privacy. -2. Tutela della sfera privata nella costituzione italiana; -2.1. Tutela ex articolo 2 costituzione: interpretato come "clausola aperta"; -2.2. Fondamento di tutela ex articoli 13-14-15 Costituzione; -2.3. Tutela a contrario ex articolo 21 Costituzione ed ulteriori osservazioni. -3. Diritto alla privacy e identità personale. -4. Dal segreto al controllo: la ridefinizione del diritto alla riservatezza. -5. Il diritto alla protezione dei dati personali: habeas data. -6. La nozione di dato personale; -6.1. Categorie particolari di dato personale. -7. Il trattamento dei dati personali nel mondo contemporaneo. -8. Il quadro normativo. -8.1. La legge 300/1970 Statuto dei lavoratori e La legge 121/1981 Nuovo ordinamento dell'amministrazione della pubblica sicurezza; -8.2. La convenzione di Strasburgo 108 e La direttiva madre 95/46; -8.3. La legge 675/96; -8.4. Il codice della privacy d.lgs. 196/2003; -8.5. Dal GDPR fino al d.lgs. 101/2018.*

1. La nascita del diritto alla privacy

Analizzare la genesi della *privacy* significa intraprendere un percorso a ritroso nella storia.

La nozione di *privacy* ha antiche e nobili origini, sin dagli albori l'uomo aveva tra i suoi principali obiettivi quello di proteggersi e tutelarsi, di cercare un ambiente protetto per lui e per quelli che vivevano con lui.

Abraham Maslow,[4] noto psicologo statunitense, ci ricorda con la sua "piramide dei bisogni", che il secondo bisogno, dopo quelli c.d. "fisiologici", è proprio quello della tutela della protezione.

Gli antichi greci ritenevano fondamentale, quasi un dovere per i propri cittadini maschi, la partecipazione alla vita pubblica, essi riconoscevano anche la necessità per ognuno di avere una sfera privata «*oikos*», ma si

[4]MASLOW A., *Motivazione e personalità*, Roma, *2010*, in cui si espone la teoria di una gerarchia dei bisogni umani, la cd "piramide di Maslow".

trattava dell'ambito strettamente limitato all'espletamento dei propri bisogni e delle proprie necessità, vicino alla fondamentale «*bios politikos*[5]».

La *polis* considerava e tutelava come sacri i confini della proprietà ma a fondamento di ciò non vi era il rispetto della proprietà privata, come saremmo portati a credere, bensì il fatto che «senza una casa un uomo non poteva partecipare agli affari della città, perché in essa non aveva un luogo che fosse propriamente suo»[6].

Fondamentale è la visione di uno dei colossi della letteratura greca, il noto drammaturgo Sofocle, che, nella tragedia Antigone[7], espose, per la prima volta, in maniera sorprendentemente attuale, una concezione sociale e giuridica di diritto alla libertà personale in contrapposizione alla volontà dispotica del tiranno Creonte che offende la *Dike*.

Proseguendo nella propria evoluzione, possiamo immaginare che il termine *privacy*, sia divenuto, in età medievale, sinonimo di "familiare".

Con la feudalizzazione, la società finì per essere caratterizzata da una fitta rete di relazioni tra gli individui appartenenti al feudo-monade, che favorì lo sviluppo del "senso di intimità"[8].

Il tramonto della società feudale e la progressiva costruzione dello stato moderno, favorirono lo sviluppo della alfabetizzazione, e con essa la nascita di un concetto di *privacy* in una connotazione a noi più vicina.

In Europa la *privacy* comincia ad assumere il significato moderno di diritto fondamentale della persona già alla fine del 1700.

---

[5] Tali sono definite da ARISTOTELE tutte le attività necessarie e presenti nella sfera politica, *La politica*, Le Monnier, Firenze, 1981.

[6] NIGER S., *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*.

[7] SOFOCLE, *Edipo re – Edipo a Colono – Antigone*, a cura di Dario Del Corno, Oscar Mondadori, 2006. Tali opere, hanno segnato l'apice della tragedia sofoclea. In particolar modo, nell'Antigone viene messo in evidenza il profumo della libertà e la rappresentazione dello scontro tra volontà tirannica e ribellione del giusto; Sofocle racconta la storia di Antigone che decide di dare sepoltura al cadavere del fratello Polinice contro la volontà del tiranno Creonte. Scoperta, viene condannata dal re a vivere il resto dei suoi giorni imprigionata in una grotta, nella quale poi si impicca. Ciò porta, conseguentemente al suicidio del figlio di Creonte (promesso sposo di Antigone) poi della moglie di Creonte, Euridice, lasciando il solo Creonte a maledire la propria stoltezza. Le azioni della protagonista, che nascono nella sua coscienza come diritto naturale si contrappongono alle leggi positive di Creonte che negano la sepoltura del fratello così come la sfera privata dell'O*ikos* comincia a staccarsi dalla sfera pubblica della P*olis* greca.

[8] Chiaramente esposto da MUMFORD L., *La cultura delle città*, Torino, 2007.

Con l'avvento dell'illuminismo, la nascita della *privacy* si presenta non come la realizzazione di un'esigenza naturale di ogni individuo, ma come l'acquisizione di un privilegio da parte di un gruppo.

Basti pensare che «i dati raccolti da Engels a Londra, Edimburgo, Bradford, Leeds, Manchester e in molte altre città inglesi costituiscono un'impressionante testimonianza sulle condizioni abitative della classe operaia inglese; condizioni in cui parlare di *privacy* o frivolezze di questo genere sarebbe stato come offrire le proverbiali *brioches*»[9]. È stato infatti asserito «*poverty and privacy are simply contradictoires*»[10].

Il nucleo centrale del concetto di *privacy*, inteso come "vita privata", fu assunto ad autonoma oggettività giuridica. Nel codice penale francese, una sezione era dedicata agli «*atteintes a la vie privee*»[11] e, nel nostro codice penale italiano, viene introdotto a caratterizzazione di una fattispecie criminosa[12].

«*Every man's home is his castle*», pronuncia Lord Chatam, di fronte al Parlamento inglese «...il più povero degli uomini può, nella sua casetta lanciare una sfida opponendosi a tutte le forze della corona. La casetta può essere fragile, il suo tetto può essere traballante, il vento può soffiare da tutte le parti, la tempesta può entrare e la pioggia può entrare, ma il re d'Inghilterra non può entrare; tutte le sue forze non osano attraversare la soglia di tale casetta in rovina»[13].

Un'efficace metafora che consente di osservare che la *privacy* nell'Europa illuminista e pre-rivoluzionaria, nasce dal diritto soggettivo dell'individuo di opporsi alla forza della Corona. Siamo in un contesto, sociale e istituzionale,

---

[9] MARTINOTTI G. *La difesa della privacy, Politica del diritto*, Bologna, 1971

[10] BENDICH A., P*rivacy, Poverty, and the Constitution, Berkeley*, 1966.

[11] Cfr. Code pénal, Partie législative, Livre II: Des crimes et délits contre les personnes, Titre II: Des atteintes à la personne humaine, Chapitre VI: Des atteintes à la personnalité, Section 1: De l'atteinte à la vie privée.

[12] Si tratta dell'articolo 615 bis c.p. rubricato: "Interferenze illecite nella vita privata" che recita: «Chiunque, mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'articolo 614, è punito con la reclusione da sei mesi a quattro anni. Alla stessa pena soggiace, salvo che il fatto costituisca più grave reato, chi rivela o diffonde mediante qualsiasi mezzo d'informazione al pubblico le notizie o le immagini, ottenute nei modi indicati nella prima parte di questo articolo».

[13] PITT W., The Elder Lord Chattam, discorso del marzo 1763, citato in BROUGHAM H.P. *Historical Sketches of Statesmen Who Flourished in the Time of George III*, Charles Knight e Co., Londra, 1839, voli I. 52.

in cui la *privacy* non era la realizzazione di un diritto naturale di ogni individuo, ma l'acquisizione di un privilegio da parte di un gruppo.

E proprio per la particolare realtà socio-istituzionale anglosassone, si avvertiva l'esigenza di una tutela della sfera privata della persona, nelle sue componenti fisiche e psichiche.

La moderna accezione di *privacy* e l'insieme di diritti che si sono conseguentemente venuti a individuare con riguardo ad essa, appaiono dunque, come il risultato di un complesso percorso di maturazione giuridica che ha trovato terreno fertile in un contesto culturale e giuridico di ispirazione liberale come quello degli ordinamenti di *common law*.

Il diritto alla *privacy* assume metaforicamente il ruolo di un prisma, attraverso cui è possibile ricavare l'immagine stessa della società, che avendone avvertito il bisogno, ne reclama la tutela e successivamente ne forgia le forme[14].

La dottrina, per individuare la data di nascita formale dell'accezione moderna di *privacy* è solita far riferimento a un articolo pubblicato da due studiosi e giuristi statunitensi, Samuel. D. Warren e Louis. D. Brandeis sulla *Harward Law Review*, un saggio dal titolo "*The Right to Privacy*"[15].

L'intento dei due avvocati era quello di offrire protezione, alle esigenze di tutela della sfera privata, che prima di allora, seppur avvertite a livello sociale, faticavano a trovare riconoscimenti giuridico, incappando nelle ostilità di quella parte della dottrina ancora fortemente propensa a ricondurle all'interno delle logiche di diversi diritti, quali il diritto alla reputazione e all'onore. Furono loro a concepire il c.d. "*the right to be let alone"*, moderna formula dello *ius solitudinis*, dello *ius excludendi alios*, concetti essenziali, riconosciuti come diritto fondamentale della cultura statunitense, nonché baluardo della stessa Costituzione americana.

La prima affermazione giurisprudenziale del diritto alla *privacy* da parte della Suprema Corte americana, avvenne nel caso *Katz vs. United States*, nel

[14] BUSIA G., voce *Diritto alla riservatezza*, in *Digesto Disc. Pubbl*., Torino, 2000.

[15] WARREN S. D. E BRANDEIS L. D., *The Right to privacy. The implicit made explicit*, in *Harward Law Review*, 1890. La monografia rappresenta una pietra miliare in materia di privacy, in quanto riconosce per la prima volta l'esistenza di un autonomo diritto alla *privacy*.

1967[16]. La Suprema Corte stabilì il principio della "ragionevole aspettativa di privacy" affermando che una conversazione, per quanto fatta da una cabina telefonica e dunque in un luogo pubblico, merita comunque tutela ai sensi del quarto emendamento.

L'apporto, seppur critico, della suprema corte americana al tema del diritto alla *privacy*, successivamente al caso Katz, costituisce una solida base al mutamento intrinseco del concetto di *privacy*, dalla originale connotazione del *right to be let alone*, alla successiva connotazione positiva, come diritto della persona di esaminare e ispezionare tutte le informazioni che la riguardano e far sì che queste vengano trattate e utilizzate da terzi solo in caso di stratta necessità, in funzione di una corretta utilizzazione degli stessi.

2. Tutela della sfera privata nella Costituzione italiana

Prima di soffermarci sulla ricerca di un fondamento costituzionale del diritto alla *privacy* è opportuno partire dalla protezione e tutela dello stesso, su un versante europeo.

Il più importante riferimento si rinviene all'articolo 8 della Convenzione europea dei diritti dell'uomo, CEDU[17] nel quale il diritto alla vita privata ha trovato la propria consacrazione.

L'articolo 8, rubricato "Diritto al rispetto della vita privata e familiare" stabilisce che: «1.Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza. 2.Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale

[16] Cfr. KATZ V. UNITED STATES, 389 US 347 (1967), è stato un caso emblematico della Corte Suprema degli Stati Uniti in punto di natura del " diritto alla privacy " in un contesto di proprietà intangibile, come quella elettronica di comunicazioni basate su telefono come le chiamate telefoniche.
La sentenza della Corte ha perfezionato le precedenti interpretazioni dell'irragionevole clausola di ricerca e sequestro del Quarto Emendamento per contare un'intrusione immateriale con la tecnologia come ricerca, annullando *Olmstead v. Stati Uniti* e *Goldman v. Stati Uniti*. *Katz ha* anche esteso la protezione del Quarto Emendamento a tutte le aree tramite il "test Katz" per determinare quando una persona ha una "ragionevole aspettativa di privacy".

[17] La Convenzione Europea dei diritti dell'uomo è stata firmata nel 1950 dal Consiglio d'Europa, si tratta di un trattato internazionale volto a tutelare i diritti umani e le libertà fondamentali in Europa. Tutti i 47 paesi che formano il Consiglio d'Europa, sono parte della convenzione, 28 dei quali sono membri dell'Unione europea (UE).

ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, per la pubblica sicurezza, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui».

La disposizione è finalizzata fondamentalmente a difendere l'individuo da ingerenze arbitrarie dei pubblici poteri. In particolare, agli Stati contraenti è posto il divieto di ingerenza, salvo specifiche espresse deroghe. Al riguardo, l'ingerenza può essere prevista dalla legge ovvero motivata da una delle esigenze imperative di carattere generale di cui al secondo comma dell'articolo 8. All'impegno di carattere negativo degli Stati parti si aggiungono gli obblighi positivi di adottare misure atte a garantire il rispetto effettivo della "vita familiare e della vita privata".

Il confine tra obblighi positivi e negativi posti a carico degli Stati contraenti, ai sensi dell'articolo 8, non si presta ad una definizione precisa ma i principi applicabili sono, comunque, assimilabili. Nell'adempiere ad entrambi gli obblighi (positivo e negativo), lo Stato deve trovare un giusto equilibrio tra i concorrenti interessi generali e dei singoli, nell'ambito del margine di apprezzamento che gli è conferito. Inoltre, la procedura decisionale prevista deve essere "equa" e tale da garantire il dovuto rispetto degli interessi tutelati dall'articolo 8[18]. In particolare, deve esistere «un principio di proporzionalità tra la misura (contestata) e lo scopo perseguito»[19].

[18] V. Corte Edu Sentenza del 3 giugno 2014, sez. III, *Lopez Guiò contro Slovacchia*.

[19] V. Corte Edu, Sentenza del 3 ottobre 2014, *Jeunesse contro Paesi Bassi*. La Grande Camera della Corte di Strasburgo, in tema di immigrazione, ha ritenuto sussistente la violazione dell' art. 8, in una fattispecie in cui i Paesi Bassi avevano denegato la concessione del permesso di soggiorno per motivi familiari nonostante l'esistenza di circostanze eccezionali. Quanto al merito del giudizio, relativo alla censura di violazione degli artt. 8 e 14, rispettivamente sul diritto al «rispetto della vita privata e familiare» e sul divieto di discriminazione, la Corte Edu ha individuato una disparità di trattamento nei confronti del ricorrente rispetto ad altri lavoratori cittadini UE, i quali, avendo famiglie altrettanto numerose, possono invece beneficiare, secondo la legislazione italiana, della corresponsione di assegni familiari. Per tale giudizio, i giudici convenzionali ricorrono all'applicazione del principio di proporzionalità, ritenendo che una tale differenza di trattamento tra lavoratori stranieri, fondata essenzialmente soltanto sulla nazionalità del richiedente, debba essere considerata sproporzionata rispetto al fine perseguito di contenere i costi economici delle prestazioni sociali, come invocato dal Governo italiano in giudizio a sostegno della propria decisione.

Ulteriore fondamentale riferimento normativo si rinviene agli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione Europea[20].

L'articolo 7, rubricato «Rispetto della vita privata e della vita familiare» stabilisce che: «Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni»; l'articolo 8, «Protezione dei dati di carattere personale», enuncia: «1.Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2.Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3.Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

I diritti di cui all'articolo 7 corrispondono a quelli garantiti dall'articolo 8 della CEDU. Per tener conto dell'evoluzione tecnica, il termine "comunicazioni" è stato sostituito a "corrispondenza".

Diversamente invece, l'articolo 8 è stato fondato sull'articolo 286 del trattato che istituisce la Comunità europea, sulla direttiva 95/46/CE del Parlamento europeo e del Consiglio relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati, ma anche sull'articolo 8 della CEDU e sulla convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale del 28 gennaio 1981, ratificata da tutti gli Stati membri. Tale articolo è fondamentale nello studio del diritto alla protezione dei dati personali, in quanto consente di prendere atto che il diritto alla protezione dei dati personali sia riconosciuto anche nell'Unione Europea a pieno titolo come diritto fondamentale.

Ancora, fondamentale è menzionare l'articolo 12 della Dichiarazione universale dei diritti dell'uomo[21] e l'articolo 17 della Convenzione

[20] Il testo della Carta è quello solennemente proclamato a Nizza il 7 dicembre 2000 e riproclamato il 12 dicembre 2007, in vista della firma del Trattato di Lisbona, a Strasburgo dal Parlamento europeo, dal Consiglio e dalla Commissione.

[21] La Dichiarazione universale dei Diritti dell'uomo è stata approvata e proclamata dall'Assemblea generale delle Nazioni Unite, a Parigi il 10 dicembre 1948.

internazionale sui diritti civili e politici[22]. Tali articoli stabiliscono, rispettivamente: «1. 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. 2.Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni»; «1. Nessuno può essere sottoposto ad interferenze arbitrarie o illegittime nella sua vita privata, nella sua famiglia, nella sua casa o nella sua corrispondenza, né a illegittime offese al suo onore e alla sua reputazione. 2.Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze od offese».

Si noti come l'articolo 17 del Patto internazionale sui diritti civili e politici riprende integralmente l'articolo 12 della Dichiarazione.

Tali articoli riconoscono il diritto alla *privacy* come diritto a mantenere il controllo sulle proprie informazioni quale presupposto per l'esercizio di molti altri diritti di libertà. L'articolo 12 della Dichiarazione universale menziona luoghi ed ambiti in cui il diritto alla riservatezza deve essere particolarmente garantito: famiglia, casa, corrispondenza.

La protezione del diritto alla *privacy* comporta che ci siano appropriate normative dei singoli stati, le quali dispongano per l'istituzione di appositi organi di garanzia e la messa in opera di adeguate procedure.

Analizzati i principali riferimenti giuridici in ambito europeo, possiamo passare all'analisi della tutela della sfera privata nella Costituzione italiana.

Il riconoscimento del diritto alla *privacy* e lo studio degli strumenti giuridici idonei a garantirlo si deve, in Italia, soprattutto al prezioso intervento della dottrina e della giurisprudenza che si sono occupate di colmare la mancanza di un *corpus* di regole giuridiche che consentisse una definizione univoca di tale diritto.

Vista l'assenza nel nostro ordinamento di una norma generale che definisce il diritto alla *privacy*, uno dei problemi principali, legati a questo concetto, è

[22] La convenzione internazionale sui diritti civili e politici, (meglio nota come Patto internazionale sui diritti civili e politici), è un trattato delle Nazioni Unite nato dall'esperienza della Dichiarazione Universale dei Diritti dell'Uomo, adottato nel 1966 ed entrato in vigore il 23 marzo del 1976.

stato quello di trovare un appiglio normativo dal quale far derivare la tutela generale dell'interesse alla riservatezza.

Ciò, in quanto, è opportuno premettere, la Carta costituzionale italiana non disciplina espressamente il diritto alla tutela della vita privata (in quanto tale); la ragione di ciò risiede, essenzialmente, nel fatto che la *privacy* ha assunto un crescente interesse nell'ambito della scienza giuridica e dell'ordinamento italiano soprattutto a partire dagli anni sessanta, quindi in epoca successiva alla approvazione della nostra Costituzione.

Ciò nonostante, la Costituzione presentando un insieme di disposizioni che formano un sistema diretto a proteggere il singolo nella sua vita privata, risponde adeguatamente alle emergenti esigenze di tutela.

La giurisprudenza eloquente della Corte costituzionale, invero, ha evitato di ricondurre il diritto alla tutela della vita privata ad un parametro costituzionale rigorosamente individuato.

Così, nella sentenza n. 38 del 1973, la definizione «del proprio decoro, del proprio onore, della propria rispettabilità, riservatezza, intimità e reputazione»[23] alla stregua di "diritti inviolabili dell'uomo" è stata collegata, ovviamente, all'articolo 2 della Costituzione, ma si è al contempo riconosciuto che l'affermazione di siffatti valori è contenuta altresì negli articoli 3, secondo comma, e 13, primo comma.

Ancora nella prospettiva di dare un rilievo particolare all'articolo 2 della Costituzione, senza però trascurare gli altri parametri costituzionali che contribuiscono a strutturare l'ordinamento sulla base del principio "personalista", il diritto alla tutela della vita privata è stato indicato come un corollario della dignità della persona.

Al riguardo, può innanzi tutto menzionarsi, a titolo esemplificativo, la sentenza n. 54 del 1986, laddove si evidenzia «l'impossibilità – senza arrecare pregiudizio alla tutela dei diritti fondamentali – di disporre mezzi istruttori che mettano in pericolo la vita o l'incolumità o, che risultino, lesivi della dignità della persona o invasivi dell'intimo della sua psiche»[24].

[23] Così Corte Cost. sentenza n. 38 del 1973 in Giur. Cost., 1973
[24] Così Corte Cost. sentenza n. 54 del 1986 in Giur. Cost., 1986

Nel medesimo senso, la sentenza n. 238 del 1996 ha ribadito che la dignità umana è «comprensiva del diritto alla riservatezza»[25], alla stessa stregua di quanto già rilevato nella sentenza n. 218 del 1994 in ordine al «diritto alla riservatezza sul proprio stato di salute ed al mantenimento della vita lavorativa e di relazione compatibile con tale stato»[26].

In termini ancor più espliciti e con argomentazione più analitica, la Corte si è pronunciata con la sentenza n. 467 del 1991, allorché ha rilevato che, «quando sia ragionevolmente necessaria rispetto al fine della garanzia del nucleo essenziale di uno o più diritti inviolabili dell'uomo, quale, ad esempio, la libertà di manifestazione dei propri convincimenti morali o filosofici (art. 21 della Costituzione) o della propria fede religiosa (art. 19 della Costituzione)», «la sfera intima della coscienza individuale deve esser considerata come il riflesso giuridico più profondo dell'idea universale della dignità della persona umana che circonda quei diritti, riflesso giuridico che, nelle sue determinazioni conformi a quell'idea essenziale, esige una tutela equivalente a quella accordata ai menzionati diritti, vale a dire una tutela proporzionata alla priorità assoluta e al carattere fondante ad essi riconosciuti nella scala dei valori espressa dalla Costituzione italiana»[27].

Gli approdi operati dalla giurisprudenza costituzionale, dimostrano che i profili caratterizzanti la vita privata sono stati essenzialmente due: per un verso, la vita privata è stata collegata alla libertà – costituzionalmente garantita – nello svolgimento della propria personalità; per altro verso, la vita privata è stata declinata come il diritto alla protezione contro le altrui interferenze.

La prima dimensione si riconduce direttamente al combinato disposto degli articoli 2 e 3, secondo comma, della Costituzione, e si configura come la "libertà di" essere se stessi e di formare il proprio essere senza subire indebiti condizionamenti dall'esterno. In maniera più pregnante, però, la tutela della vita privata non è sinonimo soltanto di libertà, ma anche delle estrinsecazioni immediate dello stesso: le manifestazioni dell'individuo che più intimamente

[25] Così Corte Cost. sentenza 238 del 1996
[26] Così Corte Cost. sentenza 218 del 1994
[27] Così Corte Cost. sentenza 467 del 1991

si collegano alla sua personalità ed alla formazione della stessa non possono, infatti, non trovare la più ampia protezione, quanto meno nella misura in cui siffatte estrinsecazioni siano esse stesse funzionali al pieno svolgimento della persona umana.

La seconda dimensione della tutela della vita privata, si costruisce come una classica "libertà da". Certo è che, come si evince chiaramente dallo stesso tessuto costituzionale, la protezione da altrui interferenze non può non conoscere limiti: è in questo senso che l'affermazione del «diritto ad essere lasciati soli» – o, nella più moderna e compiuta formulazione, ad essere «lasciati in pace» – deve essere costantemente oggetto di un bilanciamento con altri valori costituzionali, che ben possono rivelarsi prevalenti, in parallelo con il loro essere latori di esigenze meritevoli di tutela.

Sul punto, la giurisprudenza costituzionale offre una casistica particolarmente ricca, dalla quale si desume tutta una serie di contrapposizioni tra vita privata ed altri interessi, di ordine generale, collettivo, ma anche, talvolta, individuale.

I due profili rappresentati, costituiscono il nucleo tradizionale del diritto alla tutela della vita privata. Tuttavia, nell'ambito del secondo profilo, non si può prescindere dal ricordare un precipuo aspetto, relativo al potere di controllo dell'individuo sulla circolazione delle informazioni che lo riguardino e che, forse, configura l'ambito più delicato, a causa dello sviluppo tecnologico degli ultimi lustri. Non a caso, è proprio sul trattamento dei dati personali che, nell'ultimo decennio, più intensa è stata l'attività legislativa (per lo più collegata all'evoluzione del diritto comunitario in materia).

In ordine alle esigenze di riservatezza in materia di protezione dei dati personali, giova operare un richiamo alla sentenza n. 271 del 2005, con la quale la Corte rileva come «la complessa legislazione statale tende a tutelare per la prima volta in modo organico il trattamento dei dati personali, riferendosi all'intera serie dei fenomeni sociali nei quali questi possono venire in rilievo: da ciò una disciplina che, pur riconoscendo tutele differenziate in relazione ai diversi tipi di dati personali ed alla grande diversità delle situazioni e dei contesti normativi nei quali tali dati vengono

utilizzati, si caratterizza essenzialmente per il riconoscimento di una serie di diritti alle persone fisiche e giuridiche relativamente ai propri dati, diritti di cui sono regolate analiticamente caratteristiche, limiti, modalità di esercizio, garanzie, forme di tutela in sede amministrativa e giurisdizionale»[28]. Ciò rende evidente, secondo la Corte, che «ci si trova dinanzi ad un corpo normativo essenzialmente riferibile, all'interno delle materie legislative di cui all'art. 117 Cost., alla categoria dell'"ordinamento civile", di cui alla lettera l) del secondo comma, in considerazione del fatto che la legislazione sui dati personali non concerne prestazioni, bensì la stessa disciplina di una serie di diritti personali attribuiti ad ogni singolo interessato, consistenti nel potere di controllare le informazioni che lo riguardano e le modalità con cui viene effettuato il loro trattamento. Deve, peraltro, notarsi che, pur nell'ambito di questa esclusiva competenza statale, la legislazione vigente prevede anche un ruolo normativo, per quanto di tipo meramente integrativo, per i soggetti pubblici chiamati a trattare i dati personali, evidentemente per la necessità, almeno in parte ineludibile, che i principi posti dalla legge a tutela dei dati personali siano garantiti nei diversi contesti legislativi ed istituzionali. In questi ambiti possono quindi essere adottati anche leggi o regolamenti regionali, ma solo in quanto e nella misura in cui ciò sia appunto previsto dalla legislazione statale»[29].

2.1. Tutela ex articolo 2 Costituzione: interpretato come "clausola aperta"

Nella nostra Costituzione non vi è alcuna *grundnorm* in tema di tutela della vita privata, per quanto l'articolo 2 della Costituzione[30] rappresenti, senza dubbio, la cornice entro cui inscrivere la gran parte, se non la totalità, delle manifestazioni riconducibili alla vita privata suscettive di tutela costituzionale.

[28] Così Corte Cost. sentenza n. 271 del 2005
[29] Ibidem
[30] L'art. 2 Cost sancisce espressamente che: «La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale».

La disposizione normativa ricordata costituisce l'architrave dell'affermazione del principio c.d. "personalista" (che pone l'individuo al centro dell'ordinamento giuridico), riconoscendo e garantendo i diritti inviolabili dell'uomo, oltre che nella dimensione sociale, anche in quella prettamente individuale (come singolo) e ciò costituisce la base per poter affermare il riconoscimento della vita privata come valore costituzionale protetto[31].

Il fondamento della sicurezza riposa sulla necessità di salvaguardare i diritti fondamentali e nel profondo convincimento che questi ultimi costituiscono la massima espressione del rispetto della persona umana[32].

In via generale, quindi, il diritto alla riservatezza ha seguito una sorte simile ad altri diritti "nuovi" ed ha trovato tutela costituzionale tramite un ancoraggio alla "fattispecie aperta" rappresentata dall'articolo 2.

La Corte di Cassazione, accogliendo un'interpretazione lata dell'articolo 2, ha precisato che «la finalità dell'articolo 2 Cost. è proprio quella di tutelare la persona umana integralmente e in tutti i suoi modi essenziali. Tale norma costituzionale non ha una funzione meramente riassuntiva dei diritti espressamente tutelati nel testo costituzionale od anche di quelli inerenti la persona umana previsti nel codice civile; essa si colloca al centro dell'intero ordinamento costituzionale ed assume come punto di riferimento la persona umana nella complessità ed unitarietà dei suoi valori e bisogni, materiali e spirituali. Appunto perciò, la norma non può avere un compito soltanto riepilogativo; essa costituisce una clausola aperta e generale di tutela del libero e integrale svolgimento della persona umana ed è idonea di conseguenza, ad abbracciare nel suo ambito nuovi interessi emergenti della persona umana purché essenziali della medesima»[33].

Come affermato dalla stessa Corte di Cassazione, «la disciplina degli ambiti di tutela della vita privata del soggetto, pur non trovando espressa menzione

---

[31] BELLOCCI M., MAGNANENSI S., PASSAGLIA P., RISPOLI E., (a cura di), *Tutela della vita privata: realtà e prospettive costituzionali*, Quaderno predisposto in occasione dell'incontro trilaterale delle Corti costituzioni spagnola, portoghese e italiana, Lisbona, 1–4 ottobre 2006.

[32] CALAMANDREI P., *L'avvenire dei diritti di libertà*, Introduzione a Ruffini F., *Diritti di libertà*, Firenze, 1946

[33] Cass., 22 giugno 1985, n.3769, in *Nuova giurisprudenza civile commentata*, 1985.

nelle disposizioni costituzionali, ha il suo primo referente nel complesso dei principi da questa ricavabili; il diritto alla riservatezza, quale diritto della personalità, consente di individuare il correlativo fondamento giuridico ancorandolo direttamente all'art 2 Cost., norma di carattere precettivo e non programmatico»[34].

La possibilità di fondare il rango costituzionale della riservatezza sull'articolo 2 è stata, però, in vario modo anche avversata.

Il problema generale all'interno del quale si può a grandi linee circoscrivere l'intero dibattito è quello che ruota intorno alla natura e funzione dell'articolo 2. La spaccatura dottrinale si concentra sull'interrogativo se esso vada considerato come una sorta di clausola generale aperta[35] , tale da permettere di non considerare l'elenco dei diritti di libertà costituzionalmente tutelati come un numero chiuso, oppure come una norma che riassume in sé le caratteristiche comuni alle libertà stesse, che però nella Costituzione risulterebbero tassativamente indicate. Se si accogliesse quest'ultima interpretazione, cadrebbe, tuttavia, la possibilità di ampliare in via interpretativa tale elenco, dal quale resterebbe pertanto esclusa in radice la riservatezza stessa.

Per contro, l'art. 2 come norma aperta ha il sicuro pregio di conferire un certo grado di elasticità al testo costituzionale che, al pari della generalità delle norme scritte, soffre inevitabilmente dello scarto temporale che corre tra la sua entrata in vigore e i mutamenti storico-sociali sopravvenuti.

D'altro canto, si sente l'esigenza, di matrice garantista, di non permettere che la norma in esame possa fungere da varco incontrollato per l'ingresso nel sistema costituzionale di interessi e situazioni non contemplati in esso *ab origine*, con tutte le conseguenze che tale operazione porta con sé.

All'interno di questo scenario d'insieme si muovono le diverse opinioni sulla costituzionalizzazione del diritto alla riservatezza operato per il tramite dell'articolo 2.

---

[34] Cfr. Cass., sentenza n. 5658 del 1998

[35] Per la decisa affermazione di questa posizione e sul contenuto immediatamente precettivo dell'art. 2 v., tra gli altri, ZATTI P., *Il diritto alla identità e l'"applicazione diretta" dell'art. 2 Cost.*, in AAVV, *Il diritto alla identità personale*, a cura di ALPA G. e BESSONE M., Padova, 1981, pp. 55 ss.

La sua natura di clausola generale è stata criticata da diversi punti di vista, ad esempio invocando una sentenza della Corte costituzionale, la n. 98 del 1979, dove in tre righe è stato detto che «l'elenco dei diritti di libertà contenuto nella Costituzione non può essere ampliato in via di interpretazione»[36].

Da parte di altri ci si è riferiti all'argomento testuale, indagando il significato e la storia dell'espressione "diritti inviolabili" contenuta nell'articolo 2. In tale prospettiva si afferma che la scelta della parola "inviolabili" in luogo di "naturali", pur prospettata in seno alla Costituente, testimonia il rifiuto di impostazioni di tipo giusnaturalistico da cui deriverebbe la preclusione ad accordare tutela costituzionale a diritti che in essa non ricevono esplicita menzione e riconoscimento.

Su un piano diverso si svolge la critica di autorevole dottrina[37], la quale tende a concentrare l'attenzione sull'attributo dell'inviolabilità che l'articolo 2 conferisce ai diritti cui è indirizzato, qualità che «implica il riferimento a diritti che siano, per così dire, situati alla sommità della scala gerarchica dei valori costituzionali»[38].

L'attributo dell'inviolabilità sancisce l'appartenenza dei diritti che di tale carattere partecipano all'essenza stessa della Costituzione, «un nucleo che si ritiene sia in ogni caso intangibile ed immodificabile: immodificabile cioè anche di fronte allo stesso potere di revisione costituzionale»[39], con riferimento all'essenza dei diritti stessi. Facendo così attenzione soprattutto alle conseguenze dell'inclusione del diritto alla riservatezza nell'ordine costituzionale, l'autore lo condiziona all'accertamento positivo sull'inviolabilità, concludendo che la riservatezza sembra non possedere tale attributo.

---

[36] PIZZORUSSO A., *I profili costituzionali di un nuovo diritto della persona*, in AAVV, *Il diritto alla identità personale*, cit., p. 30. Ad ogni modo, l'autore stesso tempera l'importanza del riferimento giurisprudenziale: «Poiché tuttavia mi sembra che la Corte costituzionale non possa cancellare con tre righe di motivazione un'elaborazione dottrinale e giurisprudenziale ormai cospicua, penso che a questo precedente non si possa dare gran peso».

[37] FOIS S., *Questioni sul fondamento costituzionale del diritto alla «identità personale»*, in AAVV, *L'informazione e i diritti della persona*, Jovene, Napoli, 1983, pp. 159 ss.

[38] *Ibidem*, p. 161

[39] *Ibidem*, p. 161

Il sicuro sostegno alla tesi positiva sulla utilizzabilità dell'articolo 2 si può trovare allontanandosi dalle concezioni troppo formalistiche o da quelle che concentrano l'analisi sul momento degli effetti, piuttosto che sul nucleo effettivo del problema.

In ogni caso, al di là di seppur illustri referenti giurisprudenziali, sembra opportuno evidenziare il carattere fondamentalmente "personalistico" della Costituzione italiana[40] che si risolve in una maggiore considerazione e dignità dei diritti della personalità umana, rispetto ad altri interessi che pur ricevono tutela costituzionale.

Partendo da questa impostazione di fondo sui valori di base cui la Costituzione è intimamente informata, si apre la prospettiva di una valutazione del ruolo dell'articolo 2 da un punto di vista sostanziale, teleologico e non astratto dal divenire storico-sociale, mantenendo in subordine i criteri formalistici e di rigida analisi testuale.

In questo contesto «l'art. 2 avrebbe quindi il compito di garantire costituzionalmente tutti quegli aspetti che, in un determinato momento storico, in base ad un'interpretazione evolutiva della Costituzione, il diritto inviolabile può assumere, in vista di una sua completa tutela. In tal modo si realizza il fine dell'ordinamento, di proteggere in maniera efficace la persona umana»[41].

La natura di "norma aperta" dell'articolo 2 risponde alla precisa e fondamentale funzione di conferire al testo costituzionale quel necessario grado di elasticità che permette l'adeguamento del diritto alle modificazioni sociali e culturali cui il consorzio umano fatalmente è soggetto e quindi di garantire dignità e rango costituzionale, in una prospettiva realistica della cosiddetta "costituzione vivente", ad interessi che il contesto sociale ha reso meritevoli non di una tutela semplice, ma di una tutela rafforzata tanto da

[40] Cfr. MANTOVANI F., *Diritto alla riservatezza e libertà di manifestazione del pensiero con riguardo alla pubblicità dei fatti criminosi*, in AAVV, *Il diritto alla riservatezza e la sua tutela penale*, Atti del terzo simposio di studi di diritto e procedura penali, Varenna, Villa Monastero, 5-7 settembre 1967 promosso dalla Fondazione "Avv. Angelo Luzzani" di Como - Milano, 1970, p. 391 ss., in cui è presente anche un'analisi delle diverse correnti di pensiero in seno alla Costituente e della loro influenza sui valori di fondo recepiti nel testo costituzionale.

[41] AULETTA T. A., *Riservatezza e tutela della personalità*, Milano, 1978, pp. 42-43.

limitare in questo modo lo stesso potere del legislatore ordinario (salva sempre la facoltà di servirsi dell'*iter legis* aggravato *ex* art. 138 Cost.), anche se prima tale protezione non si prospettava come necessaria.

Chiaramente trattasi di interessi non completamente nuovi o estranei al tessuto costituzionale (giacché altrimenti sarebbe necessario innescare i suddetti rituali meccanismi di revisione costituzionale con lo scopo opposto di introdurre piuttosto che espungere), ma che invece trovano precisi addentellati in principi frutto di sussunzione e astrazione e costituiscono dunque il risultato finale di un processo di specificazione e articolazione pienamente legittimo e necessario.

Ecco che, in base a tali considerazioni, il riconoscimento costituzionale della riservatezza perde quel sospetto di forzatura del testo costituzionale nel momento stesso in cui soddisfa il fine superiore di apprestare effettiva tutela alla persona umana e alle sue esigenze fondamentali.

Tra queste ultime la dottrina più sensibile e attenta pone a pieno titolo quella del riserbo, che «costituisce una necessità addirittura biologica dell'uomo, è aspetto inalienabile della persona umana»[42].

La riservatezza inoltre, pur rivestendo rilevanza autonoma, svolge un non meno basilare ruolo strumentale: la garanzia di una sfera sottratta alle intrusioni di terzi e la sicurezza che determinate informazioni resteranno private rappresentano la condizione «per assicurare alla persona il pieno godimento dei diritti fondamentali sanciti dalla Costituzione»[43] e cioè: la dignità, il pieno e libero sviluppo della persona e l'effettivo esercizio di altre libertà fondamentali, quali, esemplificando, la libertà (negativa) di manifestazione del pensiero, l'inviolabilità di domicilio e corrispondenza[44].

---

[42] CATAUDELLA A., *Scritti giuridici*, Padova, 1991, p. 545.

[43] BELVEDERE A., *Riservatezza e strumenti d'informazione,* in *Dizionario del dir. priv.*, Milano, 1980, p. 750. L'autore si dice contrario, tuttavia, ad una rilevanza costituzionale di tipo autonomo del diritto alla riservatezza, esaltandone solo il citato ruolo strumentale.

[44] MANTOVANI F., *Op. cit*., pp. 399 – 400. Il profilo strumentale del diritto alla riservatezza trova un completo riconoscimento nella sentenza della Corte Costituzionale tedesca, *Op. cit.*, p. 422: nel passo citato la Corte sviluppa il concetto di autodeterminazione individuale quale presupposto per l'esercizio delle libertà democratiche. Esso risulta gravemente inibito dalla non conoscenza della sorte delle informazioni personali cedute dagli individui. Chi ignora cosa verrà raccolto e da chi non sa quali comportamenti può legittimamente tenere e, temendo che alcuni fatti siano schedati, rinuncia ad esempio a partecipare ad assemblee, manifestazioni, riunioni sindacali, cioè all'esercizio di diritti costituzionali. Ciò avrebbe conseguenze non solo sul suo sviluppo personale, ma anche su quello

2.2. Fondamento di tutela ex articoli 3, 13, 14, 15 Costituzione

A rafforzare ulteriormente la tutela della *privacy* nella Costituzione, sono invocate altre disposizioni, che hanno riguardo ad aspetti specifici della vita privata dell'individuo.

È opportuno menzionare, in quanto consente un approccio generale al tema della rilevanza costituzionale della riservatezza, l'articolo 3[45].

Tale disposizione è stata analizzata sia in riferimento al I comma, laddove si parla di «pari dignità sociale», sia al II comma, il quale contiene la garanzia del «pieno sviluppo della persona umana».

Le posizioni critiche circa il possibile uso di tali formule come indici di tutela costituzionale della vita privata, che invero sembrano prevalere sulle opinioni positive, si fondano su molteplici argomentazioni.

Alcune di queste sono di carattere formale e indagano la natura e la funzione dell'articolo 3 nel generale contesto costituzionale: si afferma che sarebbe erroneo ritenere che il principio di eguaglianza possa, in assenza di una specifica *relatio* ad altre norme costituzionali, valere a fondare diritti soggettivi: tale principio, invece, è produttivo solo di "effetti riflessi" sul contenuto dei singoli diritti, ma solo se ed in quanto essi risultino già specificamente riconosciuti.

---

collettivo, poiché l'autodeterminazione è una condizione elementare che si basa sulla possibilità di agire e coagire dei cittadini e quindi sulla democrazia. Il libero sviluppo della personalità presuppone la protezione del singolo dalla memorizzazione, utilizzazione e trasferimento incontrollato di dati personali.

[45] Cfr. BRICOLA F., *Prospettive e limiti della tutela penale della riservatezza,* in AAVV, *Il diritto alla riservatezza e la sua tutela penale*, Atti del terzo simposio di studi di diritto e procedura penali, Varenna, Villa Monastero, 5 – 7 settembre 1967/ promosso dalla Fondazione "Avv. Angelo Luzzani" di Como – Milano , 1970, p. 84, il quale evidenzia il parallelismo tra l'art. 3 Cost. e gli artt. 1 e 2 della Costituzione tedesca che impiegano formule analoghe a tutela della dignità e dello sviluppo della personalità. Sono queste le disposizioni in cui "la dottrina tedesca ravvisa l'affermazione costituzionale del diritto alla vita privata".

L'articolo 3 stabilisce che: «Tutti i cittadini hanno pari dignità sociale e sono eguali davanti alla legge, senza distinzione di sesso, di razza, di lingua, di religione, di opinioni politiche, di condizioni personali e sociali. È compito della Repubblica rimuovere gli ostacoli di ordine economico e sociale, che, limitando di fatto la libertà e l'eguaglianza dei cittadini, impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese».

La disposizione in esame non potrebbe quindi essere invocata per attribuire cittadinanza costituzionale al diritto alla riservatezza, essendo la sua operatività relegata ad un ambito per così dire di secondo grado, una volta risolta positivamente, ma per altra via, la questione dell'esistenza costituzionale del diritto in oggetto.

Le altre critiche, varie ed eterogenee, sono di tipo sostanziale.

Da parte di alcuni si lamenta l'eccessiva genericità della disposizione[46]. Altri si interrogano sulla reale natura di ostacolo allo sviluppo della persona rappresentato dalla conoscenza di notizie private e dall'«attacco alla sfera privata da parte soprattutto dei grandi mezzi di comunicazione di massa»[47].

Altri ancora fanno appello alla marcata dimensione sociale cui l'articolo 3 sarebbe ispirato: gli interessi da esso tutelati, dignità e sviluppo della persona, andrebbero visti in un'ottica eminentemente sociale, che non può non contrapporsi alla dimensione individuale in cui si esplicano la vita privata e la riservatezza[48].

L'esattezza di tali affermazioni deve tuttavia essere ridiscussa alla luce delle mutate caratteristiche del problema in relazione all'avvento della c.d. "società dei *computers*" e, nello specifico, alle conseguenti modificazioni a cui il concetto di *privacy* è andato incontro[49], per cui non è più possibile, né

---

[46] Ad esempio, FOIS S., *Questioni sul fondamento costituzionale del diritto all'«identità personale»,* in AAVV, *L'informazione e i diritti della persona*, Jovene, Napoli, 1983, p. 167. L'autore si dimostra contrario all'utilizzazione delle clausole generali dell'art. 3: "il richiamo al valore della persona umana rischia di diventare l'invocazione ad una specie di formula magica per dar forma a fantasmi normativi tali da implicare le conclusioni più diverse e più opposte".

[47] BRICOLA F., *Op. cit*., p. 84. In particolare, secondo l'autore, «non è provata la correlazione fra violazioni della sfera privata e impedimento al pieno sviluppo della persona umana», ed anzi giunge ad affermare che «una migliore conoscenza della vita privata può giovare ad un migliore inserimento sociale dell'individuo». Da parte di altri, v., per tutti, T. A. Auletta, *Op. cit.*, pp. 2 ss., è stato giustamente evidenziato come gli individui spesso coltivino l'interesse opposto a mantenere divisi i diversi ambienti in cui, per piacere o necessità, si trovano a vivere le proprie esperienze, con un minimo di continuità. Capita facilmente che il soggetto dia di sé una rappresentazione diversa a seconda del contesto in cui si trova, avendo cura che gli ambienti tra loro eterogenei e separati (ad esempio luogo di lavoro e cerchia di amici) non abbiano a partecipare di tali diverse rappresentazioni.

[48] MANTOVANI F., *Op. cit*., pp. 388 ss. L'autore riferisce tale opinione per poi criticarla sotto il profilo della contrapposizione troppo decisa tra *civis* e singolo, evidenziando invece l'opportunità di riferirsi alla persona umana integralmente intesa. Nello stesso senso v. R. Tommasini, *L'interesse alla riservatezza ed i valori della persona di fronte alla libertà di manifestare il pensiero,* in AAVV, *L'informazione e i diritti della persona*, cit., p. 40.

[49] Cfr., per tale tema, RODOTÀ S., *Tecnologie e diritti*, Bologna, 1995, pp. 29 ss.

opportuna, una precisa separazione tra individualità e collettività, se non si vuole incorrere in una falsa e incompleta rappresentazione del problema.

Infine, il riferimento alla dignità sociale contenuto nel I comma dell'art. 3 è giudicato improprio da parte di chi evidenzia come il concetto di dignità miri a tutelare in via diretta interessi diversi dalla riservatezza, che sono identificabili nel decoro e nella reputazione della persona [50].

La dottrina favorevole all'utilizzo dell'articolo 3 come suggello costituzionale del diritto alla riservatezza ha accentuato la necessità della garanzia di una sfera privata inviolabile affinché la dignità[51], ma soprattutto lo sviluppo della persona, siano effettivamente assicurati e non restino invece pura affermazione di principio o addirittura lettera morta. In realtà, su tutti gli spunti critici appena esposti, sembrano prevalere le impostazioni che reclamano la diretta operatività dell'articolo 3 quale garanzia del libero sviluppo della persona.

A sostegno di questa impostazione si vedano le considerazioni esposte nella famosa sentenza della Corte Costituzionale tedesca[52] relative al diritto all'autodeterminazione individuale (*Individuelle Selbstbestimmung*) e informativa (*Informationelle Selbstbestimmung*) quali presupposti per l'esercizio effettivo di libertà democratiche, anche di natura collettiva (salvaguardando la dimensione sociale dell'articolo 3) e quindi direttamente funzionali proprio al pieno sviluppo della persona umana.

Anche queste norme, che sanciscono l'inviolabilità della libertà personale, del domicilio, della libertà e segretezza della corrispondenza e ogni altra forma di comunicazione, sono state esaminate al fine di attribuire rango costituzionale al diritto alla riservatezza. In questa prospettiva la libertà personale viene intesa non tanto e non solo in senso fisico, ma con riguardo

[50] In tal senso v. CATAUDELLA A., *Op. cit.*, p. 546.

[51] Anche l'elemento della dignità, spesso passato in secondo piano dalla dottrina, offre importati appigli al tema della rilevanza costituzionale della riservatezza. Il punto più spinoso è quello di fornire un concetto di dignità umana che si armonizzi con le esigenze definitorie e di rigore concettuale proprie del diritto. Per un inquadramento giuridico del valore della dignità umana v. VALENTI A. M., *La dignità umana quale diritto inviolabile dell'uomo*, Perugia, 1995, pp. 9 ss.

[52] Cfr. Bundesverfassungsgericht 24-01-2012, 1 BvR 1299/05

alla persona nella sua interezza, ivi compresa la sua sfera spirituale e la sua personalità.

Viene in rilievo, quindi, l'articolo 13[53], che nell'affermare l'inviolabilità della libertà personale garantisce il singolo da ogni indebita ingerenza nella sua sfera fisica e psichica.

Ma anche l'articolo 14[54], che sancisce l'inviolabilità del domicilio ed attribuisce rango costituzionale al principio secondo cui «*my home is my castle*», proteggendo così una delle sedi – anzi, la sede per eccellenza – in cui la vita privata si svolge.

Parimenti, nell'ottica relazionale, di particolare importanza è l'articolo 15[55], ai termini del quale «la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili»: la disposizione garantisce l'individuo da ogni intromissione che non trovi giustificazione in esigenze di ordine generale, debitamente vagliate dall'autorità giudiziaria.

La corrispondenza è interpretata come proiezione spirituale dell'individuo[56].

[53] Articolo 13 Cost: «La libertà personale è inviolabile. Non è ammessa forma alcuna di detenzione, di ispezione o perquisizione personale, né qualsiasi altra restrizione della libertà personale, se non per atto motivato dell'autorità giudiziaria nei soli casi e modi previsti dalla legge. In casi eccezionali di necessità ed urgenza, indicati tassativamente dalla legge l'autorità di pubblica sicurezza può adottare provvedimenti provvisori, che devono essere comunicati entro quarantotto ore all'autorità giudiziaria e, se questa non li convalida nelle successive quarantotto ore, si intendono revocati e restano privi di ogni effetto. E` punita ogni violenza fisica e morale sulle persone comunque sottoposte a restrizioni di libertà. La legge stabilisce i limiti massimi della carcerazione preventiva».

[54] Articolo 14 Cost: «Il domicilio è inviolabile. Non vi si possono eseguire ispezioni o perquisizioni o sequestri, se non nei casi e modi stabiliti dalla legge secondo le garanzie prescritte per la tutela della libertà personale. Gli accertamenti e le ispezioni per motivi di sanità e di incolumità pubblica o a fini economici e fiscali sono regolati da leggi speciali».

[55] Articolo 15 Cost: «La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge».

[56] MORSILLO G., *La tutela penale del diritto alla riservatezza*, Milano, 1966, p. 274.

Invero, la posizione dominante in dottrina afferma che le disposizioni in esame si riferiscono in primis a diritti distinti dalla riservatezza[57], o ad aspetti settoriali e manifestazioni parziali di essa[58], o ancora a diritti qualificati "affini", con particolare riferimento al diritto al segreto[59].

L'atteggiamento piuttosto diffuso che sembra emergere dalle posizioni esaminate è di pressoché generalizzato sfavore verso l'utilizzo delle tre norme in esame come esclusiva ancora costituzionale del diritto alla riservatezza, forse per il timore di indulgere ad operazioni ermeneutiche non sufficientemente supportate da adeguati indicatori di diritto positivo[60].

---

[57] Tra le rare voci contrarie cfr.: SANDULLI A. M.- BALDASSARRE A. *Profili costituzionali della statistica in Italia*, in *Dir. soc*., 1973, pp. 382-383, nota 87: « a livello costituzionale, tale diritto è riconosciuto e garantito dagli artt. 13 (che, occorre ripeterlo, si riferisce pure alla libertà personale morale, ossia anche ai beni immateriali inerenti o attinenti alla persona fisica), 14, 15 Cost.» . Inoltre anche la giurisprudenza di merito, oltre a quella costituzionale già citata, ha, in alcune sentenze, posto a rapporto diretto corrispondenza epistolare e riservatezza. Si vedano, in questa prospettiva, le seguenti sentenze: Pretura di Verona 30 ottobre 1990 (in *Giur. merito*, 1992, p. 852); Tribunale di Milano 30 giugno 1994 (in *Foro it.*, 1995, I, p. 1667) e 15 settembre 1994 (in *Dir. Informatica*, 1995, p. 626, nota (Ricciuto). Nelle suddette decisioni si trova ribadito, indipendentemente dal caso di specie, il diritto alla riservatezza epistolare. In particolare la seconda sentenza lo definisce come la legittima aspettativa che l'autore ripone nel destinatario circa il mantenimento del più rigoroso riserbo in merito al contenuto della corrispondenza. Anche la Corte di Giustizia delle Comunità europee (sentenza del 18 maggio 1982, in *Riv. dir. internaz.*, 1983, p. 893) ha ravvisato l'esistenza, tanto nell'ordinamento comunitario, quanto in quelli degli Stati membri, di norme a tutela della riservatezza della corrispondenza (nella fattispecie tra avvocato e cliente).

[58] BRICOLA F., *Op. cit.*, pp. 80-81; MANTOVANI F. *Op. cit.*, pp. 387-388; BELVEDERE A. *Op. cit.*, p. 750: la Costituzione presenta «varie disposizioni che regolano aspetti parziali del problema (talora insieme ad altri interessi), ma che non offrono alcun criterio per formulare una norma generale».

[59] Sull'argomento v. CATAUDELLA A. *Segreto, privato e cronaca*, in AAVV, *Il riserbo e la notizia*, cit., pp. 89 ss., il quale, nel precisare i caratteri distintivi del segreto rispetto al privato, rileva che, in relazione agli artt. 14 e 15 Cost., sicuramente c'è coincidenza tra ambito del segreto e ambito del privato, ma ciò ha indotto « una parte della dottrina a spiegare tale normativa esclusivamente in chiave di difesa del segreto: "segreto domestico" e "segreto della corrispondenza"». Tuttavia, contro l'assolutezza di tali affermazioni, si deve notare che « non vi è, peraltro, un interesse del soggetto a tenere segreti tutti gli eventi che si verifichino nell'ambito spaziale del domicilio o siano affidati a mezzi riservati di comunicazione». Quindi, a seconda della natura delle notizie, il soggetto avrà interesse a limitarne, in misura variabile, la circolazione (notizie riservate), ovvero ad escluderla del tutto (notizie segrete), oppure ancora non si opporrà a consentirne la diffusione. L'autore, tuttavia, esclude che le norme in esame siano pertinenti al tema della riservatezza, poiché direttamente finalizzate ad impedire non l'indebita divulgazione di notizie riservate ma, più precisamente, il loro apprendimento: v. CATAUDELLA A, *La tutela civile della vita privata*, Milano, Giuffrè, 1972, p. 27.

[60] PIZZORUSSO A., *Sul diritto alla riservatezza nella Costituzione italiana*, in *Prassi e Teoria*, 1976, p. 37: «pur contribuendo indubbiamente alla tutela della riservatezza, le norme di questo tipo non possono dunque essere considerate come il fondamento di un corrispondente diritto costituzionale, ma soltanto essere utilizzate per operazioni interpretative dirette a combinare insieme gli effetti di precetti diversi».

2.3. Tutela a contrario ex articolo 21 Costituzione ed ulteriori osservazioni

In un'analoga prospettiva, la tutela della libertà di manifestazione del pensiero, di cui all'articolo 21[61], si pone, in una delle sue articolazioni, a presidio anche della pretesa di non rendere noto ai terzi quanto intimamente connesso al proprio modo di essere.

Questa norma è stata utilizzata dagli interpreti per due operazioni tra loro perfettamente antitetiche, volte, l'una a negare la rilevanza costituzionale del diritto alla riservatezza perché ritenuto incompatibile con la libertà di espressione; l'altra a fondare il suo rango costituzionale proprio su questa disposizione.

Punto di avvio della prima tesi è l'articolo 21 considerato in positivo, il quale tutela la libertà di manifestare il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione, potendosi esprimere attraverso la cronaca, l'arte, la scienza, la storiografia.

È assai probabile che l'esercizio di questa libertà possa entrare in conflitto con l'interesse alla riservatezza. La manifestazione del pensiero si realizza, infatti, mediante l'apprendimento delle notizie, la comunicazione e il libero scambio delle idee. In altre parole, essa ha il necessario presupposto nella libertà di informarsi e di informare, di modo che ogni limite alla circolazione delle informazioni si traduce, *ipso facto*, in un limite alla manifestazione del pensiero.

Queste premesse possono senz'altro essere condivise. Tuttavia, è necessario precisare che, già dall'applicazione dei principi giuridici generali, e aldilà di riferimenti specifici, si ricava che nessuna libertà ha carattere assoluto, ma, nel momento in cui ci si muove dall'enunciazione astratta di principio al suo

[61] Articolo 21 Cost: «Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione. La stampa non può essere soggetta ad autorizzazioni o censure. Si può procedere a sequestro soltanto per atto motivato dell'autorità giudiziaria nel caso di delitti, per i quali la legge sulla stampa espressamente lo autorizzi, o nel caso di violazione delle norme che la legge stessa prescriva per l'indicazione dei responsabili. In tali casi, quando vi sia assoluta urgenza e non sia possibile il tempestivo intervento dell'Autorità giudiziaria, il sequestro della stampa periodica può essere eseguito da ufficiali di polizia giudiziaria, che devono immediatamente, e non mai oltre ventiquattro ore, sporgere denunzia all'Autorità giudiziaria. Se questa non lo convalida nelle ventiquattro ore successive, il sequestro s'intende revocato e privo di ogni effetto. La legge può stabilire, con norme di carattere generale, che siano resi noti i mezzi di finanziamento della stampa periodica. Sono vietate le pubblicazioni a stampa, gli spettacoli e tutte le altre manifestazioni contrarie al buon costume. La legge stabilisce provvedimenti adeguati a prevenire e a reprimere le violazioni».

inserimento in un contesto ordinamentale, essa e le altre libertà soggiacciono a reciproci condizionamenti.

In altri termini, entrano a far parte di un sistema dal quale traggono gli strumenti essenziali alla loro realizzazione, ma anche, necessariamente, le correlative limitazioni[62].

Ciò si traduce, in concreto, nella conseguenza che le attività strumentali alla manifestazione del pensiero, quelle di ricerca e divulgazione delle informazioni, non possono essere illimitate, ma debbono misurarsi con altre libertà parimenti garantite, a condizione che se ne ammetta il rango costituzionale.

Da quest'ultima considerazione discende poi l'importante corollario che l'informazione non rappresenta un valore assoluto, ma può essere reputata tale solo se funzionale allo sviluppo della persona che, in taluni casi, è maggiormente assicurato dalla non informazione, in ossequio al diritto di non sapere, quale presupposto per la libera autodeterminazione personale.

L'articolo 21 è stato anche considerato in chiave completamente opposta a quella ora descritta, cioè come norma su cui basare il fondamento costituzionale del diritto alla riservatezza, conducendo al singolare risultato che l'articolo 21 sarebbe limite di sé stesso, poiché la manifestazione del pensiero troverebbe i suoi limiti nella stessa norma che la riconosce.

La particolare interpretazione in esame [63] muove dal rilievo che l'articolo 21, così come riconosce il diritto, esercitabile in positivo, di manifestare il proprio pensiero, parimenti ed intrinsecamente prevede la possibilità che un individuo abbia anche la libertà di tacere, di manifestare parzialmente il proprio pensiero o di rivelarlo soltanto ad alcuni soggetti, giacché, e ciò è

[62] I limiti all'art. 21 sono soliti essere classificati in interni ed esterni: tra gli altri v. Mantovani, *Op. cit.*, pp. 415 ss: «i primi, ricavabili dalla sola considerazione degli interessi e dei valori che sottostanno al riconoscimento del diritto in questione nel nostro ordinamento, nonché dalla formulazione letterale del medesimo, al di fuori dell'esigenza di tutelare altri interessi diversi. I secondi, desumibili dalla esigenza di salvaguardare altri interessi, individuali, collettivi, pubblici, coi quali il diritto di manifestazione del pensiero può entrare in collisione». Tra i limiti interni alcuni sono desumibili dalla stessa formulazione letterale dell'art. 21, la quale, « col parlare di "pensiero proprio", porta, a rigore, ad escludere dalla fattispecie ivi prevista, sia il "non pensiero" sia "il pensiero non proprio"» . Sulla problematica dei limiti esterni al diritto d'informare v., inoltre, C. Chiola, *L'informazione nella Costituzione*, Padova, Cedam, 1973, pp. 92 ss.

[63] CATAUDELLA A., *Op. ult. cit.*, pp. 32 ss.

evidente, la norma in questione non stabilisce un dovere di esprimere il pensiero.

Da queste premesse discende che tutte le attività di terzi finalizzate a carpire, apprendere e diffondere un pensiero che l'individuo non vorrebbe manifestare, ledono la sua libertà negativa garantita dall'articolo 21.

Il "diritto al silenzio", proprio in quanto partecipe degli stessi valori e presupposti per i quali è stato ritenuto meritevole di riconoscimento costituzionale il diritto di parlare, ha una dignità ed un'estensione pari a quest'ultimo, senza possibilità di creare una sorta di gerarchia interna tra le due libertà, trattandosi, invece, di situazioni pari-ordinate e parallele[64].

Anche la giurisprudenza, ormai consolidata, si è mossa lungo queste linee guida. Nelle svariate sentenze di merito che hanno affrontato il problema del conflitto tra i due interessi in esame, si ravvisa la tendenza a risolvere i reciproci rapporti attraverso l'applicazione di un criterio di bilanciamento, relativo e non assoluto, ispirato ai tre parametri dell'interesse sociale della notizia, della verità dei fatti narrati e della continenza[65].

* * * * * * *

A coronamento del predetto sistema di tutela della *privacy*, che discende dal combinato disposto dei citati articoli 2, 3, 13, 14, 15 e 21, possono poi indicarsi ulteriori disposizioni normative, anch'esse rilevanti al fine di proteggere la "personalità" dell'individuo, le sue estrinsecazioni ed i presupposti del pieno svolgimento della persona: a tal riguardo, non possono

[64] Sull'affermazione della pari dignità della libertà di parlare e di tacere v. CERRI A., *Libertà negativa di manifestazione del pensiero e di comunicazione - diritto alla riservatezza: fondamento e limiti*, in *Giur. Cost*., 1974, I, p. 611 ss. *Contra*: PIZZORUSSO A., *Op. ult. cit.*, p. 38: secondo l'autore il difetto di questa tesi sta «nel fatto che essa non tiene conto della circostanza che la tutela spettante alla libertà "negativa" di manifestazione del pensiero non può essere identica a quella propria della corrispondente libertà "positiva" giacché, mentre può ammettersi che, almeno di regola, sia rimesso all'insindacabile volontà del singolo il potere esclusivo di decidere se manifestare o meno un'opinione oppure una notizia, è invece evidente che al singolo come tale normalmente non è rimesso un corrispondente potere di tenere segreta qualunque opinione o qualunque notizia», pena l'annullamento del diritto di cronaca.

[65] V., a titolo di esempio, la sentenza della Corte d'appello di Roma dell'11 febbraio 1991, in *Dir. aut.*, 1992, p. 377, nella quale, inoltre, la libertà di manifestazione del pensiero e la riservatezza vengono entrambe considerate dotate di riconoscimento costituzionale.

dimenticarsi, almeno, l'articolo 19[66], che garantisce il diritto di professare la propria fede religiosa, l'articolo 16[67], in tema di libertà di circolazione, l'articolo 17[68], ai sensi del quale si riconosce il diritto di riunirsi pacificamente e senz'armi, e l'articolo 18[69], sulla libertà di associazione.

Alquanto scarsi sono gli appigli cui far riferimento per attribuire garanzia costituzionale alla riservatezza per il tramite dell'articolo 27 comma 2[70]. Come è noto, questa disposizione sancisce il principio della presunzione di non colpevolezza, cioè l'esigenza e il dovere che l'imputato sia considerato innocente, sia in seno al processo, sia nel contesto sociale, sino alla condanna definitiva.

Le perplessità discendono dal fatto che non esiste accordo su quale sia l'interesse che la norma mira a proteggere (reputazione e onore o riservatezza in senso stretto), e, in seconda battuta, se essa abbracci solo garanzie di natura squisitamente processuale (divieto di applicare misure e trattamenti incompatibili con lo stato di presunta innocenza), oppure si possa estenderne il raggio d'azione, in via mediata, a beni quali reputazione e riservatezza che acquistano importanza nell'ambito dei rapporti extraprocessuali e sociali[71].

Tuttavia, anche ammettendo che la norma in esame, tesi non pacifica in dottrina, copra specificamente la riservatezza, c'è da dire che essa interesserebbe comunque un ambito troppo settoriale e particolare, da cui

---

[66] Articolo 19 Cost: «Tutti hanno diritto di professare liberamente la propria fede religiosa in qualsiasi forma, individuale o associata, di farne propaganda e di esercitarne in privato o in pubblico il culto, purché non si tratti di riti contrari al buon costume».

[67] Articolo 16 Cost: «Ogni cittadino può circolare e soggiornare liberamente in qualsiasi parte del territorio nazionale, salvo le limitazioni che la legge stabilisce in via generale per motivi di sanità o di sicurezza. Nessuna restrizione può essere determinata da ragioni politiche. Ogni cittadino è libero di uscire dal territorio della Repubblica e di rientrarvi, salvo gli obblighi di legge».

[68] Articolo 17 Cost: «I cittadini hanno diritto di riunirsi pacificamente e senz'armi.
Per le riunioni, anche in luogo aperto al pubblico, non è richiesto preavviso.
Delle riunioni in luogo pubblico deve essere dato preavviso alle autorità, che possono vietarle soltanto per comprovati motivi di sicurezza o di incolumità pubblica».

[69] Articolo 18 Cost: «I cittadini hanno diritto di associarsi liberamente, senza autorizzazione, per fini che non sono vietati ai singoli dalla legge penale. Sono proibite le associazioni segrete e quelle che perseguono, anche indirettamente, scopi politici mediante organizzazioni di carattere militare».

[70] Articolo 27 Cost: «La responsabilità penale è personale. L'imputato non è considerato colpevole sino alla condanna definitiva. Le pene non possono consistere in trattamenti contrari al senso di umanità e devono tendere alla rieducazione del condannato. Non è ammessa la pena di morte.»

[71] Così: MANTOVANI F., *Op. cit.*, p. 388, nota n. 9.

sarebbe metodologicamente non corretto o quantomeno azzardato astrarre una tutela di carattere generale.

Ciò perché la norma si riferisce ad un soggetto che versa in uno *status* ben preciso, la cui condizione non può evidentemente essere estesa alla generalità dei consociati. L'art. 27 comma 2 conserva pur sempre la valenza, da tenere presente in chiave sistematica, di indice di natura culturale (considerazione comune alle altre norme costituzionali a carattere settoriale), atta a testimoniare che l'esigenza del riserbo ha trovato considerazione all'interno della Carta.

L'indagine appena compiuta permette di affermare che dalla mancanza di una norma costituzionale espressa a tutela della riservatezza non può certo dedursi, *sic et simpliciter*, il corrispondente disinteresse del Costituente. Gli argomenti che si oppongono a tale tesi scaturiscono sia dalle numerose disposizioni dettate a tutela di aspetti particolari del diritto unitario, sia dalle norme a carattere generale, secondo la lettura che se ne è data.

La considerazione unitaria di tutti questi dati, insieme alla interpretazione del microsistema risultante dalle reciproche relazioni tra clausole generali e norme specifiche, porta ad asserire, in base ad un'interpretazione evolutiva del testo costituzionale, la sicura ed innegabile rilevanza, in seno ad esso, del diritto alla riservatezza[72].

3. Diritto alla privacy e identità personale

La *privacy*, di per sé, è un concetto «*exasperatingly vague and evanescent*»[73], conseguentemente, il diritto alla privacy non viene concepito come una formula unitaria, bensì come una costellazione di diritti, cosicché il suo nucleo costitutivo di situazioni soggettive non è a struttura semplice, bensì composita e articolata.

---

[72] In questo senso v. PIZZORUSSO A., *Op. ult. cit.*, pp. 39 – 40, il quale ritiene che «il riconoscimento, anche a livello costituzionale, del diritto alla riservatezza abbia a fondarsi, più che su una od un'altra norma scritta, su un complesso di argomenti interpretativi che consentono di dimostrarne l'esistenza come principio non scritto della Costituzione vigente in Italia».

[73] Cosi MILLER A. R., *The assault on privacy, Computers, Data Banks and Dossier*, University of Michigan Press, Ann Arbor, 1971.

Come analizzeremo nei paragrafi successivi, il diritto alla *privacy*, infatti, oggi, non si riferisce più soltanto all'inviolabilità della sfera privata, come proiezione di un indifferenziato interesse al «*right to be let alone*», ma si realizza una notevole metamorfosi qualitativa, che orienta irreversibilmente il diritto alla *privacy* a caratterizzarsi come potere di controllo sulla circolazione delle informazioni personali.

Dalle prime applicazioni della normativa in materia di dati personali, derivava, in relazione all'indicazione in tema di bene giuridico, che le fattispecie previste, si prestassero nella loro ampia formulazione, a essere impiegate, non a tutela della *privacy stricto sensu* intesa[74], bensì di beni quale l'onore e la reputazione.

E il potere di controllo sulla circolazione delle informazioni personali, ha, come fine primario, quello di proteggere e tutelare la dignità delle persone prevalentemente sotto il profilo della loro identità. Da qui si parla spesso di *privacy* come protezione dell'identità personale.

Nel diritto all'identità personale è indubbiamente ricompreso il modo in cui un soggetto viene presentato agli occhi del pubblico attraverso il complesso delle informazioni che lo riguardano.

Una regolamentazione di tale diritto[75], dovrebbe affondare le radici in una nozione di *privacy* definita non solo nel senso tradizionale, borghese e proprietario, ma soprattutto come «l'aspirazione che ha ciascuno di noi a essere così com'è» e «a venire riconosciuto come tale anche dall'esterno, in maniera corretta e adeguata all'immagine che ciascuno di noi ha di sé».

In giurisprudenza si è spesso parlato di «interesse ad essere rappresentato nella vita di relazione, con la sua vera identità»[76].

La Corte di Cassazione definisce, l'identità personale, per differenza rispetto alla riservatezza, in questi termini: «il diritto all'identità personale si distingue da quello alla riservatezza: il primo assicura la fedele

[74] Ricordiamo che in relazione all'oggetto di tutela si individua un duplice contenuto: uno originario e tradizionale, afferente al right to be let alone, e l'altro meno individualistico, come interesse al controllo dei propri dati personali.

[75] NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza, alla protezione dei dati personali*, Padova, 2006.

[76] Cass. penale 22.6.1985, n. 3769

rappresentazione della propria proiezione sociale, il secondo, invece, la non rappresentazione all'esterno delle proprie vicende personali non aventi per i terzi un interesse socialmente apprezzabile»[77].

Possiamo quindi affermare che, tale diritto, nasce, per così dire, in provetta, a seguito degli esperimenti nati nel laboratorio giurisprudenziale, anche grazie all'apporto scientifico della dottrina. Dai predetti esperimenti è stata creata una nozione fluida, necessariamente mutevole nel tempo, indeterminata.

In linea con l'approccio della Corte di Cassazione del 1985, l'identità personale viene ritenuta dalla dottrina, come la proiezione sociale della personalità, che deve essere veritiera, non diffamatoria e non sviante, come il diritto alla propria immagine sociale.

Ma per tracciare una linea maggiormente evolutiva, è interessante riportare delle osservazioni condotte dal Professor Rodotà, il quale sosteneva come la stessa costruzione dell'identità fosse insidiata dalle nuove tecnologie e dalla loro capacità di influenzare modi di essere e comportamenti. Oggi, ad esempio, attraverso la creazione di profili di consumatori, e l'indirizzazione della produzione commerciale verso specifici modelli di utenza creati per assecondarne i gusti, si rischia di favorire un processo di omologazione di massa, basato su facili etichettamenti che rischiano di pregiudicare la possibilità dell'autodeterminazione individuale e di favorire l'esclusione di chi non voglia riconoscersi nel modello dominante e di tendenza. Pertanto, al fine di evitare che l'identità personale si riduca alla determinata tipologia di consumatore, elettore, comunque utente, che i profili e gli algoritmi attribuiscono a ciascuno, annullando l'unicità della persona, il suo valore, la sua eccezionalità, è necessario uno statuto forte della protezione dei dati personali.

Nella direzione tracciata dal Professor Rodotà, sono dignità, libertà ed eguaglianza i pilastri su cui si è articolato il percorso evolutivo del nuovo

[77] Cass. penale 22.6.1985, n. 3769. La sentenza, meglio nota come "Caso Veronesi" aveva riconosciuto la lesione del diritto all'identità personale del Presidente dello IEO, poi Ministro, Prof. Veronesi, in seguito all'uso alquanto subdolo e strumentale di alcune sue frasi a supporto di una campagna promozionale di sigarette.

diritto alla *privacy*. E di fronte alla frammentazione della persona determinata dalla proiezione dell'identità in mille banche dati diverse, la protezione dei dati personali si è rivelata l'unico strumento per la ricomposizione dell'io diviso, per garantire una rappresentazione della persona nella sua integralità. Non già diritto all'autorappresentazione quindi, ma strumento di tutela rispetto al riduzionismo o, peggio, alla distorsione che comporta la digitalizzazione e la conseguente "polverizzazione" dell'identità. Rodotà aveva compreso come, con Internet e la sua eterna memoria, il diritto all'identità non sia più confinabile in una dimensione statica e istantanea e non si esaurisca nel diritto all' "intangibilità della propria proiezione sociale", ma si estenda alla tutela di quel processo evolutivo e incrementale in cui si snoda oggi la costruzione della persona.

4. Dal segreto al controllo: la ridefinizione del diritto alla riservatezza

La riservatezza dovrebbe rappresentare il bene giuridico principale intorno al quale viene costruita e ruota la tutela penale della *privacy*: un bene da tempo emerso in maniera autonoma, la cui rilevanza è di certo avvertita nella collettività.

Verso la fine degli anni 60 e nei primi anni 70, con l'avvento dell'informatica, la raccolta e la conservazione dei dati non avviene più su supporti cartacei e con metodologie di reperimento manuale, (ad esempio consultando i vari diversi archivi), ma inizia ad esservi la possibilità di raccogliere, scambiare, collegare, selezionare grandi masse di dati, che vengono elaborati con processi elettronici. Ciò impone un adeguamento della protezione dei dati personali, che trova la sua *ratio* nel timore delle lesioni che le nuove tecnologie avrebbero potuto arrecare alla riservatezza.

Prima di soffermarci sulla disciplina dedicata alla protezione dei dati personali, è opportuno soffermarsi sulla riservatezza come bene giuridico in sé e sulle norme che si occupano della sua protezione e della sua tutela.

Nonostante ci fosse un mosaico di norme che proteggeva la sfera privata, quali ad esempio, l'articolo 10[78] del codice civile in tema di diritto all'immagine, l'articolo 614[79] del codice penale sull'inviolabilità del domicilio, l'articolo 616[80] dello stesso codice penale sull'inviolabilità della corrispondenza, dal tenore letterale delle disposizioni della Carta Costituzionale, non vi era un esplicito riferimento alla tutela della riservatezza, come diritto a sé[81].

Nel 1975 una importante sentenza della Corte di Cassazione[82] si è occupata di indicare i fondamenti e i punti salienti della riservatezza e ciò segna il punto di svolta del riconoscimento per la prima volta di un vero e proprio "diritto alla riservatezza".

In questo scenario, la riservatezza diventa «il forte diritto di non perdere mai il potere di mantenere il pieno controllo sul proprio "corpo elettronico", distribuito in molteplici banche dati nei luoghi più diversi. Un diritto che si caratterizza ormai come componente essenziale della nuova cittadinanza, da intendere come fascio di poteri e doveri che appartengono ad ogni persona, e non più come il segno di un legame territoriale o di sangue»[83].

---

[78] Art. 10 codice civile: «Qualora l'immagine di una persona o dei genitori, del coniuge o dei figli sia stata esposta o pubblicata fuori dei casi in cui l'esposizione o la pubblicazione è dalla legge consentita, ovvero con pregiudizio al decoro o alla reputazione della persona stessa o dei detti congiunti, l'autorità giudiziaria, su richiesta dell'interessato, può disporre che cessi l'abuso, salvo il risarcimento dei danni».

[79] Articolo 614 codice penale: «Chiunque s'introduce nell'abitazione altrui, o in un altro luogo di privata dimora, o nelle appartenenze di essi, contro la volontà espressa o tacita di chi ha il diritto di escluderlo, ovvero vi s'introduce clandestinamente o con inganno, è punito con la reclusione da sei mesi a tre anni. Alla stessa pena soggiace chi si trattiene nei detti luoghi contro l'espressa volontà di chi ha il diritto di escluderlo, ovvero vi si trattiene clandestinamente o con inganno. Il delitto è punibile a querela della persona offesa. La pena è da uno a cinque anni, e si procede d'ufficio, se il fatto è commesso con violenza sulle cose, o alle persone, ovvero se il colpevole è palesemente armato».

[80] Articolo 616 codice penale: «Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da euro 30 a euro 516. Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, è punito, se dal fatto deriva nocumento ed il fatto medesimo non costituisce un più grave reato, con la reclusione fino a tre anni.
Il delitto è punibile a querela della persona offesa. Agli effetti delle disposizioni di questa sezione, per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica, ovvero effettuata con ogni altra forma di comunicazione a distanza».

[81] RAVÀ, *Istituzioni di diritto privato*, Padova, 1934

[82] Cass. 27 maggio 1975, Santuosso, in VISINTINI, *I fatti illeciti* Padova 2004.

[83] Relazione annuale del Garante, RODOTÀ S., Roma, 2003

Dal punto di vista del penalista, basandosi sul dogma della legalità, il nucleo del problema si incentra sulla ricerca del riferimento normativo e costituzionale della riservatezza dal quale trarre le basi per valutare l'opportunità politico criminale di una sua tutela penale.

Sul versante costituzionale la tutela, come osservato nei paragrafi precedenti, sembra basarsi essenzialmente sugli articoli 14 e 15 della Costituzione, rispettivamente riguardanti il domicilio, la libertà e la segretezza della corrispondenza e sull'articolo 21 (a contrario), concernente invece la libertà di manifestazione del pensiero, ma ancora e soprattutto, su una più approfondita analisi interpretativa dell'articolo 2 della Costituzione, non più concepito come formula riassuntiva ma come fattispecie aperta, che, riconoscendo e garantendo «i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità», va letto alla luce dell'articolo 12[84] della Dichiarazione Universale dei diritti dell'uomo «nessun individuo può essere sottoposto a interferenze nella sua vita privata (…)» e dell'articolo 8[85] della Convenzione europea sulla salvaguardia dei diritti dell'uomo e delle libertà fondamentali che afferma il «diritto di ogni persona al rispetto della sua vita privata e familiare». Pertanto, il diritto alla riservatezza, per il disposto dell'articolo 2 della costituzione, è, oggi, un diritto inviolabile.

Assodato ciò, è inoltre necessario precisare che siamo in presenza di un bene giuridico suscettibile di modificazioni nel tempo, con il mutare del contesto storico e sociale, delle esigenze degli ambienti, delle zone e dei tempi, che ne richiedono la duttilità del contenuto. Perciò, a causa della mancanza di una definizione rigida di diritto alla riservatezza non è possibile delineare *ex ante* tutte le condotte concretamente o potenzialmente lesive del bene

[84] Articolo 12 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».

[85] Articolo 8 CEDU: «Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, per la pubblica sicurezza, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui».

protetto, né sperare di costruire delle fattispecie di incriminazione tanto generiche da passare indenni col mutare del tempo e dei mutamenti sociali[86].
Autorevole dottrina, interrogandosi sulla matrice del diritto alla riservatezza, ne individua un contenuto ulteriore: il diritto alla riservatezza non è solo il diritto ad essere lasciati in pace, ma è anche e soprattutto il diritto a che nessuno possa utilizzare, a nessun titolo e per nessuna ragione, senza il necessario consenso, qualunque informazione[87].
Sembra possibile affermare che la tutela della persona con particolare riguardo alla sfera della sua riservatezza, si sia caratterizzata da un duplice contenuto: la libertà negativa, che inquadra il diritto alla riservatezza come diritto a mantenere riservati i propri dati, diritto al segreto, e la libertà di segno positivo, come diritto a valenza poliedrica di salvaguardare la propria identità personale, di proteggere i propri dati, come diritto al controllo.
Da qui una nuova ridefinizione della riservatezza: si passa da un concetto statico relativo al mero segreto delle informazioni riguardanti la propria sfera privata e dunque la protezione da condotte di aggressione a questa particolare sfera, al più dinamico e attuale diritto ad avere sotto controllo tutte le informazioni, le notizie, i dati, che nella moderna società dell'informazione, circolano in un modo sempre più veloce e incontrollabile.
Il legislatore nazionale ha reagito a questa fondamentale svolta, minuscola se paragonata alle svolte epocali in altri campi, ma enorme se misurata rispetto al diritto del singolo[88], aggiornando il catalogo delle fattispecie incriminatrici, e dotando l'arsenale repressivo di strumenti capaci di reprimere fatti abusivi in relazione a questo profilo di tutela della riservatezza.
Il fatto che oggi la vita privata vada tutelata non solo più in termini di intimità, e dunque come diritto a restare solo, ma anche come libertà, ossia diritto a poter compiere libere scelte senza essere condizionato dai fattori esterni, rende necessaria un'interpretazione estensiva delle espressioni

[86] MUCCIARELLI F. *Informatica e tutela penale della riservatezza,* in *Il diritto penale dell'informatica nell'epoca di internet*, PICOTTI L. Padova, 2004.
[87] CARNELUTTI F., *Diritto alla vita privata, in Riv. Trim. dir. Proc*., 1995.
[88] MUCCIARELLI F, *Informatica e tutela penale della riservatezza* in *Il diritto penale dell'informatica nell'epoca di internet*, PICOTTI L. Padova, 2004.

"*intimidad*", "*vie privee*", "riservatezza" e così via, in modo da poterle adattare alle nuove esigenze che progressivamente emergono in relazione ai cambiamenti del contesto storico, culturale e tecnologico di riferimento.

Il Garante ha reso una felice sintesi della doppia valenza (passiva e attiva) della riservatezza: «La *privacy* cammina ormai con due gambe: la riservatezza e il controllo. Alla prima si addice il silenzio, all'altra la trasparenza»[89].

5. *Il diritto alla protezione dei dati personali: habeas data*

Il diritto alla protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (articolo 8). Oggi è tutelato, in particolare, dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), e dal Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196), adeguato alle disposizioni del Regolamento (UE) 2016/679 dal Decreto legislativo 10 agosto 2018, n. 101.

Diversamente dal diritto alla riservatezza e dal diritto all'identità personale, che pure per anni sono stati il centro di un'elaborazione dottrinaria e giurisprudenziale, il diritto alla protezione dei dati personali, è introdotto *per tabulas* dal legislatore con l'emanazione del codice *privacy*.

Il codice in materia di protezione dei dati personali si apre con la solenne dichiarazione del diritto di chiunque alla protezione dei dati che lo riguardano. Si fa riferimento al riconoscimento di un nuovo diritto, protetto dall'articolo 1 del Codice *privacy* che riproduce esattamente la disposizione contenuta nell'articolo 8 della Carta di Nizza[90].

---

[89] Relazione annuale del Garante, anno 1997, p.11.

[90] Articolo 8 Carta di Nizza: «Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge.

Il diritto alla tutela dei dati personali può essere considerato, in senso affermativo, come il diritto del soggetto a che i propri dati personali siano registrati, gestititi, custoditi, trasmessi a terzi, divulgati in modo corretto e *secundum legem*, e, in senso negativo come il diritto di non subire qualsiasi tipo di acquisizione, utilizzazione, o manipolazione di informazioni relative ai propri dati personali.

La previsione di tale diritto in un articolo separato nel codice della *privacy*, rispetto alla disposizione sulle finalità del trattamento conferma la sua autonoma configurazione, infatti si tratta del complesso delle facoltà specifiche riconosciute ai soggetti in rapporto al trattamento dei dati personali, che superano quelle attinenti al più generale diritto alla riservatezza.

Ciò non implica *ex se* che ogni soggetto abbia un diritto dominicale su tutti i dati che lo riguardano.

In primis, analizzando la natura di tale diritto alla protezione dei dati personali, diversamente da quanto accade per la riservatezza, da sempre caratterizzata dall'immaterialità, sicuramente tale diritto attiene a una sfera tangibile, concreta, percepibile, ma non perciò assimilabile *tout court* agli altri "beni" suscettibili di appropriazione. Per di più, essendo tale diritto collocato tra i diritti della personalità, gode di una forma di tutela propria e speciale tipica dei diritti fondamentali della persona.

Soffermarsi sulla questione circa la personalità unica o plurima dei diritti della personalità, porterebbe a conseguenze sterili, quello che è importante notare è che tale diritto, riconosciuto dal codice *privacy*, ma prima ancora dalla Carta di Nizza, consente di "modernizzare" e "rimodellare" i classici diritti alla riservatezza e all'identità personale.

La *ratio* principale di tale diritto è attribuire al soggetto la possibilità di autogovernarsi e autodeterminarsi sulla base della propria consapevolezza, che lo strumento primigenio di cui è fatta l'idea di sé presso gli altri è

Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

costituito dalle informazioni personali, il cui controllo gradua o addirittura impedisce l'invadenza degli altri nella propria sfera privata[91].

La salvaguardia dell´autodeterminazione informativa, dell´autonomia e della responsabilità delle scelte, articolata non soltanto nei vari istituti del consenso informato, ma anche nella valutazione di impatto *privacy*, della minimizzazione del trattamento, della protezione sin dalla progettazione e per impostazione predefinita, è in questo senso presidio essenziale per mantenere il governo sulle nostre tracce digitali, che più di ogni altro aspetto concorrono oggi a definire la nostra identità e, con essa, la nostra libertà.

Nel contesto giuridico internazionale si parla di "*data protection*" «per sottolineare che non si tratta di stare chiusi nel proprio mondo privato, al riparo da sguardi indiscreti, ma anche di potersi proiettare liberamente nel mondo attraverso le proprie informazioni mantenendo però sempre o controllo sul modo in cui queste circolano e vengono da altri utilizzate»[92].

La rappresentazione sociale dell'individuo, nella odierna c.d. "società dell'informazione" è legata spesso ai dati personali circolanti sul *web,* e ciò se da un lato fa emergere nuovi rischi nell'agire di ogni giorno, dall'altro fa sorgere la necessità di creare una sorta di "*Internet Bill of Rights*".

Oggi si avverte sempre di più il bisogno di una tutela del proprio "corpo elettronico"[93], della propria identità digitale, della autodeterminazione informativa.

Da qui vi è il fondamentale passaggio dall'*habeas corpus* all'*habeas data*[94] o più specificamente all'«*habeas corpus* in chiave digitale», per dirlo in altri termini, corrispettivo, nella società digitale, di ciò che *l'habeas corpus* ha rappresentato sin dalla *Magna Charta*.

Il denominatore comune è il controllo, controllo sul proprio corpo, nel primo caso, controllo sui propri dati, nel secondo.

Il professor Rodotà, allora presidente dell'Autorità rappresentava che «i cittadini mostrano di preoccuparsi assai del loro "corpo elettronico", di una

[91] CIRILLO G. P., La tutela della Privacy nel sistema del nuovo codice dei dati personali, Padova, 2004.
[92] RODOTÀ S., *in Intervista su Privacy e Libertà*
[93] RODOTÀ S., *in Intervista su Privacy e Libertà*
[94] RODOTÀ S., *Il mondo nella rete.* Quali i diritti, quali i vincoli, Roma – Bari, 2014

esistenza sempre più affidata alla dimensione astratta del trattamento elettronico delle loro informazioni, nella società digitale, noi siamo i nostri dati. Le persone sono ormai conosciute da soggetti pubblici e privati quasi esclusivamente attraverso i dati che le riguardano, e che fanno di esse una entità disincarnata. Con enfasi riduzionista, per molti versi pericolosa, si dice che "noi siamo le nostre informazioni". La nostra identità viene così affidata al modo in cui queste informazioni vengono trattate, collegate, fatte circolare. La tutela dei dati è un diritto fondamentale della persona, una componente essenziale della nuova cittadinanza […] non solo per respingere invasioni illegittime o indesiderate, ma anche per evitare di essere "costruiti" dagli altri»[95].

La legge sul trattamento dei dati personali assume oggi il ruolo di uno statuto della libertà informatica; ciò significa che la riservatezza altro non è che un limite di esercizio di tale libertà che deve inevitabilmente contemperarsi con la libertà di organizzazione e utilizzazione dei dati[96].

Quanto finora premesso, potrebbe essere sufficiente per una mera analisi del diritto alla protezione dei dati personali, in sé considerato. Ma, per il giurista, o ancor di più per il penalista, emergono ulteriori quesiti. Nonostante nel linguaggio comune si sia soliti sovrapporre il concetto di riservatezza o più specificamente di diritto alla *privacy*, cui la riservatezza costituisce una *species*, con il concetto di diritto alla protezione dei dati personali[97], la realtà giuridica è ben diversa.

In primis, è necessario precisare che si tratta di due istituti giuridici ontologicamente diversi che regolano situazioni contigue ma non sovrapponibili.

---

[95] RODOTÀ nel discorso di presentazione della relazione annuale del Garante al Parlamento dell'anno 2001.

[96] MESSINETTI D. in *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali* in Enc. Dir., Milano, 1983.

[97] Contribuiscono all'immedesimazione il fatto che la raccolta delle norme in tema di trattamento dei dati personali abbia preso il nome di "Codice della Privacy" e non "Codice della protezione dei dati personali", o ancora, che di conseguenza l'Autorità Garante del trattamento dei dati personali si sia autodefinita "Autorità Garante della Privacy"[97]- (tale fraintendimento interessa anche la nozione di riservatezza, anche essa spesso utilizzata erroneamente come sinonimo di diritto alla protezione dei dati personali).

La protezione dei dati personali, può in senso lato, comprendere anche la *privacy*, ove questa sia intesa come il diritto di scegliere cosa, nel nostro spazio personale, vogliamo rendere conoscibile agli altri, ma non si esaurisce in ciò. Il diritto alla protezione dei dati personali è molto più ampio, non è il solo controllo delle informazioni private, la mera autodeterminazione informativa, come espressione della ridefinizione della riservatezza, ma si estende «alla tutela di ogni informazione riferita o riferibile a una persona identificata o identificabile, quale che ne sia il contenuto o l'oggetto»[98].

La Corte di Giustizia dell'Unione Europea mantiene distinte le due nozioni, inquadrando il diritto alla *privacy* come diritto ad avere uno spazio privato immune da ingerenze, mentre il diritto alla protezione dei dati personali come il diritto a un corretto trattamento dei propri dati personali, indipendentemente dal fatto che siano dati privati.

È lecito pertanto affermare che, il *discrimen* tra le due nozioni si rinviene nel bene oggetto di tutela, la sfera privata, che ha una portata esclusivamente individualistica, nel diritto alla *privacy* e l'interesse generale alla correttezza e liceità del trattamento dei dati, nel diritto alla protezione dei dati personali, che ha la duplice natura di diritto dell'individuo e interesse della collettività[99].

In tal senso, la dottrina osserva che la disciplina della raccolta e del trattamento dei dati personali si rivela irriducibile alla sola cifra individualistica, in quanto attinge alle garanzie di trasparenza e legalità quali presupposti di funzionamento del sistema democratico[100].

Possiamo pertanto affermare che il rapporto intercorrente tra le due nozioni è di specialità bilaterale o reciproca, in quanto la prima tutela la vita privata anche al di fuor del contesto del trattamento dei dati, la seconda tutela la

[98] Corte Giustizia UE (Grande Sezione), 6 ottobre 2015, C-362/14, nel celebre caso *Maximilian Schrems c. Data Protection Commissioner*.
[99] LAMANUZZI M. *Diritto penale e trattamento dei dati personali. Codice della privacy, novità introdotte dal regolamento UE 2016/679 e nuove responsabilità per gli enti*.
[100] RODOTÀ S. *Tecnologie e diritti*, Bologna, 1995.

correttezza del trattamento dei dati personali anche a prescindere della sua incidenza sulla sfera privata dell'individuo[101].

In un mondo iper-connesso e in un'economia fondata sui dati e alimentata dall'intelligenza artificiale, presupposto per la dignità e quindi anche per la libertà dell'uomo è la protezione di ciò che, come i suoi dati personali, lo caratterizza più emblematicamente.

E se il diritto in generale svolge oggi, sempre più, una funzione di umanizzazione della tecnica, soprattutto quando il soggetto di diritto rischia di divenire mero oggetto di calcoli predittivi e tecniche manipolative, il diritto alla protezione dei dati personali rappresenta una straordinaria risorsa per mantenere la persona, nella sua libertà e nella sua responsabilità, al centro della società digitale.

6. La nozione di dato personale

Il *fulcrum* della normativa sulla *privacy* è il dato personale, che rappresenta lo strumento tecnico-giuridico attraverso il quale i legislatori, nazionali e comunitari, tutelano l'insieme dei diritti collegati all'identità personale; il dato personale, può essere considerato, dunque, come un bene giuridico di secondo livello, un contenitore vuoto all'interno del quale l'interprete inserisce uno specifico contenuto relativo al patrimonio informativo dell'interessato.

Il dato personale è definito come: «qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale»[102].

È da precisare che, la persona a cui si riferiscono i dati soggetti al trattamento si definisce "interessato" e può essere solo una persona fisica e non un'azienda. Dalla definizione suddetta, si comprende che, *condicio sine qua non* alla classificazione di un dato come "personale", sia il fatto che

[101] LAMANUZZI M. *Diritto penale e trattamento dei dati personali. Codice della privacy, novità introdotte dal regolamento UE 2016/679 e nuove responsabilità per gli enti*.
[102] Così come stabilito dall'articolo 4 del D.lgs. 196/2003.

consenta l'identificazione dell'individuo o descriva l'individuo in modo tale da consentirne l'identificazione acquisendo altri dati.

L'identificazione è fondamentale, in quanto permette di distinguere la persona da qualsiasi altro soggetto, ma non occorre che l'informazione sia in grado di individuare fisicamente la persona perché sia considerata dato personale, basta pensare ai c.d. "*cookie*", "*fingerprint*", che sono considerati anche dati personali, in quanto identificano il *browser* o il dispositivo digitale tramite il quale la persona naviga in rete.

Identificabile è la persona che può essere identificata anche mediante il riferimento ad ulteriori elementi.

Possiamo perciò affermare che il dato personale è un concetto dinamico, sul quale ha preponderante rilevanza il contesto nel quale è situato e le componenti intrinseche dello stesso, nel senso che anche se un'informazione isolata non è in grado di portare all'identificazione di un individuo, il fatto che detta informazione possa essere utilizzata per l'identificazione tramite incrocio con altri dati ne determina comunque la natura di dato personale.

6.1. Categorie particolari di dato personale

I dati personali sono classificabili in varie tipologie che, a seconda della loro peculiarità, devono essere trattati con cautele e regole diverse.

La tassonomia dei dati personali riflette un sistema di tutela graduate in ragione della natura del dato e della sua capacità di incidere nel concreto vivere degli interessati.

In primo luogo è opportuno evidenziare che i dati personali possono essere solo comuni e mai anonimi, in quanto, i primi comprendono tutte quelle informazioni (nome, cognome, partita I.V.A., codice fiscali, indirizzo) che consentono di individuare una persona fisica, i secondi, sono dati che *ab origine*, o a seguito di trattamento, non possono essere associati a un interessato e, di conseguenza, non assolvono il requisito dell'identificabilità del soggetto, in mancanza del quale il dato personale, non può essere considerato tale.

Il Garante, per chiarire il concetto di "identificabilità" dell'interessato, ha utilizzato il riferimento agli "sforzi ragionevolmente prevedibili" che il titolare può porre in essere per identificare, appunto, l'interessato.

Quei dati personali idonei a rivelare «l'iscrizione nel casellario giudiziale[103], l'iscrizione nell'anagrafe delle sanzioni amministrative dipendenti da reato, l'avere carichi pendenti in relazione ai due punti precedenti, la qualità di imputato o indagato», sono i c.d. "dati giudiziari"[104]. La categoria dei dati giudiziari comprende anche altri dati personali, riferiti ad esempio a provvedimenti giudiziari non definitivi o alla semplice qualità di imputato o indagato[105].

Il trattamento dei dati giudiziari è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichi le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili[106].

Una delle *species* più delicate rientranti all'interno dei dati personali, è quella relativa ai dati sensibili, con tale formula si intende far riferimento a quei dati che sono idonei a rivelare «l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona»[107]; i dati relativi alla salute e alla vita sessuale sono detti anche "super-sensibili" in quanto sono gli unici per i quali non sussiste alcune esenzione che ne consente l'uso in assenza di un consenso.

In particolare, nella categoria dei dati sensibili, distinguiamo tra[108] dati genetici, dati biometrici e dati personali relativi alla salute. I primi sono relativi alle caratteristiche genetiche ereditarie o acquisite e forniscono

[103] Ad esempio: condanna penale, interdizione dai pubblici uffici.
[104] Articolo 10 GDPR
[105] Non sono considerati dati giudiziari i seguenti provvedimenti: quelli definitivi di interdizione e inabilitazione e revoca, quelli che dichiarano fallito l'imprenditore, quelli di omologazione del concordato fallimentare, quelli di chiusura del fallimento, quelli di riabilitazione del fallito.
[106] Art. 21 D.lgs. 196/2003
[107] Così come definiti dall'articolo 9 GDPR.
[108] Per i dati genetici articolo 4 punto 13 *GDPR*, per i dati biometrici articolo 4 punto 14 *GDPR*, per i dati personali relativi alla salute articolo 4 punto 15 *GDPR*.

informazioni univoche sulla fisiologia o sulla salute di detta persona, e risultano in particolare dall'analisi di un campione biologico; i secondi sono dati ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona, come ad esempio i dati dattiloscopici; i terzi sono dati personali attinenti alla salute fisica e mentale di una persona, che rivelano informazioni sul suo stato di salute, e vengono raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria.

La definizione di dato sensibile è esclusiva: sono considerati tali solo i dati specificamente indicati, indipendentemente dal carattere di rilevanza, o riservatezza, che secondo il senso comune, si potrebbe attribuire ad altre tipologie di dati[109].

Salvo eccezioni, il *GDPR* prevede, come principio generale, il divieto di trattare i dati sensibili.

La *ratio* di una tutela differente e rafforzata di tali dati, risiede nella considerazione, anche sulla scia dei principi statuiti in costituzione, che non si tratta, dunque, di dati di carattere "neutro", bensì di dati che riguardano gli aspetti più intimi della vita di un individuo, che si preferisce non siano resi facilmente di pubblico dominio, vista anche la macro-dimensione del fenomeno di diffusione del flusso degli stessi, in quanto se non trattati secondo i principi di liceità e correttezza, potrebbero arrecare gravi danni all'interessato.

Meritano di essere menzionati, in questa sede, anche i c.d. "dati semi-sensibili", che comprendono per fare degli esempi, i dati relativi alle liste sospettati di frode, i nominativi inseriti nelle centrali rischi, i dati relativi alla situazione finanziaria. Si tratta di una categoria non ben definita, non ancora circoscritta, un *tertium genus,* a cavallo tra i dati comuni e i dati sensibili, il cui trattamento potrebbe arrecare danni al titolare.

Per quel che rileva ai fini della presente trattativa, l'appartenenza di un dato personale a una delle predette categorie, incide in modo significativo sulla

[109] Ad esempio: stato di divorzio, stato di figlio adottato, codice bancomat. Si tratterà di dati particolari, ma non di dati sensibili.

responsabilità penale discendente dalle violazioni della disciplina dettata dal D.lgs. 196/2003, aggravando notevolmente il carico sanzionatorio.

7. Il trattamento dei dati personali nel mondo contemporaneo

Partendo dall'assunto che, il diritto alla protezione dei dati si è sviluppato a partire dal diritto al rispetto della vita privata e che il concetto di vita privata si riferisce agli esseri umani, sembrerebbe che siano le persone fisiche dunque, i principali beneficiari della protezione dei dati.

Ma, la Corte europea dei diritti dell'uomo ha evidenziato che non esiste una netta separazione tra vita privata e vita professionale per quanto riguarda i dati personali, per cui anche le informazioni riguardanti la vita professionale e pubblica di una persona, sono dati personali.

In tal senso si potrebbe ritenere che i diritti della CEDU appartengano non solo alle persone fisiche ma anche alle persone giuridiche.

Per queste ultime la Corte dei diritti dell'uomo tende a considerare più che altro il diritto al rispetto del "domicilio" e della "corrispondenza". In realtà la Convenzione 108/81 consente alle parti contraenti di estendere la tutela prevista per le persone fisiche anche alle persone giuridiche. C'è da dire, però, che il diritto dell'Unione europea, comunque, non contempla norme a tutela dei dati personali delle persone giuridiche, e nemmeno la normativa italiana.

Partiamo dall'articolo 4 del Regolamento europeo, che definisce il trattamento dei dati personali**.**

Trattamento dei dati personali è «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».

Il concetto di trattamento ingloba tutte quelle operazioni che implicano una conoscenza di dati personali**.**

L'interessato (*data subject*) al trattamento è la persona fisica a cui si riferiscono i dati personali.

Il concetto di interessato è cambiato rispetto al passato, nel senso che oggi siamo tutti potenzialmente interessati in considerazione del fatto che i trattamenti dei dati personali inglobano l'intera società. Basti pensare alle telecamere di controllo del traffico, per capire che in ogni istante siamo potenziali interessati di un trattamento. Il concetto di interessato, quindi, è dinamico. L'interessato, può essere solo una persona fisica, e non una persona giuridica, un ente o un'associazione.

La normativa attribuisce specifici diritti all'interessato, che è opportuno brevemente osservare; si tratta del diritto di revocare il consenso in qualsiasi momento, il diritto di ottenere informazioni su quali dati sono trattati dal titolare (anche detto diritto di informazione), il diritto di chiedere ed ottenere in forma intellegibile i dati in possesso del titolare (diritto di accesso), il diritto di esercitare l'opposizione al trattamento in tutto o in parte e di opporsi ai trattamenti automatizzati[110], da non confondere con il diritto alla cancellazione dei dati, in base al quale l'interessato può impedire il trattamento che non sia compatibile con le finalità del consenso (anche detto diritto all'oblio); ma ancora, il diritto di ottenere l'aggiornamento o la rettifica dei dati conferiti, il diritto di chiedere ed ottenere trasformazione in forma anonima dei dati; il diritto di chiedere ed ottenere il blocco o la limitazione dei dati trattati in violazione di legge e quelli dei quali non è più necessaria la conservazione in relazione agli scopi del trattamento e da ultimo, ma non per importanza, il diritto alla portabilità dei dati[111].

[110] Art. 21 del Regolamento europeo, che trova la sua ragion d'essere nella tutela dell'individuo dal controllo eccessivo dello Stato;

[111] Si tratta di un diritto che differisce dal diritto all'accesso ai dati. Riconosciuto all'art. 20 del GDPR, «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 forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti».

L’interessato, per l'esercizio di tali diritti, può rivolgersi direttamente al titolare del trattamento, il quale è tenuto a collaborare col titolare ai fini dell’esercizio dei diritti.

I dati debbono essere trattati in modo lecito, corretto e trasparente nei confronti dell’interessato. Le finalità devono essere determinate, esplicite e legittime; i dati adeguati, pertinenti, esatti ed aggiornati, oltre che limitati a quanto necessario rispetto alle finalità, e comunque da trattare in modo da garantirne un’adeguata sicurezza.

8. Il quadro normativo

Ad onor del vero, dalla ricerca sociologica di situazioni giuridiche soggettive emergenti, coniugata con una seria analisi del diritto, è stato possibile, negli ultimi decenni passati, “agganciare” la rivoluzione tecnologica di fine millennio al sistema dei diritti, evitando, in più occasioni, ma mai definitivamente, quella tanto paventata “deriva tecnologica” che genererebbe il dominio incondizionato e irrefrenabile delle macchine sull’uomo, della tecnologia sui diritti, della logica dei *microchip* sui valori fondamentali dell’individuo.

In Italia, il merito dell’introduzione di tale nuovo metodo di analisi giuridica, va ascritto a una serie di giuristi contemporanei, che, partendo dallo studio senza pregiudizi e ad ampio spettro della responsabilità civile e del danno extracontrattuale, sono approdati a una lunga riflessione che ha coinvolto e travolto la galassia dei diritti della persona, teorizzando contestualmente, quelle che sono state definite nuove ipotesi di danno: quello biologico, quello esistenziale, quello ambientale, fino ad arrivare al danno prodotto dall’esercizio di un’attività apparentemente lineare e ordinaria, quale il trattamento dei dati personali, ma a ragione, considerata dal legislatore, prima del 1996 e poi del 2003, quale attività pericolosa. Parliamo quindi, del danno da illecito trattamento dei dati personali.

Lungo questa scia, considerando l’importanza attribuita ai dati personali nella società attuale, vi sono diverse legislazioni rivolte a proteggerli.

Oltre a mettere in evidenza una serie di indicazioni regolatrici rinvenibili in Italia[112], quello che appare importante sottolineare è che, il diritto alla protezione dei dati personali, prima della sua concreta attuazione nell'ordinamento nazionale, era stato oggetto di diversi interventi normativi a livello internazionale e/o sovranazionale; costituiscono, pertanto, i pilastri sui quali si fonda la normativa italiana: la Convenzione di Strasburgo (Convenzione del 28 gennaio 1981 n.108) intesa a disciplinare proprio i trattamenti elettronici di dati personali, nonché le innumerevoli Raccomandazioni adottate in materia in seno allo stesso organismo, e la Direttiva 95/46/CE del Parlamento europeo e del Consiglio che ha determinato l'attuazione di norme specificatamente aventi ad oggetto la tutela delle persone rispetto al trattamento dei dati personali.

Sulla base di questi *input* derivanti dall'appartenenza all'Unione Europea, in Italia, venne emanata la legge 31 dicembre 1996 n. 675, "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali", una complessa disciplina, volta alla regolamentazione, finalizzata in primis alla libera circolazione, dei flussi informativi, con ricadute su specifiche posizioni giuridiche soggettive di individui, soggetti privati e pubblici, in sede di trattamento dei dati personali.

La primissima fase di applicazione di detta normativa è stata caratterizzata dal tentativo di far capire e diffondere i nuovi strumenti a disposizione di persone fisiche e giuridiche nell'ottica di tutela della loro riservatezza, piuttosto che puntare immediatamente alla comprensione del valore e dei molteplici diritti sottesi al corretto e lecito trattamento dei dati personali.

L'uscita di scena della legge 675/96 si ha ad opera del decreto legislativo 196/2003 recante il "Codice in materia di protezione dei dati personali", che oltre a riordinare interamente la materia, nasce con l'intento di dare un segnale forte nella direzione dell'affermazione della complessità e poliedricità della disciplina, cercando di far uscire la materia dall'ormai

[112] I riferimenti sono alla legge 20 maggio 1970 n. 300 (c.d. *Statuto dei lavoratori*) che ha introdotto limiti all'utilizzo di impianti audiovisivi (art.4), agli accertamenti sanitari e prevedendo il divieto di indagini sulle opinioni (art. 8); e alla legge 1 aprile 1981 n.121 "*Nuovo ordinamento dell'amministrazione della pubblica sicurezza*" che disciplina taluni profili relativi alla natura ed entità dei dati e delle informazioni raccolte (art. 7) ed i controlli (art. 10).

riduzionistico steccato della *privacy*, per approdare, finalmente, a una nozione, forse meno *appealing*, ma più rispondente alla natura dei diritti tutelati, di diritto alla protezione dei dati personali[113].

Il nuovo quadro giuridico europeo in materia di protezione dati rappresenta dunque un grande passo avanti nella direzione di un governo equilibrato delle innovazioni tecnologiche che hanno profondamente modificato la nostra società. Ma ciò che, più di ogni altra misura, garantirà l'effettività dei diritti sanciti sarà la diffusione di quella "cultura della *privacy*" necessaria per promuovere, a un tempo, sviluppo economico e libertà, efficienza amministrativa e dignità della persona.

8.1 La Legge 300/1970 "Statuto dei Lavoratori" e la Legge 121/1981 "Nuovo ordinamento dell'amministrazione della pubblica sicurezza"

Un contributo importante al diritto alla *privacy* e al trattamento dei dati personali proviene dalla legge 20 maggio 1970, n. 300 – meglio conosciuta come "Statuto dei lavoratori" – che costituisce una delle fonti normative fondamentali del diritto del lavoro. Uno dei meriti da riconoscere a tale legge, è quello di aver messo in evidenza, in alcuni suoi articoli, la questione concernente il bilanciamento tra il diritto alla riservatezza del lavoratore, e il controllo dello stesso da parte del datore di lavoro.

La protezione dei dati personali è esigenza particolarmente avvertita nell'ambito del rapporto di lavoro[114], in ragione dell'intenso coinvolgimento della persona del lavoratore nell'esecuzione della prestazione e dello stato di debolezza economica e contrattuale che generalmente caratterizza la posizione del lavoratore medesimo nei confronti del datore.

Connaturale alla costituzione del rapporto di lavoro, e addirittura alla fase precedente del reclutamento del personale, è che il datore di lavoro raccolga e gestisca una serie di dati relativi ai propri dipendenti o aspiranti tali. Posto

[113] PANETTA R., *Libera circolazione e protezione dei dati personali*, Milano, 2006.

[114] Sull'argomento è interessante CAUTADELLA S., *Accesso ai dati personali, riserbo e controllo sull'attività di lavoro*, in *Arg. Dir. Lav.* 2001, n.1; CHIECO P., *Privacy e lavoro. La disciplina dei dati personali del lavoratore*, Bari, 2000; ICHINO P., *Il contratto di lavoro, vol III, Trattato di diritto civile e commerciale* Milano 2003, pag 217 ss;

che ciò sia espressione legittima dei diritti che appartengono al datore di lavoro ovvero riconducibile all'esecuzione di obblighi derivanti dalla legge o dal contratto, presenta anche notevoli rischi per il lavoratore, se e nella misura in cui, a causa della posizione di debolezza contrattuale che lo caratterizza, questo potrebbe subire derive deprecabili, ove il datore di lavoro fosse tentato dall'utilizzare il patrimonio di informazioni possedute, in modo non strettamente funzionale alla realizzazione della causa del contratto[115].

Oltre a ciò, è interessante osservare come, se in via generale, le regole di circolazione delle informazioni sono destinate a incidere sulla distribuzione del potere nella società[116], nell'impresa, l'asimmetria di potere che generalmente caratterizza la posizione del datore e del prestatore potrebbe assumere connotazioni ingiustificatamente arbitrarie, a danno del lavoratore, se le succitate regole non fossero improntate a un canone di trasparenza e correttezza e a un adeguato contemperamento degli interessi in gioco.

Da qui la necessità di intervenire predisponendo adeguati argini e filtri normativi all'etica datoriale, a presidio della suddetta libertà e dignità del prestatore.

Il legislatore prende atto della necessità di trovare un giusto temperamento tra i diritti contrapposti proprio a partire dagli anni 70, quando con lo Statuto dei Lavoratori detta, al titolo I, norme a tutela della libertà e dignità del lavoratore, con ciò ponendo limiti specifici all'autonomia negoziale individuale e collettiva in materia di disponibilità dei diritti della persona, tra i quali in particolare quelli della riservatezza[117].

Nello specifico, tale normativa prevede all'articolo 4 il divieto di uso di «impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori»; e ancora più interessante, in questa sede, all'articolo 8 il divieto di «effettuare indagini sulle opinioni politiche,

[115] ICHINO P., *Il contratto di lavoro, vol III, Trattato di diritto civile e commerciale* Milano 2003, pag. 222 e ss.
[116] RODOTÀ S., *Tecnologie e diritti*, Bologna, 1995 pag. 46.
[117] Si osservi che lo Statuto è la prima legge italiana nella quale compare il termine riservatezza quale oggetto di un diritto della persona.

religiose e sindacali del lavoratore, nonché su fatti non rilevanti ai fini dell'attitudine professionale del lavoratore»[118].

La disciplina Statutaria pertanto, dovrà essere integrata dalla normativa generale in tema di trattamento dei dati personali.

Le due discipline non necessariamente si sovrappongono, ma in certi casi la generalità della seconda deve essere, dall'interprete, integrata e armonizzata con la specificità della prima.

Lo Statuto dei lavoratori è la sintesi di esigenze concrete e riflessioni scientifiche che si collegano tra loro, ed è piena espressione di quello che il professor Rodotà definisce il primo paradosso della *privacy*. «Si attribuì una tutela forte ad alcuni aspetti della vita privata per realizzare in realtà una protezione della sfera pubblica. Il divieto di controlli a distanza, di impropri accertamenti sanitari […] non serviva a tener nascosto qualcosa. Al contrario, venne di fatto rafforzata la libertà di agire nella sfera pubblica. […]. Ecco il paradosso: grazie allo statuto, io ottenevo anche il pieno diritto di andare regolarmente nella sezione del mio partito, di fare attività sindacale, di essere malato, di frequentare la chiesa o la sinagoga, di lasciare mia moglie e scappare con un'altra donna, senza che questo si traducesse in un elemento di discriminazione. Cioè: guadagnavo il pieno diritto di non nascondere le mie scelte di vita […]. Non per niente l'articolo 8 dello Statuto dei Lavoratori diventò il cavallo di battaglia per tutti coloro che cominciarono a impegnarsi per conquistare un nuovo diritto collettivo, quello appunto alla *privacy,* che perdeva così ogni connotato di privilegio di una borghesissima ma ormai lontana età dell'oro»[119].

La legge 1° aprile 1981 n. 121 "Nuovo ordinamento dell'Amministrazione della pubblica sicurezza"[120], agli articoli 6-12, disciplina l'uso e la segretezza dei dati personali dei singoli cittadini in possesso delle Forze dell'Ordine, istituisce il Centro elaborazione dati presso il Ministero dell'interno, ai fini del trattamento dei dati personali ritenuti utili per l'azione di lotta e prevenzione contro la delinquenza.

---

[118] ICHINO P., *Diritto alla riservatezza e diritto al segreto nel rapporto di lavoro*, Milano, 1979

[119] RODOTÀ S., Intervista su Privacy e Libertà, Roma- Bari, 2005.

[120] Legge 1 Aprile 1981, n. 121**.** Pubblicata sulla Gazzetta Ufficiale del 10 aprile 1981, n. 100.

I profili analizzati da questa legge e inerenti al tema della *privacy* riguardano la natura e l'entità dei dati e delle informazioni raccolte, nonché i controlli sugli stessi.

Nello specifico, l'articolo 6 prevede che il dipartimento della pubblica sicurezza, ai fini dell'attuazione delle direttive impartite dal Ministro dell'Interno nell'esercizio delle attribuzioni di coordinamento e di direzione unitaria in materia di ordine e di sicurezza pubblica, espleti compiti di classificazione, analisi e valutazione delle informazioni e dei dati che devono essere forniti anche dalle forze di polizia in materia di tutela dell'ordine, della sicurezza pubblica e di prevenzione e repressione della criminalità.

Si comprende dalla lettura dell'articolo come le finalità della raccolta dei dati e delle informazioni sia quella di assolvere i compiti assegnati dalla legge in materia di tutela dell'ordine, sicurezza pubblica, prevenzione e repressione della criminalità.

L'articolo 7 si occupa della natura ed entità dei dati e delle informazioni raccolte; precisa inoltre che è vietato raccogliere informazioni sui cittadini per il solo fatto della loro razza, fede religiosa, opinione politica ecc.

Con l'articolo 8 viene istituito il Centro Elaborazione dati (CED) cui spetta il compito di provvedere alla raccolta, elaborazione, classificazione e conservazione negli archivi magnetici delle informazioni e dei dati nonché alla loro comunicazione ai soggetti autorizzati.

L'accesso ai dati e alle informazioni conservati negli archivi automatizzati del Centro e la loro utilizzazione sono consentiti agli ufficiali di polizia giudiziaria appartenenti alle forze di polizia, agli ufficiali di pubblica sicurezza e ai funzionari dei servizi di sicurezza, nonché agli agenti di polizia giudiziaria delle forze di polizia debitamente autorizzati, ma anche all'autorità giudiziari per gli accertamenti necessari per i procedimenti in corso nei modi e nei limiti previsti dal codice di procedura penale. È vietata altresì ogni utilizzazione delle informazioni e dei dati predetti per finalità diverse da quelle previste dall'articolo 6, lettera a).

Il successivo articolo 11 si preoccupa di stabilire che i dati e le informazioni conservati negli archivi del Centro, possono essere utilizzati in procedimenti

giudiziari o amministrativi solo attraverso l'acquisizione delle fonti originarie.

L'unica fattispecie criminosa contenuta nella legge del 1981 è quella prevista all'articolo 12, che punisce il pubblico ufficiale che comunica o fa uso di dati e informazioni «in violazione delle disposizioni della presente legge, o al di fuori dei fini previsti dalla stessa».

Si tratta di un reato caratterizzato dalla "disobbedienza" ai precetti contenuto dalla legge e ovviamente tale fatto si aggrava quando si deve accertare se tale fatto è stato o no commesso anche al di fuori dei fini della legge stessa; la difficoltà sta nella ricerca probatoria, non di lieve entità, poiché richiede la ricerca della *ratio* sottesa alla fattispecie concreta il successivo confronto, al fine di verificarne la corrispondenza, con le *rationes legis*.

8.2 La Convenzione di Strasburgo 108/81 e la Direttiva madre 95/46

Nell'ambito dell'Unione Europea, il riconoscimento del diritto alla *privacy*, coma anche per gli altri diritti fondamentali, è avvenuto inizialmente a livello giurisprudenziale[121].

Nel frattempo, però, all'interno del Consiglio d'Europa veniva firmata una prima forma di disciplina con la Convenzione di Strasburgo n. 108 del 1981 "Sulla protezione delle persone rispetto al trattamento automatizzato di dati personali". Nonostante si tratti del primo atto normativo sovranazionale in materia di protezione dei dati personali, tale Convenzione subordinava però l'efficacia della sua entrata in vigore all'adozione di leggi interne di attuazione nei Paesi membri.

Analizzando la Convenzione, possiamo notare come nel Preambolo venga sancito il principio secondo cui la libera circolazione delle informazioni tra i popoli non può prescindere dalla tutela dei diritti e delle libertà fondamentali di ciascuno e in particolare dal diritto al rispetto della vita privata.

[121] BUTTARELLI G. *Banche dati e tutela della riservatezza: la privacy nella società dell'informazione*, Milano, 1997. Fu proprio una questione riguardante la divulgazione di informazioni sanitarie relative a un cittadino tedesco a inaugurare la giurisprudenza comunitaria sui diritti fondamentali. Sent. Stauder, 12 novembre 1969, C-26/69.

Pertanto, si comprende come premura della Convenzione, così come degli altri atti vincolanti che successivamente l'Unione Europea avrebbe per parte sua adottato, fosse quella di proteggere le persone, in particolar modo quelle fisiche, senza tuttavia compromettere il libero scambio delle informazioni.
La finalità trae diretta ispirazione dall'articolo 8 della Convenzione europea dei diritti dell'uomo[122].
Dal testo della Convenzione si cercò di far emergere come la protezione dei dati sia al tempo stesso un concetto più ampio della protezione della *privacy,* in quanto relazionato con altre libertà fondamentali, e più ristretto poiché riguarda solo le fattispecie di trattamento dei dati e non altri casi di invasione della vita privata[123].
La Convenzione n. 108 si applica a tutti i trattamenti di dati personali, effettuati sia nel settore privato che nel pubblico, e, in tale ambito, anche a quelli effettuati da autorità giudiziarie e di polizia.
L'articolo 1 recita: «Scopo della presente Convenzione è quello di garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano (protezione dei dati)».
Notiamo come la Convenzione miri a proteggere l'individuo dagli abusi che possono accompagnare la raccolta e il trattamento dei dati personali e, nel contempo, cerca di regolamentare il flusso transfrontaliero di dati personali.
La Convenzione reca un'articolata enunciazione di principi cui dovrebbero (o almeno avrebbero dovuto) conformarsi le varie legislazioni nazionali; per quanto concerne la raccolta e il trattamento dei dati personali, tali principi enunciati nella Convenzione, riguardano in particolare, la correttezza e liceità della raccolta e del trattamento automatizzato dei dati, archiviati per scopi legittimi, non destinati a un uso incompatibile con tali scopi, né

[122]Articolo 8 CEDU: «Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza».
[123] SILEONI S., *Autori delle proprie regole. I codici di condotta per il trattamento dei dati personali e il sistema delle fonti,* Padova, 2011.

conservati oltre il tempo necessario. Tali principi riguardano anche la qualità dei dati, in particolare in riferimento alla loro adeguatezza, pertinenza e non eccedenza (proporzionalità) nonché esattezza.

I principi *de quo*, sono i pilastri dell'intera normativa in materia di protezione dei dati personali, ed il fine perseguito, rimane sempre quello di assicurare il rispetto del diritto alla *privacy* degli individui nei confronti di ogni elaborazione automatizzata di dati concernenti soggetti identificati o identificabili.

Oltre a fornire garanzie sulla raccolta e sul trattamento dei dati personali, la Convenzione, in assenza di adeguate garanzie giuridiche, vieta il trattamento dei dati "sensibili", come quelli riguardati la razza, le opinioni pubbliche, la salute, la religione, l'orientamento sessuale o i precedenti giudiziari di un individuo.

Stabilisce inoltre, il diritto del cittadino ad ottenere informazioni in merito a quali dei suoi dati sono conservati ed eventualmente chiederne la rettifica, se inesatti. Le restrizioni dei diritti stabiliti nella Convenzione sono possibili solo quando sono in gioco interessi prevalenti, quali la sicurezza o la difesa dello Stato.

Infine, la Convenzione, benché preveda la libera circolazione dei dati personali tra le parti contraenti, prevede delle restrizioni alla possibilità di trasferire dati verso paesi la cui regolamentazione giuridica non fornisca una tutela equivalente.

Al fine di sviluppare ulteriormente i principi generali e le norme previste dalla Convenzione n. 108, il Comitato dei ministri del CDE ha adottato diverse raccomandazioni giuridicamente non vincolanti.

Tutti gli Stati membri dell'UE hanno ratificato la Convenzione n. 108, che nel 1999 è stata emendata per consentire all'UE di diventarne parte contraente. Nel 2001 è stato adottato un Protocollo addizionale, che introduce disposizioni in materia di flussi transfrontalieri dei dati verso le parti non contraenti, i c.d. "paesi terzi", e l'istituzione obbligatoria delle autorità di controllo nazionali per la protezione dei dati.

A seguito della decisione di modernizzare la Convenzione n. 108, una consultazione pubblica effettuata nel 2011 ha consentito di confermare i due obiettivi principali di tale lavoro: il rafforzamento della protezione della vita privata nel settore digitale e il consolidamento del meccanismo di attuazione della Convenzione.

La direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla "Tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati", viene anche definita "Direttiva madre", proprio in quanto costituisce l'ossatura fondamentale della disciplina comunitaria in merito alla protezione dei dati personali. Prevede, infatti, le disposizioni basilari per equilibrare la tutela dei diritti e delle libertà individuali, da un lato, e la promozione degli scambi e dei flussi informativi necessaria al mercato unico, dall'altro.

Pietra angolare nell'impianto della vigente normativa UE, la Direttiva è stata adottata con lo specifico fine di armonizzare il livello di tutela dei diritti delle persone riguardo al trattamento di dati personali, esigenza sorta a causa della frammentazione in materia tra i diversi paesi aderenti all'Unione.

Fondamentale la *ratio* ispiratrice, che è proprio quella di rimuovere gli ostacoli al libero scambio delle informazioni, che rappresentano, in termini economici una barriera al mercato e un costo di transazione alto, ma allo stesso tempo, imporre un equivalente livello di protezione in tutti gli Stati e simili strumenti di garanzia dei dati.

Ma essendo stata adottata, come direttiva per il mercato interno, aveva come riferimento la regolazione degli scambi commerciali e sia essa che le leggi nazionali di recepimento, concepivano la protezione dei dati personali all'interno di una relazione statica, tra il titolare e l'interessato, in una visione proprietaria del dato stesso. In tal senso, si favoriva un'applicazione formalistica. Per questa ragione, per lungo tempo, è stata vista come un mero adempimento burocratico.

Nonostante ciò, la direttiva ha introdotto il concetto che un elevato livello di protezione delle persone nel trattamento dei dati personali che li riguardano

è condizione essenziale per consentire la libera circolazione di tali dati all'interno dei Paesi dell'Unione ed ha disciplinato vari aspetti.

La Direttiva poggia su quattro pilastri metodologici, ossia i principi relativi al trattamento dei dati personali, lo sfruttamento della tecnologia a fini di protezione, la regolamentazione specifica per settore e infine, la cooperazione con i titolari del trattamento.

Percorrendone sommariamente il contenuto, aldilà di una prima parte, con un valore puramente introduttivo, dedicato alla definizione dei termini e dell'oggetto della direttiva, segue una parte sulle regole generali, in cui viene chiarito che il diritto che viene tutelato è quello al rispetto della vita privata con riguardo al trattamento dei dati personali e in cui si vieta agli Stati membri di limitare o restringere la libera circolazione dei dati per motivi connessi alla tutela garantita a norma della direttiva. Limita altresì l'ambito di applicazione, escludendo i trattamenti effettuati per ragioni di pubblica sicurezza, difesa, sicurezza nazionale, nonché i trattamenti effettuati nell'ambito di attività statale in materia penale o da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico. Fino ad arrivare poi all'analisi delle Condizioni generali di liceità dei trattamenti dei dati personali ed infine alla disciplina dei ricorsi giurisdizionali e le previsioni concernenti responsabilità e sanzioni per lo scorretto uso dei dati.

Per quanto riguarda i principi cui la Direttiva madre si fa portatrice, alcuni erano già stati accolti dalla Convenzione di Strasburgo che ne ha rappresentato il punto di partenza[124]. Accanto a una serie di principi di carattere sostanziale, come il principio teleologico secondo cui il trattamento è ammesso solo per finalità espressamente predeterminate e per quanto strettamente necessario al loro raggiungimento, ve ne sono molti altri di natura formale, quali tra i più importanti, il principio del consenso dell'interessato che sembra essere lo strumento giuridico con cui la direttiva tenta di trovare un equilibrio tra i due interessi in gioco (trattamento dei dati

[124] HUSTINX P. *The European Approach: Regulation through Protection Authorities*, 8 november 2005, speech at the colloquium Information technologies: servitude or liberty? Paris, 2005.

personali e libero scambio di informazioni)[125]. Oltre al consenso, la protezione dei dati personali viene garantita tramite l'obbligo di informazione agli interessati e di notificazione alle autorità nazionali garanti, che sono estrinsecazioni del dovere di fedeltà.

Uno degli strumenti più innovativi per la protezione dei dati personali, introdotto dalla direttiva 95/46/CE, che deve essere necessariamente menzionato, è l'obbligo di istituire, a livello nazionale, autorità garanti di controllo, che con maggiore indipendenza, efficienza e competenza rispetto agli apparati pubblici, presidiano al corretto adempimento degli obblighi e instaurino tra loro una rete di collaborazione a livello europeo.

La regolamentazione del trattamento dei dati personali è il frutto, dunque, dell'idea che la protezione dei dati non debba consistere unicamente in un complesso di regole atte a favorire il superamento delle barriere che dividono l'Europa, ma possa divenire un vero e proprio elemento costitutivo della cittadinanza in tempi di costante esposizione dell'individuo all'osservazione di innumerevoli soggetti.

Sembra pertanto, che il *leitmotiv* della direttiva sia quello di un continuo gioco di equilibri tra l'interesse delle persone fisiche a mantenere il riserbo circa le informazioni che le riguardano e quello, speculare, della comunità a utilizzare i dati, per una serie indefinita di finalità[126].

La Corte di Giustizia europea, con sede a Lussemburgo, competente sulle questioni relative all'applicazione di tale Direttiva e quindi sull'interpretazione della stessa, ne ha rilevato una serie di evidenti carenze, dovute in particolar modo all'evoluzione della tecnologia e dei trattamenti automatizzati, successivi alla sua approvazione. Per tale motivo, ed anche perché col Trattato di Lisbona il diritto alla protezione dei dati personali diventa un diritto fondamentale dei cittadini, da garantire in tutto il territorio dell'Unione, si è reso necessario sostituirla con il regolamento europeo, GDPR.

---

[125] SIMITIS S., *Il contesto giuridico e politico della tutela della privacy*, in Rivista critica del diritto privato, Bologna, 1997.

[126] SILEONI S., *Autori delle proprie regole. I codici di condotta per il trattamento dei dati personali e il sistema delle fonti*, Padova, 2011.

8.3 La legge 675/96

La normativa sulla *privacy* arriva in Italia sulla spinta dell'Unione Europea. La firma della Convenzione di Strasburgo, non aveva sortito alcun intervento legislativo di portata reale, cosa che invece realizzano il Trattato di Schengen e la Direttiva n. 95/46. Il primo, attraverso complicati meccanismi, consentendo l'eliminazione dei controlli alle frontiere e dando effettiva attuazione alla libera circolazione delle persone; la seconda imponendo agli stati il recepimento della stessa entro tre anni dalla sua entrata in vigore.

L'iter parlamentare che ha portato al varo della legge n. 675/96, "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali", si contraddistingue per la non comune celerità.

Pur non essendo formalmente una legge di recepimento della Direttiva 95/46/CE, ne ha seguito piuttosto fedelmente l'impianto nella costruzione degli adempimenti e nella definizione dei ruoli, ma ne ha ampliato notevolmente l'ambito di applicazione, con l'estensione ai trattamenti non organizzati in banche dati e ai dati delle persone giuridiche[127].

L'intento dei Parlamentari, con tale disciplina, non fu tanto quello di soffermarsi circa la strutturazione delle fattispecie ovvero il riparto tra sanzione penale e sanzione amministrativa, ma di colmare il ritardo della nostra legislazione in tema di disciplina dei dati personali.

Dunque, volendo inserire la legge 675/96 in uno dei filoni che caratterizzano la più recente produzione legislativa penale, è chiaro che l'intendimento perseguito è, però, quello dell'adempimento internazionale, volendo con ciò alludere a quelle leggi che, anche indipendentemente da altri scopi di politica interna, sono adottate per assolvere i sempre più numerosi obblighi internazionali di uniformità di disciplina, soprattutto all'interno della Comunità Europea[128]. Ciò ovviamente non contrasta, ma si aggiunge al nuovo bisogno di tutela, anche penale emerso nella nostra società in seguito

[127] IMPERIALI R., *Codice della Privacy*, Milano, 2005.
[128] PALAZZO F., Legislazione penale

al processo di tecnologizzazione della stessa, sotto il peculiare profilo della sempre maggiore consistenza del fenomeno del trattamento dei dati personali.

La legge 675/96 enuncia all'articolo 1 le finalità perseguite, identificandole, tra l'altro, nella garanzia del rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale[129].

Tale formula appare ispirata a un principio di garanzia in quanto il legislatore, nel prendere atto di una realtà nella quale il trattamento dei dati personali costituiva una costante delle relazioni sociali ed economiche, voleva che tale attività fosse comunque rispettosa delle esigenze di tutela dei diritti della persona[130] e ciò ovviamente influiva e determinava, conseguentemente, le modalità nel rispetto delle quali si sarebbe dovuto svolgere il trattamento.

Sembra si possa osservare come, per effetto della legge n. 675, acquistava rilievo un'attività, individuata dall'espressione normativa "trattamento dei dati personali", sino ad allora sostanzialmente ignota all'attenzione del legislatore e, in quanto tale, giuridicamente irrilevante se non nella misura in cui, i singoli comportamenti, che *ex post* appaiono ora alla stessa riconducibili, avessero potuto essere considerati nella diversa e sino ad allora conosciuta prospettiva dei diritti della personalità.

È interessante osservare che il fatto che la nuova normativa non «si apra con l'enunciazione del principio di libertà di informazione ma con la proclamazione delle garanzie della persona»[131], porterebbe a escludere che si tratti di una mera fonte di regolamentazione delle banche dati o del potere informatico in genere, per indirizzare invece l'interprete a una visione della

---

[129] Art. 1: «La presente legge garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale; garantisce altresì i diritti delle persone giuridiche e di ogni altro ente o associazione». Formula riportata ora nell'art. 2 comma 1 Codice privacy, con la significativa, ma ridondante, integrazione del riferimento anche al diritto alla protezione dei dati.

[130] MIRABELLI V., *Identità personale e dato personale*, in CUFFARO V., RICCIUTO V. (a cura di), Il trattamento dei dati personali, Torino, 1997.

[131] ALPA G., *La normativa sui dati personali. Modelli di lettura e problemi esegetici*, in Dir. Inf., 1997, pag. 705.

stessa come statuto a tutela di tutti quei soggetti che, con un tale potere informatico, vengano in contatto.

Fatta questa premessa, tale normativa sembra dunque, aver effettuato una scelta ben precisa nel delicato e inevitabile bilanciamento tra diritti della persona e diritto di informazione: la persona è collocata in una posizione di centralità nella scala dei valori.

L'articolo 1, comma 2 della l. 675/96 fornisce un'ampia serie di definizioni che contribuiscono a chiarire il significato e il contenuto di altrettanti termini e locuzioni che compaiono in tale testo normativo e che giocano un ruolo determinante, non solo nella normativa extra-penale, quali, ad esempio, la nozione di "trattamento", "dato personale", "titolare", "responsabile", "interessato", "comunicazione", "diffusione" e di "garante".

La tassatività di tali definizioni legislative, si pone in funzione di certezza: «nell'area della legislazione speciale, l'uso della definizione in chiave chiarificatrice sta diventando veramente imponente: probabilmente qui è il contenuto altamente tecnico della materia disciplinata a imporre un largo uso delle definizioni, senza le quali il contributo precettivo – non potendo contare sul contributo chiarificatore del senso comune – rischierebbe di rimanere insopportabilmente indeterminato»[132].

La legge 675/96 ha costituito un sistema normativo complesso, in cui si sono intrecciate disposizioni di vario genere, risultato di molteplici fattori concorrenti.

In primis il fatto che si trattasse di un testo normativo molto più articolato e ricco rispetto ad analoghi modelli comunitari cui espressamente si ispirava ed inoltre, aveva l'ambizione, implicita ma evidentissima, di «seguire, passo dopo passo, qualunque dato relativo a qualsiasi figura soggettiva presente nell'ordinamento, a partire dal momento dell'ingresso nel circuito informativo e fino alla sua uscita»[133].

[132] PALAZZO F. C. *Sulle funzioni delle norme definitorie*, in AA. VV., *Omnis definitio in iure periculosa? Il Problema delle definizioni legali nel diritto penale*. CADOPPI A. (studi coordinati da), Padova, 1996.
[133] PARDOLESI R., *Un bilancio interlocutorio e le prospettive sulla legge Privacy,* Roma, 1998.

La l. 675/96 disciplinava qualsiasi operazione avente ad oggetto dati suscettibili di essere associati a una persona fisica o giuridica, indipendentemente dal mezzo a tal fine utilizzato.

Si tratta della disciplina più ampia e rigorosa di tale fenomeno attuabile senza ledere i fondamentali principi di libertà dell'iniziativa economica e di diritto all'informazione.

Qualsiasi trattamento di dati personali avrebbe dovuto essere effettuato secondo i principi di liceità e correttezza del trattamento, limitazione degli scopi[134], esattezza, completezza, pertinenza e aggiornamento dei dati trattati; ma ancora, non eccedenza[135], ma soprattutto nel rispetto del principio del c.d. "diritto all'oblio"[136].

La definizione di questi principi fondamentali, aveva, contrariamente alla generica affermazione contenuta all'articolo 1 della stessa legge, valore precettivo, in considerazione del fatto che il titolare del trattamento che ne avesse violato il contenuto, ponendo conseguentemente in essere una condotta di trattamento illecito, sarebbe stato tenuto a risarcire il danno eventualmente cagionato dalla sua condotta, da computarsi anche con riferimento al danno morale.

È importante mettere in evidenza come l'articolazione e la ricchezza del dato normativo porta a riconsiderare, in tale normativa, l'originaria nozione di *privacy*, dilatandone il significato «fino a ricomprendere in essa l'insieme delle regole sulla circolazione delle informazioni personali, rafforzando la rilevanza costituzionale di tale diritto»[137].

Nel momento in cui si prese coscienza che la *ratio* della disciplina non poteva essere ricondotta meramente al principio del divieto di trattamento dei dati personali, ma che, anzi, proprio il trattamento costituiva il logico presupposto della regolamentazione, acquistavano allora rilievo ulteriori e non secondarie

[134] Per tale intendendosi che i dati avrebbero dovuto essere raccolti per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi.
[135] I dati non avrebbero dovuto essere eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati.
[136] Per tale intendendosi il principio in base al quale i dati non avrebbero dovuto essere trattati per un periodo superiore a quello strettamente necessario per gli scopi per i quali erano stati raccolti e trattati.
[137] RODOTÀ S., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in Riv. Crit. Dir. Priv., 1997, p. 558.

prescrizioni normative, dedicate rispettivamente al consenso dell'interessato (articoli 11, 12 e 20), all'informativa a lui dovuta (articolo 10), ai diritti riconosciutagli (articolo 13), alle regole che sovraintendono il trattamento (articolo 9).

Da una lettura complessiva e non frettolosa dell'intero impianto normativo della legge n. 675, integrato da un complesso di indicazioni e dai codici deontologici, si trae la ragionevole convinzione, che in realtà, la vicenda del trattamento dei dati personali fosse riconducibile a uno schema che non trovava quale esclusivo punto di riferimento l'interessato, quale soggetto del quale difendere il diritto e al quale somministrare la tutela, ma a una ponderata valutazione degli interessi coinvolti nell'attività di trattamento, secondo un criterio che privilegiava l'esigenza di uno svolgimento del trattamento improntato ai principi di lealtà e correttezza, non diversamente da quanto accade nella disciplina dell'obbligazione.

In tale prospettiva sembra che, il trattamento dei dati personali, determina l'instaurazione di un rapporto obbligatorio tra titolare e interessato e trova dunque nella disciplina del rapporto, con le sue peculiarità, il referente logico giuridico per la valutazione della condotta dei soggetti coinvolti.

Quanto alla tutela in sede penale del diritto al controllo esclusivo dei propri dati personali, la legge contempla varie disposizioni.

La scelta di censurare penalmente la violazione di alcune delle disposizioni della legge medesima ha ricevuto diversi tipi di critiche soprattutto per la controtendenza dell'ordinamento alla depenalizzazione degli illeciti di lieve entità. A ben vedere, però, come chiarisce anche lo stesso estensore della legge, tale opzione normativa risultava obbligata al fine di onorare il principio che nel diritto penale chiamiamo "di effettività", il quale, oltre che cogente nell'ordinamento interno, era ribadito a livello internazionale e comunitario laddove sia la Convenzione di Strasburgo del 1981, sia la Direttiva europea del 1995 in materia di trattamento di dati personali imponevano agli Stati membri l'adozione di sanzioni appropriate.

Tale principio è tradizionalmente inteso come l'attitudine della pena a raggiungere l'obiettivo suo proprio identificato nella (apprezzabile) riduzione degli illeciti a causa dei quali la sanzione è predisposta.

È evidente che il principio di effettività non sarebbe certo stato appagato dalla previsione di sanzioni a carattere esclusivamente pecuniario, ben lontane dal realizzare un effetto di prevenzione generale o speciale quantomeno nei confronti delle pubbliche amministrazioni e delle imprese di estese dimensioni.

Le fattispecie penali introdotte dalla legge 675/96 sembrerebbero da ascrivere alla categoria dei c.d. "reati propri", che possono cioè, essere commessi solo da chi possieda una data qualifica o occupi una certa posizione.

I modelli forse più refrattari rispetto a un siffatto inquadramento sistematico sono rappresentati dai delitti di trattamento illecito di dati personali (articolo 35, commi I e II).

Peraltro, ad onta del generico "chiunque" che compare nella formulazione di tali ultimi delitti, essi possono essere realizzati soltanto dai soggetti obbligati al rispetto delle specifiche norme di cui alla legge in oggetto: pertanto, anche il soggetto agente delle fattispecie di illecito trattamento, deve caratterizzarsi in modo da risultare ricompreso tra i peculiari destinatari del precetto penale e varia a seconda delle norme extra-penali della stessa legge 675/96, cui rinvia l'articolo 35[138].

Tutte le altre fattispecie di cui agli articoli 34-36-37, rispettivamente "Omessa o incompleta notificazione", "Omessa adozione di misure necessarie alla sicurezza dei dati", "Inosservanza dei provvedimenti del Garante", sono invece contraddistinte in punto di soggetto attivo dalla locuzione «chiunque essendovi tenuto…». Il soggetto obbligato va, anche in questi casi, logicamente individuato, facendo riferimento alle disposizioni della legge 675/96, di volta in volta richiamate.

[138] Si tenga conto, per esempio, con riguardo all'articolo 35 comma 1, che gli articoli 11 e 20 riguardano il trattamento (ovvero in particolare la comunicazione e la diffusione) di dati personali da parte di privati o enti pubblici economici, mentre l'articolo 27 concerne il trattamento da parte di soggetti pubblici (esclusi gli enti pubblici economici).

Se l'intento del legislatore era, come pare, quello di tutelare penalmente un bene primario, quale la sfera della vita privata, per parafrasare un passo della Relazione, ovvero la riservatezza in rapporto ai dati personali, ebbene, l'obiettivo non sembra però essere stato centrato. Nel tipicizzare gli illeciti penali, il legislatore sembra non aver saputo approfittare della circostanza che, nel caso di specie, le nuove esigenze in materia di tutela dei dati personali, trovano un diretto aggancio a valori di sicuro rilievo e dignità costituzionali, quali, appunto, quelli che ruotano attorno al concetto di *privacy* del soggetto.

Una via più coraggiosa sarebbe forse stata quella di demandare alla legge 675 il ruolo di legge speciale di settore per ciò che concerne il trattamento dei dati personali, con le relative sanzioni amministrative, e di disporre attraverso la stessa, l'inserimento nel corpus del codice penale di disposizioni penali tali da incentrare la tutela sugli interessi sostanziali in gioco.

Viceversa, l'attuale sistema sanzionatorio penale disegnato dalla legge 675 largamente imperniato sulla protezione di funzioni strumentali rischia non solo di esporsi all'obiezione di una formalizzazione e di un'anticipazione della tutela eccessiva, ma anche di contribuire ad un processo di inflazione legislativa, la cui intollerabilità è stata puntualmente denunciata dalla più attenta dottrina penalistica[139].

È interessante concludere con un'osservazione piuttosto critica posta in evidenza da autorevole dottrina, che mette in evidenza come, in seguito a un'analisi di tale disciplina da un'ottica penalistica, il penalista stesso, può salutare con favore l'ingresso nell'ordinamento della legge 675/96, ove si consideri che effettivamente tale normativa viene a colmare una lacuna diffusamente avvertita in una materia in cui si trovano implicati interessi per lo meno astrattamente meritevoli di protezione penale, a prescindere dalla concreta strutturazione delle fattispecie e dalle tecniche di tutela adottate. Veneziani ritiene inoltre che, quanto poi alla tecnica di formulazione delle singole fattispecie si è detto di come queste "scontino" il fatto di essere dettate quali appendici sanzionatorie rispetto a norme strutturate per altri fini.

[139] PALAZZO F. C., Legislazione penale, cit. 24, PALIERO C. E., «Minima non curat praetor».

Nel caso della legge qui osservata, gli inconvenienti di siffatto, non certo inusuale, modo di legiferare sono risultati amplificati giacché in sede extra-penale sono state attuate scelte di tipo "generalista", equiparando nella disciplina situazioni anche molto disomogenee tra loro. La suddetta opzione "generalista" da un lato, e dall'altro la penalizzazione quasi "a tappeto" di cui agli articoli 34 e seguenti hanno comportato non lievi scosse ai principi di proporzione ed *extrema ratio,* ai quali pure si vorrebbe sempre informato l'intervento di un saggio ed accorto legislatore penale.

Sin da una prima lettura di tali principi e criteri, è facile rendersi conto della non esaustività della disciplina dettata dalla legge 675/96 e della necessità di apposite ulteriori normative di settore, da porre in essere, appunto, con lo strumento del Decreto legislativo.

Concludo tale analisi, ribadendo, ancora una volta, che l'oggetto della tutela prestata da tale normativa sui dati personali non è stato limitato al diritto di ciascuno ad esigere che i trattamenti automatizzati dei suoi dati personali avvengano nel rispetto di principi e regole, ma ha conglobato una parte rilevante dei c.d. diritti della personalità. Questo approccio è ancor più evidente nel Codice *Privacy.*

8.4 Il Codice della privacy 196/2003

Su proposta del Presidente del Consiglio e dei Ministri per la funzione pubblica e per le politiche comunitarie, il 27 giugno 2003 è stato definitivamente approvato dal Consiglio dei Ministri il decreto legislativo n. 196 Testo unico in materia dei dati personali, denominato Codice[140] della *privacy,* pubblicato nella Gazzetta ufficiale del 29 luglio 2003 e «ispirato all'introduzione di nuove garanzie per i cittadini, alla razionalizzazione delle norme esistenti e alla semplificazione»[141].

[140] La scelta di tale denominazione viene motivata in sede di relazione al decreto legislativo in esame, con l'esigenza da parte del legislatore delegato, di accogliere le indicazioni promananti dal disegno di legge di semplificazione 2001 in tema di riassetto normativo e di codificazione, già approvato dalle Camere.

[141] Come può evincersi dalla Relazione di accompagnamento al d.lgs. 196/2003.

L'intervento è risultato quanto mai opportuno, essendo note le problematiche sorte per l'applicazione della precedente legge regolatrice della materia, in parte determinate dall'urgenza della sua formulazione ed emanazione.

I 42 articoli cui si componeva il testo originario sono espansi nel codice della *privacy* a ben 186 disposizioni, in larga parte chiarificatrici della pregressa disciplina e in misura considerevole innovatrici[142].

Il codice rappresenta il tentativo tangibile di dominare la complessità della materia, la cui ambizione principale è di ricondurre a un ordine sistematico la molteplicità di ambiti normativi, ad una *reductio ad unum* della disciplina *in subiecta materia*, nella quale emerge in modo problematico la tutela della riservatezza.

Conformemente agli orientamenti espressi dal disegno di legge di semplificazione 2001, il codice lungi dall'esaurirsi in una ricognizione meramente compilativa delle disposizioni previgenti, ma presuppone ponderati interventi di armonizzazione e adeguamento delle stesse, nel rispetto delle scelte di fondo operate dall'organo legislativo, dei principi enunciati dalla legge delega, della normativa internazionale e comunitaria di riferimento, nonché con adeguata considerazione dei risvolti applicativi, derivanti dalle modifiche normative.

L'adozione di un testo unico di matrice puramente legislativa anziché mista, oppure *a fortiori* regolamentare *tout court*, si rivela più consona al rango del bene giuridico protetto delle norme introdotte, nonché alle finalità perseguite dall'intervento normativo in questione[143].

Il Codice *privacy* [144] costituisce non solo una raccolta delle diverse norme in tema di tutela dei dati personali, ma anche un aggiornamento e un'integrazione delle stesse sulla base delle esperienze maturate in questi anni anche alla luce dell'attività del Garante per la protezione dei dati

[142] Basti pensare alla prima parte definitoria con l'introduzione del nuovo concetto di diritto ai dati personali, CORRIAS LUCENTE G. *in La nuova normativa penale a tutela dei dati personali*.

[143] MANNA A. *Prime osservazioni sul testo unico in materia di protezione dei dati personali: profili penalistici.*

[144] Sull'applicazione della normativa vigila il Garante *Privacy*, istituito sin dalla L. 675/1996, poi confermata anche dal Testo Unico del 2003.

personali. Vari sono gli adempimenti previsti, alcuni dei quali erano già stati previsti dalla normativa precedente, altri sono stati introdotti *ex novo*.

La sua struttura appare organica e razionale: si compone di tre parti: Disposizioni generali (articoli 1- 45), Disposizioni relative a specifici settori (articoli 46- 140) e Tutela dell'interessato e sanzioni (articoli 141- 186); con in più, l'aggiunta di tre allegati[145]. L'*incipit* concerne una parte generale, in cui è possibile cogliere la trama normativa della legge 675/96, ove sono definite e disciplinate le condizioni di liceità del trattamento, le misure di sicurezza, l'informativa e il consenso. Una parte speciale dedicata invece ai singoli settori di disciplina, contiene deroghe e specificazioni della disciplina generale, recependo tutti i satelliti normativi costituiti dalle numerose riforme e integrazioni della legge 675/96. L'ultima parte è dedicata alla tutela giurisdizionale e alternativa dell'interessato e alle sanzioni[146].

Il decreto fu concepito per tutelare il diritto del singolo sui propri dati personali e, conseguentemente, alla disciplina delle diverse operazioni di gestione (tecnicamente "trattamento") dei dati, riguardanti la raccolta, l'elaborazione, il raffronto, la cancellazione, la modificazione, la comunicazione o la diffusione degli stessi.

Gli articoli 1, 2 e 3 del codice mettono in evidenza la ragionevolezza come criterio guida e paradigma metodologico di analisi delle condizioni e dei limiti di liceità del trattamento dei dati personali[147].

All'articolo 1 del testo unico viene riconosciuto il diritto assoluto di ciascuno sui propri dati, in cui si afferma testualmente, con una particolare enfasi declamatoria da parte del legislatore delegato: «Chiunque ha diritto alla protezione dei dati personali che lo riguardano». Tale diritto pertiene i diritti della personalità ed è sicuramente autonomo rispetto al più generale diritto alla riservatezza di cui all'articolo 1 della L. 675/1996.

---

[145] I tre allegati aggiunti al codice della privacy sono: il codice di deontologia, il disciplinare tecnico in materia di misure minime di sicurezza e disposizioni in materia di trattamenti non occasionali in ambito giudiziario o per fini di polizia.

[146] TORRE V. *La gestione del rischio nella disciplina del trattamento dei dati personali,* pp. 238 ss, in PICOTTI L., *Il diritto penale dell'informatica nell'epoca di internet,* Padova, 2004.

[147] PALAZZO F., *Il principio di determinatezza nel diritto penale*, Milano, 1979.

L'articolo 2 statuisce che «il codice è diretto a garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato e in particolare del diritto alla riservatezza e del nuovo diritto alla protezione dei dati personali».

Lo scopo della normativa era quello di evitare che il trattamento dei dati avvenisse senza il consenso dell'avente diritto, ovvero in modo da recargli pregiudizio. Vennero a tal scopo definiti i diritti degli interessati, la modalità di raccolta e i requisiti dei dati, gli obblighi di chi raccoglie, detiene o tratta dati personali e le responsabilità e sanzioni in caso di danni.

Giova ricordare che facendo riferimento al trattamento dei dati, il Codice della *privacy* individua due distinte categorie di soggetti: passivi e attivi; nella prima categoria comprendiamo l'interessato, cioè colui (persona fisica o giuridica, ente o associazione) al quale si riferiscono i dati personali[148] e nella seconda tutti coloro che eseguono le attività ricomprese nel trattamento medesimo.

Il diretto riferimento operato dall'articolo 2, all' "interessato", elemento normativo suscettibile di una più ampia applicazione rispetto alla dizione «persone fisiche o giuridiche» di cui al primo comma dell'articolo 1 della vecchia legge 675/96, consente la tutela di diritti fondamentali eventualmente riconosciuti in altra sede dell'ordinamento, anche a soggetti diversi da persone fisico-giuridiche[149].

Nella medesima prospettiva, l'articolo 3 introduce il "principio di necessità" nel trattamento dei dati personali, alla stregua del quale, sin dal momento della loro configurazione, i sistemi informativi e i *software* devono essere predisposti in modo da assicurare che i dati personali o identificativi siano utilizzati solo allorché indispensabili per il perseguimento delle finalità consentite, e non invece quando sussista la possibilità di raggiungere i medesimi obiettivi mediante l'uso di dati anonimi, o che comunque permettano di identificare l'interessato in maniera meno invasiva, più

[148] Articolo 4, comma 1, lettera i) Codice privacy: Ai fini del presente codice si intende per: "*interessato*", la persona fisica, cui si riferiscono i dati personali.

[149] MANNA A. *Prime osservazioni sul testo unico in materia di protezione dei dati personali: profili penalistici.*

circoscritta. Tale principio integra perfettamente i principi di pertinenza e non eccedenza già operanti in relazione ai dati *ex* articolo 9 della L. 675/96.

Il codice ha provveduto a chiarire specifiche definizioni, alcune delle quali già contenute nella legge 675/96.

Si identifica nel titolare del trattamento[150] «la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione o organismo cui competono, anche unitamente ad altro titolare le decisioni in ordine alle finalità e alle modalità del trattamento dei dati personali, nonché agli strumenti utilizzati, ivi compreso il profilo della sicurezza».

Un'ulteriore figura prevista dal Codice della *privacy*, che è necessario menzionare, è quella del responsabile, ossia «la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione o organismo preposto dal titolare al trattamento dei dati personali»[151]. Al responsabile, la cui nomina da parte del titolare è facoltativa (articolo 29, comma 1), compete di assicurare il costante rispetto della normativa da parte del personale dell'impresa, ente o amministrazione.

Il terzo ed ultimo soggetto attivo del trattamento dei dati è rappresentato dall'incaricato, «persona fisica autorizzata dal titolare o, laddove designato, dal responsabile a compiere operazioni di trattamento»[152].

Ogni titolare, sia pubblico che privato, deve rispettare precise modalità di raccolta e di elaborazione dei dati personali come stabilito dall'articolo 11 del codice della *privacy.*

In particolare, i dati oggetto di trattamento devono essere: trattati in modo lecito e corretto; raccolti e registrati per scopi determinati, espliciti e

[150] Articolo 4, comma 1, lettera f) Codice privacy: Ai fini del presente codice si intende per: "*titolare*", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

[151] Articolo 4, comma 1, lettera g) Codice privacy: Ai fini del presente codice si intende per: g) "*responsabile*", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

[152] Articolo 4, comma 1, lettera h) Codice privacy: Ai fini del presente codice si intende per "*incaricati*", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

legittimi; esatti e aggiornati; pertinenti, completi e non eccedenti rispetto alla finalità del trattamento; conservati per un periodo di tempo non superiore a quello strettamente necessario alle finalità del trattamento.

Il codice della *privacy* dedica l'articolo 13[153] alla disciplina generale dell'informativa, necessaria per la raccolta del consenso al trattamento dei dati. L'interessato o la persona presso la quale sono raccolti i dati personali devono essere previamente informati oralmente o per iscritto circa le finalità e modalità del trattamento, la natura obbligatoria o facoltativa del conferimento dei dati, le conseguenze di un eventuale rifiuto, i soggetti ai quali i dati possono essere comunicati, gli ambiti di diffusione dei medesimi, i diritti ed, infine, gli estremi identificativi del/i titolare/i e dell'eventuale/i responsabile/i e più specificamente, qualora designato, quello deputato per il riscontro dei diritti dell'Interessato.

Nel contesto generale, per i soggetti privati e gli enti pubblici economici il trattamento dei dati personali è consentito solo previo consenso informato

[153] Articolo 13 Codice *privacy*: «L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa: a) le finalità e le modalità del trattamento cui sono destinati i dati; b) la natura obbligatoria o facoltativa del conferimento dei dati; c) le conseguenze di un eventuale rifiuto di rispondere; d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi; e) i diritti di cui all'articolo 7; f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile. L'informativa di cui al comma 1 contiene anche gli elementi previsti da specifiche disposizioni del presente codice e può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati. Il Garante può individuare con proprio provvedimento modalità semplificate per l'informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico. Se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione. La disposizione di cui al comma 4 non si applica quando: a) i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria; b) i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento; c) l'informativa all'interessato comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate. dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile».

espresso dall'interessato. Nel caso di dati sensibili tale consenso deve essere prestato esclusivamente in forma scritta.

Per gli enti pubblici non economici il trattamento dei dati personali e sensibili è consentito solo per lo svolgimento delle funzioni istituzionali.

Qualunque dato deve essere custodito in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, nonché di accesso non autorizzato o di trattamento non consentito e non conforme alle finalità di raccolta. A tale scopo devono essere predisposte tutte le idonee misure di sicurezza in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento. Eventuali danni subiti dagli interessati dovranno ottenere risarcimento.

La protezione dei dati personali attraverso adeguate misure di sicurezza ricorre in più parti del Codice: nell'articolo 4 vengono elencate le definizioni con l'obiettivo di evitare o quantomeno ridurre eventuali equivoci interpretativi; il Titolo V è invece una parte completamente dedicata alla sicurezza dei dati e dei sistemi in cui vengono prescritti gli obblighi di sicurezza, i particolari titolari, le misure minime per i trattamenti svolti con l'ausilio di strumenti elettronici o informatici e l'obbligo di aggiornamento di tali misure.

Le misure minime di sicurezza, volte ad assicurare un livello minimo di protezione dei dati (articolo 33) sono distinte per i trattamenti effettuati con (articolo 34) o senza (articolo 35) l'utilizzo di strumenti elettronici.

Il trattamento dei dati tramite elaboratori centrali, reti telematiche o, più comunemente, *personal computer* è consentito solo qualora si adottino sistemi di autenticazione informatica, di gestione delle credenziali di autenticazione (codice identificativo, parola chiave, caratteristica biometrica), di autorizzazione, di aggiornamento periodico dell'ambito del trattamento, di protezione degli strumenti elettronici, di custodia di copie di sicurezza e ripristino dati.

La terza parte del Codice disciplina la tutela dell'interessato e le sanzioni relative alle disposizioni in materia di *privacy.* L'articolo 141[154] richiama le forme di tutela cui dispone l'interessato che può rivolgersi al Garante mediante reclamo circostanziato, segnalazione o ricorso.

Dopo di che si procede con un riordino del sistema sanzionatorio relativo alle violazioni delle regole in materia di dati personali. Il titolo terzo, il quale se ne occupa, suddistinto in due capi: condotte punite con sanzione amministrativa (articoli 161- 166) e illeciti penali (articoli 167-172).

– Per una analisi dettagliata della tutela penale, si rimanda al capitolo due e al capitolo tre, rispettivamente *ante e post General Data Protection Regulation*–.

In questa sede è interessante segnalare come, sul piano della tecnica di strutturazione delle fattispecie costituenti sia illecito amministrativo che penale, il legislatore per individuare la condotta sanzionata, ha scelto di adottare la tecnica del rinvio a norme extra-penali (per la maggior parte rappresentate da altre disposizioni del codice).

Tale tecnica, ricalca nella sostanza quella delle c.d. norme penali in bianco, ragion per cui, si espone ad alcuni rilievi critici sul versante del rispetto del principio di legalità.

In conclusione, è lecito affermare che, sicuramente, l'introduzione del codice *privacy* ha determinato una vera e propria rivoluzione in tutti i settori della società civile, (anche se, soprattutto per quanto riguarda le pubbliche amministrazioni, l'applicazione delle sue disposizioni è stata piuttosto lacunosa e incompleta) e, tale normativa se bene applicata, non rappresenta più solo un insieme di norme ed un ulteriore fardello burocratico, ma diventa vero e proprio strumento della qualità al fine di contribuire a quel "salto

[154] Articolo 141 Codice privacy: «L'interessato può rivolgersi al Garante: a) mediante reclamo circostanziato nei modi previsti dall'articolo 142, per rappresentare una violazione della disciplina rilevante in materia di trattamento di dati personali; b) mediante segnalazione, se non è possibile presentare un reclamo circostanziato ai sensi della lettera a), al fine di sollecitare un controllo da parte del Garante sulla disciplina medesima; c) mediante ricorso, se intende far valere gli specifici diritti di cui all'articolo 7 secondo le modalità e per conseguire gli effetti previsti nella sezione III del presente capo».

culturale" che da molti è considerato indispensabile, affinché il diritto alla protezione dei dati diventi patrimonio di tutti.

Ma, nonostante ciò e nonostante il più grande merito che si riconosca al codice *privacy* sia quello di porsi come una guida pratica con la precisa finalità di supportare i soggetti del trattamento nell'espletamento degli adempimenti richiesti dalla normativa, bisogna, purtroppo riconoscere che le difficoltà sono notevoli, in quanto gli adempimenti sono alquanto articolati e richiedono un elevato tasso tecnico, non alla portata di tutti.

8.5 Dal GDPR fino al D.lgs. 101/2018

Il 4 maggio 2016 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 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, che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

Il regolamento, nella versione inglese noto come *General Data Protection Regulation*, *GDPR*, ha introdotto alcune novità in materia di *privacy* e trattamento dei dati[155].

La procedura legislativa condotta dinanzi al Parlamento Europeo e finalizzata all'emanazione del Regolamento 679 (da ora Regolamento o acronimo inglese, *GDPR*) ha avuto inizio nel 2012.

Il motivo per il quale l'Unione Europea si sia dotata di un nuovo quadro normativo in tema di *data protection* si evince dal fatto che l'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo e tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione.

[155] Tale regolamento, concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati, è entrato in vigore il 24.5.2016, ma è stato applicabile dal 25.5.2018.

Questo «quadro più solido» è oggi rappresentato dal Regolamento. Basti pensare al *considerandum* n.13, secondo il quale, al fine di «assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possano ostacolare la libera circolazione dei dati personali nel mercato interno, è necessario un regolamento che garantisca certezza del diritto».

Pertanto, possiamo affermare che la *ratio* ispiratrice del regolamento si possa identificare nel tentativo di dare pari dignità ai diritti degli individui che intendano proteggere i propri dati personali in tutta l'Unione Europea attraverso una serie omogenea di principi e regole uniformi, da applicare in ogni stato membro, superando le asimmetrie che si sono riscontrate nel recepimento della Direttiva del 1996 modo omogeneo, con l'obiettivo di consentire una maggiore e più efficace collaborazione tra le Autorità di protezione dati e un'armonizzazione delle procedure. Questo regolamento ha messo in piedi un sistema di discipline che affronta il tema della protezione dei dati rovesciando il rapporto abituale che voleva interventi a posteriori e non preventivi[156].

In estrema sintesi, «il regolamento introduce regole più chiare in materia di informativa e consenso, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti, stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'unione europea e per i casi di violazione dei dati personali c.d. "*data breach*"»[157].

Il Regolamento consta di ben 173 considerando e 99 articoli suddivisi in 11 capitoli.

Le disposizioni contenute nel Regolamento (articolo 1 par. 1) riguardano la protezione delle persone fisiche (così come per il Codice della *privacy*, che esclude il trattamento dei dati relativi a persone giuridiche) con riferimento al trattamento dei dati personali e alla libera circolazione di tali dati.

Per quanto riguarda l'ambito applicativo, il regolamento non trova applicazione per «i trattamenti di dati personali effettuati da una persona

[156] "Proteggiamo i dati, sono la nostra vita", Intervista ad Antonello Soro, Presidente del Garante per la protezione dei dati personali.

[157] PIZZETTI F. *Privacy e il diritto europeo alla protezione dei dati personali* pp. 147 ss.

fisica per l'esercizio di attività a carattere esclusivamente personale o domestico»[158], mentre si applica anche «al trattamento interamente o parzialmente automatizzato di dati personali, in maniera parziale o totale, di dati personali e trattamento non automatizzato di dati personali contenuti in un archivio o destinati a essere ivi inclusi»[159].

Gli aspetti di interesse per l'interprete, introdotti dal nuovo Regolamento, sono molteplici. Si pensi al diritto all'oblio (articolo 17), al diritto alla portabilità dei dati (articolo 20), al diritto di accesso (articolo 15), al registro delle attività di trattamento (articolo 30), al meccanismo dello sportello unico (articolo 60), alla disciplina sui *social* e minori (articolo 8), ma in particolar modo al nuovo impianto sanzionatorio (articolo 83).

Ma gli architravi su cui poggia tutto il sistema del Regolamento, e che sono alla base del trattamento dei dati sono i seguenti: il principio di trasparenza, la garanzia del diritto all'oblio e il principio di *accountability.*

Il principio della trasparenza nell'ottica del *GDPR* impone che le informazioni destinate al pubblico o all'interessato siano facilmente accessibili e di facile comprensione e che sia utilizzato un linguaggio semplice e chiaro. Ciò ad esempio è particolarmente utile in situazioni quali la pubblicità *on line*, in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia difficile per l'interessato comprendere se vengono raccolti dati personali, da chi e a quale scopo. Si fa, inoltre, riferimento in particolare all'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento equo e trasparente con riguardo agli interessati e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano.

[158] Regolamento UE 679/2016, art. 2 comma 2 lett c.

[159] Regolamento UE 679/2016, art.1. Per quanto riguarda l'ambito applicativo territoriale, il regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare di trattamento o di un responsabile del trattamento nell'Unione, nonché al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare o da un responsabile del trattamento che non è stabilito nell'unione, quando le attività di trattamento riguardano l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato, oppure il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

Le finalità specifiche del trattamento dei dati devono essere esplicite e legittime e precisate al momento della raccolta.

I dati devono essere adeguati, pertinenti e limitati a quanto necessario per le finalità del trattamento; da qui l'obbligo, in particolare, di garantire che il periodo di conservazione dei dati sia limitato al minimo necessario. I dati personali, inoltre, devono essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi.

Il diritto all'oblio consiste nel «diritto di ottenere la cancellazione dei propri dati quando sia venuta meno la finalità per la quale se ne è consentito l'uso e soprattutto quando non sussistono più i motivi che possono aver giustificato la loro diffusione»[160]. Al fine di dare attuazione a tale diritto, il regolamento sancisce all'articolo 16 il diritto di rettifica, ossia il diritto dell'interessato «di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo» e impone agli operatori di «prevedere modalità volte ad agevolare l'esercizio, da parte dell'interessato, consentendo l'inoltro delle richieste per via elettronica e senza costi a carico del richiedente»[161].

Il fondamentale principio di *accountability* che può essere (non facilmente) traducibile come principio di resposanbilizzazione e obbligo di rendicontazione, nasce in ambito aziendale per indicare i doveri di trasparenza «intesa come garanzia della completa accessibilità alle informazioni agli utenti», di resposività, «intesa come la capacità di rendere conto di scelte, comportamenti e azioni» e di *compliance* «intesa come capacità di far rispettare le norme»[162].

---

[160] PIZZETTI F. *Il prisma del diritto all'oblio* (a cura di), *Il caso del diritto all'oblio,* Torino 2013, pp. 41-42, in cui si evidenzia come la preoccupazione per la permanenza nel web oltre la volontà dell'interessato delle informazioni che lo riguardano sia accentuata dai meccanismi di cattura e decontestualizzazione delle stesse da parte dei motori di ricerca.

[161] Al considerandum n. 66 è previsto che «per rafforzare il diritto all'oblio nell'ambiente online, è opportuno che il diritto di cancellazione sia esteso in modo tale da obbligare il titolare del trattamento che ha pubblicato dati personali a informare i titolari del trattamento che trattano tali dati personali, di cancellare qualsiasi link verso tali dati personali o copia o riproduzione di detti dati. Nel fare ciò, è opportuno che il titolare del trattamento adotti misure ragionevoli tenendo conto della tecnologia disponibile e dei mezzi a disposizone del titolare del trattamento, comprese misure tecniche, per informare della richiesta dell'interessato i titolari del trattamento che trattano i dati personali».

[162] IASELLI M. *Privacy: cosa cambia con il nuovo regolamento europeo* p.9; BISTOLFI C. *Le obbligazioni di compliance in materia di protezione dei dati,* BOLOGNINI L., PELINO E., BISTOLFI C (a cura di), *Il*

Il principio di *accountability* costituisce uno dei pilastri su cui si fonda il *GDPR* ed è recepito all'articolo 24, in forza 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», tali misure «sono riesaminate e aggiornate qualora necessario»[163].

Si tratta di un principio sviluppato nel corso della trentaduesima conferenza in tema di *privacy*, svoltasi a Gerusalemme nel 2010. Con il termine *accountability* si fa riferimento proprio alla necessità in capo al titolare del trattamento di introdurre dei meccanismi di resposanbilizzazione interna, mediante l'elaborazione di un sistema documentale di gestione della *privacy*, anche attraverso l'elaborazione di specifici modelli organizzativi, analoghi a quelli utilizzati nell'applicazione della disciplina *ex* D.lgs. 231/2001.

Il soggetto preposto dalla disciplina comunitaria a sovraintendere un determinato modello di gestione *privacy* è il *Data Protection Officer*, figura prevista agli articoli 37-39 del Regolamento, molto importante, obbligatoria in determinati casi e in grado di fornire tutta l'assistenza necessaria per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali.

È importante rilevare come, rispetto alla direttiva 95/46/CE il cui obiettivo era principalmente quello di tutelare le persone nei confronti dei titolari del trattamento dei dati personali, l'obiettivo cui mira il *GDPR* è quello di prevenire e sanzionare severamente i trattamenti dei dati illegittimi, anche a prescindere dalla necessità di tutela dei singoli cui i dati si riferiscono. Ciò dimostra come nella nuova normativa europea, la protezione dei dati personali non sia più concepita solo come diritto fondamentale

Regolamento privacy europeo, pp 323 e ss; PIZZETTI F. *Privacy e il diritto europeo alla protezione dei dati personali* pp 282 e ss.

[163]LAMANUZZI M. *Diritto penale e trattamento dei dati personali. Codice della privacy, novità introdotte dal regolamento UE 2016/679 e nuove responsabilità per gli enti* in JusOnline, 2017..

dell'individuo, ma anche, se non primariamente, come interesse della collettività, in piena sintonia con l'ormai consolidata interpretazione del diritto alla protezione dei dati personali. In particolare, con riferimento al principio di *accountability*, la Direttiva si limitava a stabilire che il responsabile del trattamento è tenuto a rispettare le disposizioni di cui all'articolo 6[164], volte a garantire la liceità del trattamento dei dati. Il Regolamento invece, attribuisce al titolare o al responsabile o all'incaricato del trattamento, un ruolo proattivo, ossia quello di assumere tutte le misure tecniche e organizzative necessarie a prevenire il rischio di violazioni in materia di trattamento dei dati personali e altresì a rilevare queste ultime, in modo tale da poter dimostrare di aver fatto tutto il possibile per assicurare la *compliance* dei trattamenti[165].

Vale la pena sottolineare che in Italia, come in altri Paesi, si è provveduto a ridefinire il ruolo del Garante *Privacy* rafforzandone la struttura, identificandone i poteri ed i controlli da realizzare all'interno di quella che è stata poi rinominata Autorità Garante per la Protezione dei Dati Personali.

Rispetto al Codice della *privacy*, nel Regolamento vi sono alcune importanti novità, che è necessario brevemente analizzare, quali: la previsione di una più specifica definizione dei rapporti fra titolare e responsabile, che deve avvenire mediante il ricorso a un contratto (o altro atto giuridico), in forma scritta (anche in formato elettronico), con uno specifico contenuto; il responsabile del trattamento può ricorrere ad un altro responsabile solo su autorizzazione scritta (specifica o generale) del titolare del trattamento; è resa

[164] L'art. 6 della direttiva 95/46/CE prevede che il responsabile del trattamento sia tenuto a garantire che i dati personali siano: a) trattati lealmente e lecitamente; b) rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità. Il trattamento successivo dei dati per scopi storici, statistici o scientifici non è ritenuto incompatibile, purché gli Stati membri forniscano garanzie appropriate; c) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati; d) esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare i dati inesatti o incompleti rispetto alle finalità per le quali sono rilevati o sono successivamente trattati, cancellati o rettificati; e) conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati. Gli Stati membri prevedono garanzie adeguate per i dati personali conservati oltre il suddetto arco di tempo per motivi storici, statistici o scientifici.

[165] LAMANUZZI M. *Diritto penale e trattamento dei dati personali. Codice della privacy, novità introdotte dal regolamento UE 2016/679 e nuove responsabilità per gli enti* in JusOnline, 2017.

possibile la nomina di un *sub*-responsabile del trattamento, per specifiche attività di trattamento, nel qual caso occorre definire i rapporti mediante un contratto o altro atto giuridico.

La violazione del regolamento da parte del responsabile del trattamento, determinando finalità e mezzi del trattamento stesso, comporta l'assunzione diretta della qualifica di titolare del trattamento.

Il responsabile del trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate onde assicurare la conformità del trattamento al regolamento e alla tutela dei diritti dell'interessato (dimostrata anche mediante il ricorso a Codici di condotta o meccanismi di certificazione).

Osservando le definizioni fornite dal Regolamento si nota che esso introduce molte definizioni assenti nel Codice della *privacy*.

Esso, infatti, all'articolo 4 definisce dato personale: «qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato) che identifichi o renda identificabile una persona fisica e che possono fornire dettagli sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc…»

Sfogliando il Regolamento risulta evidente che, nella sua stesura offre una definizione più dettagliata del termine "dato personale" (di quanto faccia il D.lgs. n. 196/2003 all'art. 4 per esplicitare le proprie definizioni)[166].

[166] https://www.agendadigitale.eu

In particolare, il Regolamento include, a differenza[167] del Codice italiano sulla *privacy* che non tratta espressamente questi vocaboli, i significati di: dato genetico[168], dato biometrico[169], dato sanitario[170].

Osservando le definizioni fornite dal Regolamento si nota che esso introduce anche molte definizioni assenti nel Codice *privacy*.

Nello specifico, richiama la definizione di "archivio", parzialmente coincidente con "banca dati" (lett. p) dell'articolo 4 del D.lgs. n. 196/2003: nel Regolamento si parla di "insieme strutturato", mentre nel Codice italiano si parla di "complesso organizzato".

Infatti, nel Regolamento si dichiara che il trattamento è «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».

---

[167] In verità, queste categorie sono poi disciplinate all'interno di altri provvedimenti normativi e amministrativi. Infatti il Codice italiano, a differenza del Regolamento, definisce in maniera autonoma i dati identificativi, sensibili, giudiziari, anonimi, la comunicazione elettronica, i dati relativi al traffico e all'ubicazione.

[168] Per dati genetici si intendono i dati personali relativi alle caratteristiche genetiche, ereditarie o acquisite, di una persona fisica, che risultino dall'analisi di un campione biologico della persona fisica in questione, in particolare dall'analisi dei cromosomi, dell'acido desossiribonucleico (DNA) o dell'acido ribonucleico (RNA), ovvero dall'analisi di un altro elemento che consenta di ottenere informazioni equivalenti.

[169] I dati biometrici sono considerati dati personali quando sono ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

[170] Sono considerati personali i dati attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute. Esse comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione, come: un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro.

Il Regolamento attribuisce anche, all'articolo 9[171], una specifica protezione per i dati personali particolari che, per loro natura, sono maggiormente sensibili.

Sono particolari, ed è vietato trattare, i dati personali che rivelino: l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

È interessante osservare come il trattamento di fotografie non costituisce sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica.

Nello stabilire il divieto di trattamento dei dati "particolari", il Regolamento evidenzia che possono ricorrere anche alcune specifiche condizioni che consentano una deroga, e conducano al trattamento anche dei dati particolari[172].

Un'altra importante attività prevista dal *GDPR* e propedeutica nella progettazione di sistemi di gestione *privacy* conformi ai principi della *privacy by design e by default*[173], è la valutazione di impatto sulla protezione dei dati personali. Si tratta di un istituto cardine nel sistema *privacy* del nuovo Regolamento. Ogni trattamento di dati personali che presenta rischi per i diritti e le libertà degli individui deve essere esaminato attentamente.

Una corretta progettazione di un sistema di gestione *privacy* è fondamentale per attenuare i danni derivanti da una *data breach*. Infatti, il Regolamento

[171] Articolo 9 *GDPR* rubricato: «Trattamento di categorie particolari di dati personali»: «È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona».

[172] Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

[173] Essi consistono nell'introduzione del principio per cui la privacy va considerata e applicata fin dalla sua fase di progettazione. In altri termini, qualsiasi progetto ad impatto privacy deve nascere ed essere costruito con impostazioni di default, che rispettino la disciplina in tema di protezione dei dati personali.

introduce, in capo ai titolari del trattamento, un obbligo generalizzato di comunicazione delle violazioni di dati personali (*data breach notification*).

Al fine di cogliere e percepire ogni minima sfumatura del decreto sarebbe opportuno analizzarlo accuratamente articolo per articolo, e ciò anche per ben comprendere, non solo da un punto di vista formale, ma anche e soprattutto sostanziale, le numerose abrogazioni in esso contenute.

Il quadro normativo non si è cristallizzato nelle sole norme comunitarie, poiché all'Italia è stato richiesto adeguamento della legislazione in materia.

Il governo ha concluso l'iter normativo di armonizzazione della normativa italiana a quella europea, con il D.lgs. 101 del 10 agosto 2018 pubblicato in Gazzetta Ufficiale il 4 settembre ed entrato in vigore il 19 settembre.

Tale decreto reca: «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)».

Tale intervento è avvenuto con un certo ritardo, avendo già trovato applicazione dal 25 maggio 2018 il Regolamento 679/2016/UE (di seguito il Regolamento o GDPR), che aveva concesso due anni di tempo agli Stati membri dell'Unione Europea per prepararsi alla riforma. La legge di delegazione europea 2016-2017[174], aveva concesso delega al Governo per il recepimento delle Direttive europee e l'attuazione di altri atti dell'Unione europea.

Detta legge, prevedeva all'articolo 13 una delega per il Governo per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679 del Parlamento europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla loro libera circolazione. Più nello specifico, l'articolo 13 indirizzava il Governo, il quale nell'esercizio della delega era tenuto ad abrogare le disposizioni del decreto incompatibili con quelle del

[174] Legge 25 ottobre 2017 n. 163, in G.U. n. 259

Regolamento, modificare il Codice limitatamente a quanto fosse necessario per dare attuazione alle disposizioni del Regolamento non direttamente appiccabili, coordinare la parte restante delle disposizioni del decreto con quelle del Regolamento, nonché preveder ove opportuno il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali. La finalità della delega avrebbe dovuto essere, pertanto, quella di adeguare, nell'ambito delle modifiche al codice, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento UE con la previsione di sanzioni penali e amministrative, efficaci, dissuasive e proporzionate alla gravità delle violazioni delle disposizioni tesse.

Non solo i termini di adeguamento (sei mesi dalla pubblicazione della legge delega) non sono stati rispettati, ma neppure la delega è stata esercitata nei termini previsti.

Le disposizioni contenute in tale decreto per l'adeguamento della normativa nazionale alle disposizioni del Regolamento 679 sono obbligatorie e direttamente applicabili in ciascuno degli Stati membri.

Il decreto legislativo 196/2003 (vecchio Codice *privacy*) non è abrogato, ma modificato e integrato dal nuovo decreto che ne realizza l'adeguamento alle disposizioni del *GDPR.*

L'attuale quadro normativo in materia di protezione dei dati personali in Italia, pertanto, è il seguente: *GDPR* e Codice *privacy*, così come novellato dal Decreto 101.

È importante tenere in considerazione la circostanza che il D.lgs. 196/2003 e il Regolamento UE 2016 hanno un approccio alla *privacy* completamente differente.

Il Regolamento si fonda sul principio dell'*accountability*, consistente nell'obbligo per il titolare del trattamento di adottare misure appropriate ed efficaci per attuare i principi di protezione dei dati, nonché nella necessità di dimostrare, su richiesta, che sono state adottate misure appropriate ed efficaci. Il Codice della *privacy*, si limitava a dettare, invece, direttamente alcune misure minime alle quali il titolare del trattamento si sarebbe dovuto

uniformare. Il d.lgs. 101/2018 reintroduce le misure di sicurezza (c.d. misure di garanzia) per i soli dati genetici, biometrici e relativi alla salute.

Possiamo affermare che la tecnica redazionale di adeguamento che ne è scaturita è c.d. "per novellazione", in quanto il legislatore, ha preso atto, da un lato che la massima parte delle disposizioni del D.lgs. 196 erano da abrogare, perché incompatibili con quelle del regolamento, e dall'atro che una parte minore delle disposizioni codicistiche nazionali andavano comunque modificate.

È bene sottolineare che la normativa italiana va interpretata e applicata conformemente a quella europea, in quanto integra, ma non sostituisce il *GDPR*, il quale *ex* articolo 288 TFUE «ha portata generale […] è obbligatorio in tutti i suoi membri e direttamente applicabile in ciascuno degli stati membri».

Per quel che concerne il profilo sanzionatorio, di preminente interesse per il penalista, menzioniamo l'inserimento degli *articoli 167-bis* (Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala) *e 167-ter* (Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala) dovuto probabilmente alla crescente preoccupazione per i *cyber* attacchi a strutture critiche (quali, tra gli altri, gli ospedali) che trattano grandi quantità di dati personali.

Inoltre, ai fatti commessi prima della data di entrata in vigore del decreto non può essere applicata una sanzione amministrativa pecuniaria per un importo superiore al massimo della pena originariamente prevista o inflitta per il reato, tenuto conto del criterio di ragguaglio di cui all'articolo 135 del codice penale.

A tali fatti non si applicano le sanzioni amministrative accessorie introdotte dal presente decreto, salvo che le stesse sostituiscano corrispondenti pene accessorie.

Tra i vari meriti che si possono riconoscere a tale decreto, vi è quello di aver definito in modo chiaro cosa si intenda per comunicazione e diffusione dei dati personali dei dati personali, di aver individuato nel Garante della *privacy* l'Autorità incaricata del controllo e della promozione delle regole

deontologiche in materia, ma ancora di aver stabilito che il consenso al trattamento dei dati personali potrà essere espresso solo al compimento dei 14 anni di età**.** Chi ha un'età inferiore necessita del consenso di chi esercita la sua responsabilità genitoriale. Il consenso poi deve essere richiesto dal titolare del trattamento in modo chiaro e semplice, facilmente comprensibile dal minore[175].

Il decreto stabilisce inoltre che tutti gli organi giudiziari avranno l'obbligo di nominare il *DPO* e si precisano le limitazioni ai diritti degli interessati in relazione a ragioni di giustizia. Si rafforza il divieto di pubblicazione dei dati dei minori, e si prevede una relativa sanzione penale a riguardo.

Inoltre, riconosciuta l'importanza attribuita all'interesse pubblico, è possibile utilizzare i dati personali di determinati soggetti.

Il decreto prevede l'adozione di misure adeguate di sicurezza, come tecniche di cifratura e di pseudonomizzazione a tutela del dato personale, misure di minimizzazione e le specifiche modalità per l'accesso selettivo ai dati.

Relativamente alle misure di garanzia che riguardano i dati genetici e i dati relativi alla salute per finalità di prevenzione, diagnosi e cura, queste sono adottate sentito il Ministero della salute che, a tal fine, acquisisce il parere del Consiglio superiore di sanità.

Nel decreto è ammesso l'utilizzo di dati biometrici, ma con riguardo alle procedure di accesso fisico e logico ai dati da parte dei soggetti autorizzati, nel rispetto delle misure di garanzia e di protezione. Ovviamente è attribuito al Garante il compito di scrivere le misure di garanzia per il trattamento di dati genetici, biometrici e sanitari.

Un'altra importante novità è stata l'introduzione del concetto di diritto all'eredità del dato in caso di decesso, con l'introduzione di una norma che consente di disporre *post mortem* dei propri dati caricati nei servizi informativi delle società, ampliando quindi i diritti informativi dell'interessato (consumatore, cliente, dipendente aziendale e così via) in tema di trattamento dei dati, prevedendo il diritto all'oblio, a portare altrove

[175] Capo II art. 2 del Decreto.

le proprie informazioni, a decidere cosa farne in caso di morte e imporre limitazioni.

Tra le forme di tutela, viene introdotta la nuova forma del reclamo, alternativo al ricorso in tribunale.

Il decreto, quindi, abroga alcuni articoli del Codice *privacy* tra i quali le c.d. "misure minime di sicurezza" che vengono lasciate alle indicazioni del Garante.

Così anche l'Italia si adegua al regolamento europeo che detta nuove norme precise sulla *privacy* dei cittadini europei. Il *General data protection regulation* è stato quindi armonizzato nel nostro Paese con il decreto n.101 del 10 agosto 2018, anche se operativamente le disposizioni dettate dal GDPR erano già entrate in vigore in modo automatico dallo scorso 24 maggio 2018.

Con la pubblicazione in Gazzetta ufficiale del Decreto 101 del 10 agosto, possiamo dire che il nostro Paese si è adeguato formalmente e a livello legislativo al *GDPR* emanato su scala europea, il cui obbiettivo era quello di dare all'Europa, ai suoi Stati e ai suoi cittadini una normativa comune sul trattamento dei dati personali dei cittadini stessi, anche alla luce dell'innovazione tecnologica e economica degli ultimi anni.

Se "protezione dei dati" è formula che riassume ed unifica tutte le regole sul trattamento dei dati, merita sottolineare che al termine "diritto", deve essere riconosciuto un ruolo fondante la situazione del soggetto rispetto all'attività di trattamento, nella consapevolezza che il rispetto delle regole contenute nel Codice rappresenta l'aggiornata espressione della libertà del soggetto in una società nella quale il trattamento dei dati personali assume una dimensione e un'intensità tali da non poter più essere ignorate.

CAPITOLO II

IL QUADRO SANZIONATORIO PRECEDENTE LA RIFORMA

SOMMARIO: -1. *La tutela penale dei dati personali nel quadro normativo 196/2003; -1.1. Le sanzioni amministrative. -2. Il vecchio trattamento illecito di dati, art. 167 d.lgs. 196/2003: nozione e ratio della tutela; -2.1 Analisi strutturale del reato; -2.2. Requisito del nocumento: configurazione come condizione obiettiva di punibilità e clausola di riserva; -2.3. Il caso Google Vividown e la responsabilità dell'ISP. -3. Falsità nelle dichiarazioni e notificazioni al garante, art. 168 d.lgs. 196/2003. -4. Omissione misure minime di sicurezza, art. 169 d.lgs. 196/2003 abrogato. -5. L'inosservanza di provvedimenti del garante, art. 170 d.lgs. 196/2003. -6. Le altre fattispecie, art. 171 d.lgs. 196/2003. -7. Le pene accessorie, art. 172 d.lgs. 196/2003. -8. Conclusioni*

1. La tutela penale dei dati personali nel quadro normativo 196/2003

«Gli individui producono ogni giorno dati di svariata natura che nel mondo contemporaneo le moderne tecnologie consentono di immagazzinare. Il trattamento dei dati è stato per molto tempo solo funzionale allo svolgimento di altre attività, mentre di recente ne sono sorte numerose che si esauriscono proprio nel solo trattamento dei dati. Occorre, pertanto, stabilire regole chiare per determinare fino a che punto può spingersi il trattamento dei dati, visto che lo stesso è suscettibile di incidere sulla dignità dell'individuo»[1].

Il nuovo codice della *privacy* lungi dall'esaurirsi in una ricognizione meramente compilativa delle disposizioni previgenti e contenuta principalmente nella legge 675/96, ha introdotto alcune innovazioni anche nella parte relativa alle previsioni di carattere penale e ora descritte negli articoli 167-172 dello stesso decreto.

Relativamente al quadro generale di riferimento sulla tutela penalistica della riservatezza e dell'identità personale al di fuori del testo unico 196/2003, è

[1] PIZZETTI F., Convegno Università di Napoli FEDERICO II.

opportuno evidenziare che, esisteva, già *ante* codice *privacy*, una vasta ma laconica normativa, che non si scontra con la nuova disciplina del codice, in quanto questa prende in considerazione condotte riguardanti il trattamento dei dati personali e quindi indirettamente lesive della riservatezza e dell'identità personale[2].

Il legislatore penale del 1930, complice il contesto storico culturale in cui il codice è stato elaborato, aveva previsto delle modalità tipiche di aggressione diretta a tali diritti[3].

Per poter meglio inquadrare le fattispecie incriminatrici introdotte per la prima volta con la l. 675/96 e confluite poi nel codice della *privacy*, è utile ricordare che la dottrina ha individuato due tipologie fondamentali di aggressione del diritto alla riservatezza ovverosia la condotta di indiscrezione e la condotta di rivelazione[4].

La prima consiste nella presa di coscienza di ciò che attiene alla vita privata; la seconda consiste nella comunicazione ad altri di ciò che si conosce sull'altrui vita privata. Tutte le fattispecie contenute nel codice penale sono riconducibili a tali due categorie, ma la disciplina penalistica lascia vuoti e carenze di tutela che solo in parte vengono colmate.

L'obbligo del legislatore di prevedere un apposito apparato sanzionatorio il quale tuteli in maniera specifica il bene della riservatezza in relazione al

---

[2] Molti sono gli autori che si sono occupati della tutela penale della privacy, già *ante legem* 675/96. Si segnalano: PALAZZO F., *Considerazioni in tema di tutela della riservatezza*, (a proposito del nuovo art. 615 bis) in Riv. Trim. dir. e proc. pen, 1975 pp. 126.
ZANGONI, *sulla tutela penale del diritto alla riservatezza* ivi 1982 pp 971 *Banche dati, telematica e diritti della persona*, (a cura di), ALPA G., BESSONE M., Padova 1984.
PATRONO P. *Privacy e vita privata* (diritto penale), in Enc Dir XXXV, Milano 1986. P. 557.
PETRONE M. *Banche dati e tutela della privacy*. *Riflessi penalistici* in Dir Inf, 1988 p. 82.
VOLTA *La tutela penale del diritto alla riservatezza*, art 615 bis cp: esegesi della norma in Riv. Pen. 1989 pp. 535.
MANNA A. *Beni della personalità e limiti della protezione penale*, Padova 1989.
PAGLIARO S. *Informatica e crimine organizzato* in Ind Pen 1990 p 414 ss.
FROSINI voce *telematica e informatica giuridica* in Enc dir vol XLIV, Milano 1992 p. 66.
MANTOVANI F. *Brevi note a proposito della nuova legge sulla criminalità informatica* in Critica del diritto, 1994 IV pp. 12.
VANNINI *La criminalità informatica: le tipologie di compter crimes di cui alla l. n. 547/93 dirette alla tutela della riservatezza e del segreto* in Riv. Trim. dir. Pen. economia, 1994 p. 427.

[3] Dei delitti contro l'inviolabilità del domicilio, dei delitti contro l'inviolabilità dei segreti, artt. 615 bis, 615 ter, 615 quater, 617 bis, 617 ter, 617 quinquies e 617 sexies

[4] MANTOVANI F. *Brevi note a proposito della nuova legge sulla criminalità informatica* in Critica del diritto, 1994 IV.

trattamento dei dati personali, deriva da fonti di natura internazionale e comunitaria.

Ricordiamo in proposito a Convenzione di Strasburgo 108/1981, ratificata in Italia nel 1989[5] che impegna all'articolo 10 ogni Parte a fissare sanzioni adeguate per la violazione delle disposizioni emanate in esecuzione della Convenzione, al fine di garantire il principio del rispetto dei diritti e delle libertà fondamentali e in particolare del diritto alla vita privata in riferimento al trattamento dei dati.

In secondo luogo, la Direttiva 95/46/CE (vedi cap. 1 par. 9.4) che prevede all'articolo 24 che gli stati membri adottino le misure appropriate per garantirne la piena applicazione, stabilendo le sanzioni da applicare in caso di violazione delle disposizioni di attuazione della Direttiva stessa.

La Corte di Giustizia ha inoltre più volte affermato il principio dell'effettività, proporzionalità, capacità dissuasiva ed omogeneità delle sanzioni per gli illeciti conseguenti alla violazione di norme di attuazione della normativa comunitaria.

L'esigenza di un adeguato apparato sanzionatorio è soddisfatta dal codice con la strutturazione di un sistema misto: penale, amministrativo e civile[6].

Per quel che qui interessa, è opportuno evidenziare come il quadro della tutela penalistica apprestata dall'ordinamento generale alle situazioni giuridiche soggettive connesse al trattamento dei dati personali sia profondamente mutato a seguito del decreto legislativo 196/2003 che ha apportato delle modifiche all'impianto sanzionatorio della 675/96.

In tale normativa infatti, il legislatore aveva espresso una particolare preferenza per lo strumento di carattere penale, nell'ottica di una valenza maggiormente dissuasiva della stessa rispetto a quella amministrativa[7], giustificata sia dall'esigenza di tener conto dell'esperienza legislativa degli

[5] Cfr. cap. 1 par. 9.3

[6] Al riguardo si sottolinea il disposto dell'art 15 del testo unico ai sensi del quale "chiunque cagiona danno ad altri per effetto del trattamento dei dati personali è tenuto al risarcimento ai sensi dell'art 2050cc".

[7] ZOTTA D *Le sanzioni* in CLEMENTE A. (a cura di) Privacy, Padova, 1999

altri paesi membri dell'Unione, che da quella di tutelare un bene di rango costituzionale quale quello della riservatezza, da interferenze illecite[8].

Occorreva, sottolineava la dottrina[9], una simmetria con le disposizioni del codice penale che qualificano i diritti della personalità come beni di carattere primario e che tutelano però la *privacy* da aggressioni realizzate con modalità diverse da quelle proprie del trattamento dei dati.

Si tratta però di un'impostazione sotto più di un profilo ampiamente criticata[10].

Autorevole dottrina al riguardo prospetta addirittura nella legge 675/96 una sostanziale sconfitta del principio di legalità, in particolare sul versante del principio di certezza e di sufficiente tassatività delle fattispecie che costituiscono (o dovrebbero costituire) sicuri punti di riferimento nella costruzione di nuove ipotesi di reato[11].

Ancora si ritiene che la soluzione tecnica adottata dal legislatore del 96 si sia mossa nella direzione di punire ad ampio raggio, con un eccesso di fattispecie penali e senza effettuare selezioni tra le condotte sanzionate; in più si sottolinea anche il carattere particolarmente mite delle pene previste originariamente.

In sintesi, sembrava che l'apparato sanzionatorio penale si presentasse servente rispetto alla disciplina di settore e disfunzionale rispetto al principio di offensività, delineati dalla dottrina penalistica più attenta.

L'intervento di sistemazione operato dal legislatore nel codice *privacy* ha investito anche la parte sanzionatoria; la legge 675 perseguiva la via del doppio binario penale e amministrativo.

---

[8] ZOTTA D *Le sanzioni* in CLEMENTE A. (a cura di) Privacy, Padova, 1999;
CORRIAS LUCENTE G. *Sanzioni* in GIANNANTONIO E., LOSANO M. ZENO ZENCOVICH V. (a cura di) *La tutela dei dati personali commentario alla l 675/96,* Padova, 1999.

[9] BUTTARELLI G. *Banche dati e tutela della riservatezza: la privacy nella società dell'informazione*, Milano, 1997

[10] I motivi dell'insoddisfazione investivano diversi aspetti; su tutti si segnala l'eccessiva ampiezza del ricorso alla sanzione penale, in controtendenza con la generica spinta di politica legislativa tesa a contenere nei limii della stretta necessità il ricorso a misure penali. Così CORASANITI G., *Sanzioni penali e depenalizzazione degli illeciti nella normativa a tutela dei dati personali*, in Danno e responsabilità, 2002, ma anche PARDOLESI R. (a cura di), Diritto alla riservatezza e circolazione dei dati personali, Milano, 2003.

[11] SGUBBI F. *Profili penalistici in Riv Trim dir e proc civ*, 1998 II pp. 753 ss.

La tecnica redazionale delle nuove fattispecie di illecito inserite nel codice *privacy* si muove nella precisa direzione di graduare il disvalore connesso a ciascuna condotta in base alla gravità della stessa, in ossequio ai principi di sussidiarietà e di necessaria lesività della condotta incriminata, laddove il sistema recedente si era acriticamente appiattito sulla omogeneizzazione di condotte *ictu oculi* espressive di disvalore penale[12].

Non è fuori luogo parlare di un'espansione dell'illecito amministrativo a rispetto all'area di rilievo penale.

Difatti, il legislatore del 2003 ha effettuato una notevole opera di depenalizzazione, degradando a illecito amministrativo le precedenti figure di reato di omessa o incompleta notificazione, già previste come delitto dalla 675. La *ratio* dell'abbandono della sanzione penale a favore di quella amministrativa si rinviene nell'intenzione del legislatore di rendere maggiormente efficiente e celere l'accertamento dell'illecito amministrativo; basti pensare all'irrogazione della punizione ed all'efficacia dissuasiva intimidatoria della medesima ed alla semplificazione e flessibilità procedimentale e processuale che concede in sede di commisurazione della sanzione all'interno del minimo e massimo edittale.

Non bisogna certo fare l'errore di leggere l'innovazione in una prospettiva indulgenzialistica che resta estranea alle intenzioni del codice. Tale soluzione però, fatti salvi alcuni problemi di coordinamento, non sempre di agevole soluzione, con gli illeciti puniti in via amministrativa, è da condividersi, in quanto si adatta perfettamente ai principi generali del diritto penale quale quello di sussidiarietà e ricorso alla sanzione penale solo come *extrema ratio*.

Le modifiche all'assetto sanzionatorio non sono state le uniche modifiche operate dal legislatore, il quale ha proceduto anche con interventi atomistici su singole fattispecie che risultano sensibilmente modificate rispetto l'archetipo della 675[13].

---

[12] CIRILLO G. P. *La tutela della privacy nel sistema del nuovo codice sulla protezione dei dati personali*, Padova, 2004.

[13] CORRIAS LUCENTE G. *La nuova normativa penale a tutela dei dati personali* in *Il codice dei dati personali temi e problemi*, CARDARELLI F., SICA S., ZENO ZENCOVICH V., Milano, 2004.

Il titolo terzo del codice è interamente dedicato alle sanzioni e suddiviso in due capi; il primo composto dagli articoli 161- 166 concernente le condotte punite con la sanzione amministrativa e il secondo (articoli 167-172) relativo agli illeciti penali.

Pertanto, nella disciplina prevista dal Codice *privacy* gli illeciti amministrativi sono previsti agli articoli 161 «omessa o inidonea informativa all'interessato»; 162 «altre fattispecie» che nella sostanza punisce la comunicazione dei dati idonei a rivelare lo stato di salute dell'interessato in violazione dell'art 84; art 163 «omessa o incompleta notificazione»; e art 164 «omessa informazione o esibizione al garante». Notiamo quindi come vi sia stato uno scorporo delle corrispondenti fattispecie *ab origine* sanzionate dall'art 39 della l 675/96.

Per ciò che attiene alla tutela penale il legislatore consapevole del carattere primario del bene della riservatezza dei dati personali ha optato per un sistema sanzionatorio caratterizzato da una accentuazione della differenziazione delle sanzioni – differenziazioni di pene, distinzione tra delitti e contravvenzioni, e tra ipotesi commissive e omissive – nel quale mostra di apprezzare il differente disvalore delle varie fattispecie[14].

Per quanto riguarda nello specifico le residue fattispecie incriminatrici, queste sono distinte in delitti e contravvenzioni.

La previsione di fattispecie delittuose a struttura contravvenzionale ha come effetto di evidenziare gli aspetti deteriori di un diritto penale che tende a un rigore sanzionatorio, giustificato esclusivamente dalla necessità di una risposta simbolica alle esigenze sociali di tutela, con il sacrificio delle garanzie fondamentali del diritto penale[15].

Figurano tra i delitti il trattamento illecito di dati personali previsto all'articolo 167, la falsità di dichiarazioni e notificazioni al Garante, prefigurata dall'articolo 168, e l'inosservanza di provvedimenti al garante delineata dall'articolo 170.

---

[14] MONDUCCI J. SARTOR G. *Il codice in materia dei dati personali*, Padova, 2004.

[15] DONINI, Il delitto il quale evidenzia come le contravvenzioni seppur soddisfano *l'horror vacui* punitivo, allargando la penalizzazione a singoli fenomeni preparatori o di disturbo, radicalizzano questa tendenza, assommando il maggior rigore sanzionatorio con la minore garanzia probatoria, sacrificando il principio di colpevolezza senza quanto meno ridurre l'entità della risposta.

Costituiscono invece fattispecie contravvenzionali la violazione delle misure minime di protezione dei dati personali di cui all'articolo 33 (articolo 169 comma 1) e la violazione di disposizioni di cui agli articoli 113 e 114 concernenti il divieto di indagini sulle opinioni del lavoratore e la violazione delle norme sul controllo a distanza dei lavoratori. In quest'ultima fattispecie (articolo 171) il legislatore inserisce un richiamo alle norme sullo statuto dei lavoratori, e non è l'unico caso in cui il legislatore ha scelto di adottare la tecnica del rinvio ad altre norme, al fine di individuare la condotta sanzionata, tecnica che, non si può fare a meno di notare, ricalca nella sostanza quella delle cd norme penali in bianco e che si espone ad alcuni rilievi critici.

La distinzione tra le due *species* del reato (delitti e contravvenzioni) è importante anche ai fini dell'applicazione della misura accessoria della pubblicazione della sentenza di condanna contemplata all'articolo 172, esclusivamente per i delitti[16].

C'è da chiedersi però se la sua mancata applicazione alle fattispecie contravvenzionali sia il frutto di una scelta consapevole o di un mancato coordinamento[17].

Le fattispecie, salva l'eccezione contenuta nell'articolo 167 sono configurate come reati propri. In alcuni casi, come nel 167, l'elemento soggettivo è caratterizzato dal dolo specifico per cui la violazione delle norme che regolano il trattamento determina la responsabilità penale solo se la condotta è sorretta da una particolare finalità.

Il codice non permette l'applicazione di misure cautelari coercitive o interdittive né l'arresto in flagranza o il fermo e tutti i reati sono perseguibili d'ufficio.

Prima di passare all'analisi delle singole fattispecie è interessante concludere osservando che la tecnica di redazione normativa, che caratterizza l'apparato

[16] CIRILLO G. P., *La tutela della privacy nel sistema del nuovo codice sulla protezione dei dati personali*, Padova, 2004.

[17] L'intenzione del legislatore non è certamente nel senso di una riduzione delle ipotesi di pubblicazione della sentenza a seguito della violazione delle disposizioni del codice: basti vedere la sanzione amministrativa accessoria di cui all'art 165 il quale prevede la possibilità di disporre la pubblicazione della sentenza del provvedimento sanzionatorio del garante.

sanzionatorio del codice, presta il fianco a critiche sotto il profilo della determinatezza della fattispecie penale in quanto questa non è descritta esplicitamente, ma deve essere ricostruita in via interpretativa, sulla base delle norme richiamate dalla disposizione sanzionatoria. In proposito è stato osservato da autorevole dottrina[18], che il difetto di autonomia conseguente alla tecnica di formulazione della norma penale, che caratterizzava l'impostazione sistematica della 675 e dalla quale il codice non differisce, non giova tuttavia alla determinatezza della fattispecie penale e alla adeguatezza dell'intervento penale.

Pertanto, seppur auspicata universalmente, la riforma non ha, tuttavia, eliminato del tutto le disfunzioni e le discrasie rilevate nell'apparato penalistico, basti pensare alla mancata analisi puntuale delle singole figure di reato[19].

1.1 Le sanzioni amministrative

Il quadro degli illeciti amministrativi, soggetti al potere sanzionatorio del Garante è delineato al Titolo II «Sanzioni», Capo I «Violazioni amministrative», articoli da 161 a 166 del D.lgs. 196/2003, che costituisce un breve *corpus* normativo teso ad ampliare, in misura modesta, l'area dell'illecito amministrativo a scapito dell'area di rilievo penale, la quale conserva altre dimensioni.

Nell'assenza di una definizione delle sanzioni[20] amministrative, offerta dalle norme vigenti, è stato osservato che le sanzioni amministrative si possono dal punto di vista sostanziale, individuare in modo soltanto residuale, quali misure afflittive non consistenti in sanzioni penali o in sanzioni civili[21].

---

[18] CORRIAS LUCENTE G. *Sanzioni* in GIANNANTONIO E., LOSANO M. ZENO ZENCOVICH V. (a cura di) *La tutela dei dati personali commentario alla l 675/96,* Padova, 1999.

[19] CORRIAS LUCENTE G. *La nuova normativa penale a tutela dei dati personali* in *Il codice dei dati personali temi e problemi,* CARDARELLI F., SICA S., ZENO ZENCOVICH V., Milano, 2004.

[20] Per sanzioni in senso ampio si intende la conseguenza sfavorevole di un comportamento illecito prevista dall'ordinamento, consistente nell'inflizione di un male ritenuto maggiore rispetto al beneficio che possa derivare dalla violazione. Utilizzando tecniche di tipo sanzionatorio si persegue, un disegno di controllo sociale delle condotte, tentando di prevenire la violazione di precetti giuridici e, ove questa si sia verificata, reprimendone il comportamento attraverso conseguenze afflittive.

[21] CASETTA E., *Sanzione amministrativa*, in Dig. Disc. Pubbl, Torino, 1994, p. 599.

Le ipotesi di violazioni amministrative previste dal codice della *privacy*, quanto ai meccanismi applicativi, sono riconducibili agli illeciti amministrativi disciplinati dalla legge 689/81[22].

Da un sintetico esame del quadro sanzionatorio possiamo dedurre alcune considerazioni.

Le norme contenute all'articolo 161 offrono protezione al diritto degli interessati a ricevere le prescritte informazioni relative alla raccolta e al trattamento dei dati che li riguardano, salvaguardando la loro possibilità di esercitare la pretesa di controllo sulla circolazione delle informazioni. Tali norme garantiscono *lato sensu* la regolarità del procedimento, finendo per curare, attraverso lo strumento della sanzione, l'interesse diffuso a un corretto svolgimento dell'attività del trattamento dei dati[23].

Le sanzioni contenute agli articoli 163 e 164 hanno ad oggetto condotte che tendono a ostacolare l'attività di vigilanza e istruttoria del Garante; in questo caso le norme prescindono dai diritti dell'interessato, il quale resta sullo sfondo, e accordano tutela alle funzioni pubbliche e agli interessi collettivi sottesi ad esse. Si comprende come la *ratio*, in questo caso sia quello di accentuare e rafforzare gli obblighi di collaborazione degli amministrati nei confronti del Garante, poiché la protezione al bene della riservatezza è solo indiretta, attribuendo maggiore importanza all'attività del Garante, in quanto considerata attività di indirizzo, conformativa, ripristinatoria, repressiva, sanzionatoria[24].

2. Il vecchio trattamento illecito di dati, art. 167 d.lgs. 196/2003: nozione e ratio della tutela

Il legislatore del codice in materia di protezione di dati personali, intervenendo sul complesso delle disposizioni penali esistenti nel settore a distanza di un brevissimo lasso di tempo dalla precedente riforma attuata con

[22] Per un'analisi esauriente GALOPPI, Aa Vv., Codice della privacy, 2004, Tomo II, p.2111.
[23] ORLANDI, *Gli adempimenti per i titolari dei trattamenti*, in SICA- STANZIONE (a cura di), *La nuova disciplina della privacy*, Bologna- Roma, 2004, p. 183.
[24] MANNA A. *Beni della personalità e limiti della protezione penale*, Padova 1989.

il D.lgs. 467/2001, non si è limitato soltanto a recepire nel testo unico le disposizioni così come introdotte poco tempo prima, ma – almeno riguardo all'ipotesi più importante, quella che rappresenta il fulcro attorno cui ruota la risposta repressiva nel suo insieme: «il trattamento illecito di dati» – ha provveduto a ridisegnare il nucleo centrale della fattispecie.

Il trattamento illecito di dati personali costituisce una delle fattispecie più complesse designate dal legislatore del 1996 con la legge n. 675, oltre ad essere una di quelle di più frequente verificazione.

La norma incriminatrice dell'articolo 167 è esattamente incastonata in un reticolo normativo che, mette in evidenza tutti i numerosi profili di controversa applicazione. Si tratta di una "norma laboratorio" che porta con sé le problematiche dei più indicativi nodi teorici del diritto penale ma che il legislatore non ha munito di quei dispositivi per risolvere le ipotesi applicative controverse.

Questo il testo del vecchio articolo 167: «Salvo che il fatto costituisca più grave reato, chiunque, 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, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.

Salvo che il fatto costituisca più grave reato, chiunque, 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 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni».

Il legislatore ha confermato la scelta di far restare nell'area del penalmente rilevante la fattispecie del trattamento illecito dei dati personali, modellandola quasi interamente sul contenuto del vecchio articolo 35[25].

[25] CIRILLO G. P., *La tutela penale, in la tutela della riservatezza, trattato di diritto amministrativo,* diretto da SANTIELLO G. Padova, 2000; MANTOVANI M., *Le fattispecie incriminatrici della legge sulla privacy; alcuni spunti di riflessione* in Critica dir., 1997.

Quest'ultima disposizione[26] era strutturata secondo il paradigma delle norme a più fattispecie individuabili mediante la tecnica del rinvio a norme extra-penali contenute nella l. 675/96.

L'art. 35 infatti si limitava a incriminare il trattamento dei dati personali avvenuto in violazione di determinate norme di disciplina dettate in materia, quando esso fosse accompagnato dal fine dell'autore di trarre per sé o per altri profitto o di recare ad altri un danno (commi I e II); contemplando un aggravamento di pena, qualora dal trattamento illecito derivasse "nocumento" (comma III).

L'articolo 167 D.lgs. 196/2003, invece, ha subordinato la rilevanza penale del trattamento illecito, fermo restando la ricorrenza del dolo specifico proprio al verificarsi del "nocumento" e ciò, sia nelle ipotesi meno gravi di cui al comma I, con le dovute puntualizzazioni, sia nell'ipotesi più grave di cui al comma II.

Per quanto possa apparire ultroneo specificarlo, è proprio la disposizione *de quo* il portato tangibile della tutela del diritto dell'interessato alla sua *privacy*, intesa nella duplice valenza positiva e negativa[27]; come diritto a mantenere nell'ambito della propria sfera privata fatti, comportamenti, notizie e informazioni personali – *right to be let alone* – e diritto di mantenere il controllo sulla correttezza delle informazioni che vengono divulgate.

Il diritto alla riservatezza non è l'unico bene che tale disposizione intende proteggere; sebbene la scelta del legislatore di subordinare la punibilità del reato alla derivazione di un nocumento evidenzi, indubbiamente, la volontà di porre l'accento sul diritto individuale alla protezione della vita privata e al controllo dei dati personali, deve ritenersi che la norma tuteli anche le mere

[26] Articolo 35 legge 675/96: «Salvo che il fatto costituisca più grave reato, chiunque, 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 articoli11, 20 e 27, è punito con la reclusione sino a due anni o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da tre mesi a due anni. Salvo che il fatto costituisca più grave reato, chiunque, 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 21, 22, 23, 24 e 24-bis (*), ovvero del divieto di cui all'articolo 28, comma 3, è punito con la reclusione da tre mesi a due anni. Se dai fatti di cui ai commi 1 e 2 deriva nocumento, la reclusione è da uno a tre anni.»

[27] Cfr. capitolo 1

funzioni e cioè le funzioni di controllo del Garante per la protezione dei dati personali.

È corretto affermare che la *ratio* dell'articolo 167, possa individuarsi nel presidio penale di norme civilistiche, avendo la norma mirato sia alla tutela del singolo, sia a fornire degli strumenti adeguati volti a sanzionare le condotte lesive la cui azionabilità è sottratta alla disponibilità del singolo.

La plurioffensività del reato risulta confermata, oltre che dall'analisi delle varie condotte descritte dalla norma, anche dal fatto che il reato a differenza di altre ipotesi delittuose lesive della reputazione, come nel caso della diffamazione a mezzo stampa, è procedibile d'ufficio e non a querela di parte[28], come sarebbe stato logico se l'unico oggetto della tutela nelle incriminazioni fosse stato il diritto alla riservatezza *tout court*[29].

2.1. Analisi strutturale del reato

Passando ora all'esame delle condotte, la disposizione prevede due diversi titoli di reato, trattati rispettivamente nel primo e nel secondo comma e differenziati dalla natura dei dati oggetto del trattamento.

Deve rilevarsi *prima facie* che le diverse fattispecie hanno in comune l'operatività di una clausola di riserva espressa[30], il dolo specifico e la previsione di un nocumento.

L'articolo 167 eleva a fattispecie di reato il mancato rispetto di alcuni presupposti del trattamento, utilizzando la tecnica del rinvio ad altre

[28] VENEZIANI P. *Beni giuridici protetti*, p. 166 osserva che ove l'unico bene tutelato dalla norma in parola fosse individuabile nella privacy, ovvero in una delle sue possibili esplicazioni, dovrebbe concludersi che, trattandosi di bene essenzialmente disponibile sia da escludere una lesione dello stesso penalmente rilevante qualora il titolare abbia validamente consentito a fatti idonei a ledere o a mettere in pericolo il bene medesimo.

[29] MANNA A. *Il quadro sanzionatorio penale ed amministrativo del codice sul trattamento dei dati personali*. L'autore osserva che una corretta politica criminale ispirata al principio di sussidiarietà avrebbe dovuto valorizzare, sul piano della promovibilità dell'azione penale, la natura spiccatamente personale di tale diritto, nonché la sua natura certamente disponibile, ricorrendo alla procedibilità a querela della persona offesa, quale congruo strumento selettivo della lesività di determinate condotte, mediante la remissione al titolare della scelta in ordine all'azionabilità dell'intervento penale. Il mantenimento della procedibilità d'ufficio, nelle ipotesi in esame, conferma la natura "anfibia" di detti illeciti, in bilico tra la tutela di mere funzioni e la protezione di un assai più pregnante bene giuridico individuale.

[30] Cfr. capitolo II par. 2.2

disposizioni contenute nel testo unico ed evitando una sorta di incriminazione a tappeto dell'inosservanza di qualunque violazione di legge da una parte, ma, dall'altra, esponendosi a rilievi critici in punto di sufficiente determinatezza e tassatività della fattispecie[31].

Da un punto di vista esegetico, l'attenzione dell'interprete deve preliminarmente soffermarsi sull'individuazione della condotta di "trattamento", per la quale si pongono non pochi problemi.

Primo aspectu la nozione risulta di facile comprensione, dato l'articolo 4 comma 1 lett. a dello stesso codice che ne definisce il contenuto, enunciando una nozione innovativa rispetto al passato, e inserendo nel minuzioso elenco una nuova operazione di trattamento –la consultazione–, specificandosi altresì che non occorre, perché si abbia trattamento, che questi dati siano registrati in una banca dati. La preoccupazione che sorge è se si possa davvero ricondurre alla nozione di trattamento anche una sola delle operazioni descritte, con un'inammissibile estensione dell'orbita operativa della fattispecie penale. Preoccupazione non condivisibile secondo parte della dottrina[32], la quale ritiene che l'*impasse* da superare sia da rinvenire nel modo errato di guardare la normativa in oggetto, considerandola come se essa tutelasse in via assoluta, primaria o anche solo concorrente, il bene della riservatezza dei dati; in quanto nessun dubbio sussiste sul fatto che il legislatore abbia inteso disciplinare l'attività di trattamento dei dati personali in rapporto al diritto di ciascuno all'esclusivo controllo dei propri dati.

E di fatti, sia la legge 675/96 prima, che il codice oggi, non si preoccupano di tutelare questo diritto contro condotte di indiscrezione e rivelazione; bensì il *fulcrum* della tutela consiste nel trattamento di tutti i dati personali, sia pubblici che privati, in relazione al quale il legislatore ha definito le condizioni della sua liceità, sia che avvenga, da parte di terzi diversi

[31] BUTTARELLI G. *Banche dati e tutela della riservatezza,* Milano, 1997: sulla indeterminatezza della fattispecie in esame; CORRIAS LUCENTE G. Sanzioni in GIANNANTONIO- LOSANO- ZENCOVICH (a cura di), *La tutela dei dati personali. Commentario alla l. 675/96,* Padova, 1997.

[32] CORRIAS LUCENTE G. Sanzioni in GIANNANTONIO- LOSANO- ZENCOVICH (a cura di), *La tutela dei dati personali. Commentario alla l. 675/96,* Padova, 1997.

dall'interessato, in vere e proprie banche dati, o in semplici archivi documentali cartacei[33].

Ne è riprova il regime di procedibilità, d'ufficio, e non a querela, come sarebbe stato logico attendersi se il bene tutelato fosse stato effettivamente solo quello della riservatezza come valore assoluto.

Pertanto, non sembra possa prescindersi nel definire la nozione di trattamento, dalla dimensione teleologica che cementa le operazioni in cui esso si scompone, ovverosia dalla circostanza essenziale che quelle operazioni in cui si articola, per assumere rilievo nella prospettiva del codice, e nello specifico, nel trattamento illecito di dati personali, devono iscriversi nell'ambito di un'attività di organizzazione di un insieme di dati personali.

Sulla base di questa premessa, è ora possibile soffermarsi sulle singole condotte incriminate dall'articolo 167.

La norma punisce il fatto di chi procede al trattamento dei dati personali in violazione delle norme richiamate. Ciò consente di sanzionare talune ipotesi di trattamento effettuato in assenza dei presupposti indicati da specifiche norme di legge e di effettuare una selezione dei comportamenti lesivi dei beni giuridici protetti dalla norma incriminatrice, ai quali corrisponderà l'applicazione della sanzione penale ivi prevista[34].

Le prime condotte sanzionate dall'art. 167 al primo comma, riguardano i trattamenti effettuati da soggetti pubblici (diversi dagli enti pubblici economici, per i quali valgono le regole contenute nel Capo III, titolo III, Parte I) e consistono nella violazione dell'articolo 18[35], che disciplina i principi applicabili a tutti i trattamenti effettuati da soggetti pubblici, o

[33] BIANCA C. M. *La protezione dei dati personali. Commentario al D.lgs. 196/2003*, Padova, 2007.

[34] BUTTARELLI G., *Banche dati e tutela della riservatezza,* Milano, 1997, 534 il quale sostiene che la norma in questione sanziona il mancato rispetto di alcuni presupposti indicati del trattamento ed evita un'incriminazione a tappeto dell'inosservanza di qualunque violazione di legge.

[35] Articolo 18 codice privacy: "Principi applicabili a tutti i trattamenti effettuati dai soggetti pubblici": «Le disposizioni del presente capo riguardano tutti i soggetti pubblici, esclusi gli enti pubblici economici. Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali. Nel trattare i dati il soggetto pubblico osserva i presupposti e i limiti stabiliti dal presente codice, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti. Salvo quanto previsto nella Parte II per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, i soggetti pubblici non devono richiedere il consenso dell'interessato. Si osservano le disposizioni di cui all'articolo 25 in tema di comunicazione e diffusione».

dell'articolo 19[36], riguardante i principi applicabili al trattamento dei dati diversi da quelli sensibili e giudiziari[37].

Nel primo caso, la violazione prevede all'interno del reato comune di trattamento illecito, una fattispecie alternativa di reato proprio del soggetto pubblico che violi la disciplina regolante l'attività attribuitagli. Analoga situazione si verifica nel secondo caso.

Preliminarmente, occorre interrogarsi sul significato da attribuire alla locuzione "Soggetti pubblici".

Alcuni autori hanno proposto un criterio di identificazione oggettivo, basato sul carattere di attività svolta in concreto. A sostegno di tale tesi si richiama la Raccomandazione del Consiglio d'Europa del 10 settembre 1991, in tema di comunicazione a terzi di dati personali detenuti da organi pubblici, in virtù della quale l'organismo pubblico va individuato avendo riguardo alla natura dell'attività esercitata. Ciò implica l'estensione della definizione di soggetto pubblico anche ai soggetti estranei alla pubblica amministrazione, i quali esercitano un'attività amministrativa[38].

In dottrina[39] si è sostenuto che tale espressione non sia utilizzabile in una prospettiva penalistica, alla luce dei criteri indicati dagli articoli 357[40] e 358[41]

---

[36]Articolo 19 codice *privacy*: "Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari": «Il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari è consentito, fermo restando quanto previsto dall'articolo 18, comma 2, anche in mancanza di una norma di legge odi regolamento che lo preveda espressamente. La comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'articolo 39, comma 2, e non è stata adottata la diversa determinazione ivi indicata. La comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento».

[37] (per i dati comuni la raccolta è consentita, anche in assenza di norme, purché presente il legame funzionale con l'attività istituzionale; mentre la comunicazione ad altri soggetti pubblici è ammessa, se prevista da norme o necessaria allo svolgimento delle funzioni istituzionali; a soggetti privati solo se consentita da norme o regolamenti).

[38] ZOTTA F., *Privacy*, a cura di CLEMENTE, Enc. Cendon, Padova 1999.

[39] CHINÈ G., La tutela penale della privacy, in *Il trattamento dei dati personali*, vol. II, a cura di. CUFFARO V. RICCIUTO V., Torino, 1999, p. 490.

[40] Articolo 357 codice penale: "Nozione del pubblico ufficiale": «Agli effetti della legge penale, sono pubblici ufficiali coloro i quali esercitano una pubblica funzione legislativa, giudiziaria o amministrativa. Agli stessi effetti è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi, e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi».

[41] Articolo 358 codice penale: "Nozione della persona incaricata di un pubblico servizio": «Agli effetti della legge penale, sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un

del codice penale (pubblico ufficiale e incaricato di un pubblico servizio), i quali forniscono un criterio di individuazione oggettivo basato sul carattere dell'attività svolta in concreto. Secondo tale dottrina, il concetto di soggetto pubblico va individuato utilizzando un criterio soggettivo di identificazione dell'autore dell'illecito; atteso che, il legislatore penale, laddove utilizza la formula "soggetto pubblico" sembra far perno sulla natura soggettiva propria dell'autore e non sull'attività in concreto svolta e, dunque, formulare un criterio meramente subiettivo di identificazione dell'autore dal quale risultano esclusi i privati che esercitano pubbliche attività.

La soluzione che tiene maggiormente conto della natura e dell'attività esercitata è più conforme al dato normativo, dato che gli stessi articoli 18 e 19 richiamati dall'articolo 167, considerano lecito il trattamento e la comunicazione di dati personali solo in quanto strumentali o comunque collegati allo svolgimento delle funzioni istituzionali dei soggetti pubblici.

In concreto, qualunque dipendente di un ente pubblico non economico –a prescindere dalla sua qualifica di servizio nonché della veste assunta – commette il reato in esame qualora: proceda a un trattamento di dati personali effettuato per scopi diversi da quelli connessi allo svolgimento di funzioni istituzionali, oppure in assenza o in violazione di una norma di legge o di regolamento che lo autorizzi, qualora il trattamento non rientri nelle finalità istituzionali; comunichi o diffonda sia a soggetti pubblici che a soggetti privati, dati personali in mancanza di un'espressa norma autorizzativa; comunichi o diffonda dati personali senza aver dato il preventivo avviso al Garante, nel caso in cui si ritenga necessario svolgere tali attività poiché rientranti nelle finalità istituzionali dell'ente, nonostante manchi una norma regolamentare o di legge che espressamente lo preveda[42].

Ovviamente possono concorrere a diverso titolo di responsabilità il contitolare, il responsabile, o l'incaricato del trattamento. Per altro, se la

pubblico servizio. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di questa ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale».

[42] CIRILLO G. P. *La tutela penale e le sanzioni amministrative*, Padova, 2004.

condotta attiva dovesse essere integrata da un soggetto pubblico al di fuori delle violazioni contenute nel testo unico e comunque connesse all'illecito trattamento dei dati personali, pur avendosi una sostanziale integrazione delle fattispecie descritta dall'articolo, si ritiene che debbano applicarsi i principi in tema di concorso apparente i norme e, in virtù della maggiore gravità ricavabile dal regime sanzionatorio, la disposizione che verrà applicata sarà quella di cui all'articolo 326 codice penale, che punisce la rivelazione e l'utilizzazione di segreti d'ufficio[43].

La seconda fattispecie delittuosa prevista all'articolo 167 del Codice consiste nella violazione dell'articolo 23[44] che detta la disciplina dei requisiti del consenso in materia di trattamento da parte dei privati e degli enti pubblici economici, i quali devono sempre richiedere ed ottenere il consenso espresso dell'interessato (manifestato in forma scritta quando il trattamento riguarda dati sensibili).

La sanzione penale interviene quando il trattamento è svolto, senza la previa acquisizione del consenso dell'interessato, ovvero –in forza del generico richiamo a tutta la norma di disciplina– con l'acquisizione del consenso in forma diversa da quella prescritta e tipicizzata, incoerente o incompleta rispetto al trattamento effettuato.

Le modalità di acquisizione del consenso assurgono dunque a parametri di liceità della condotta, introducendo una prospettiva sanzionatoria formalistica di tutela di meri aspetti burocratici, non necessariamente incidenti sul bene tutelato[45].

Innanzitutto, per l'analisi della fattispecie delittuosa, è necessario preliminarmente soffermarsi sulla disciplina del consenso, analizzandone i suoi aspetti fondamentali.

---

[43] ZOTTA F., *Privacy*, a cura di CLEMENTE, Enc. Cendon, Padova 1999.

[44] Articolo 23 codice *privacy:* "Consenso": «Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato. Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso. Il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13. Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili».

[45] MANNA A., *Il quadro sanzionatorio ed amministrativo del codice sul trattamento dei dati personali, Dir. Inf.*, 2003 p. 756, in cui l'Autore sostiene che in tal modo si è coniato un illecito di mera disobbedienza.

Il consenso costituisce il principale elemento facoltizzante il trattamento dei dati personali ovvero singole operazioni[46]. È evidente la natura autorizzatoria del consenso, incidente su ambiti propri del diritto alla personalità individuale, e ciò lo si evince dal fatto che esso integra requisito di legittimazione e regola dell'attività di trattamento, e di ciò si ha conferma dalla giurisprudenza dell'Autorità Garante che ha munito di contenuto i singoli requisiti del consenso in modo funzionale a un corretto svolgimento dell'attività di trattamento e in modo da mettere il soggetto cui i dati si riferiscono in condizione di scegliere se conferire o meno i dati in modo realmente libero.

Quanto all'oggetto del consenso, esso –a seguito dell'accorpamento delle disposizioni previgenti che distinguevano tra consenso al trattamento e consenso ala circolazione dei dati– è riferito all'intero trattamento, salvo consentire un consenso limitato solo ad alcune delle operazioni in cui esso si compone. L'attuale formulazione della norma, dunque, affida il principio della segmentazione del consenso –in base al quale l'interessato può graduare i poteri concessi al titolare, limitandoli ad alcune fasi del trattamento, con esclusione di altre– esclusivamente alla facoltà di prestare il consenso solo per alcune operazioni del trattamento.

Il consenso deve essere espresso liberamente, in forma specifica e documentata per iscritto. La revocabilità del consenso non è espressamente prevista, ma la dottrina ne ammette la sua sostanziale esistenza in base alla natura giuridica; contempla infatti due rimedi affini: la cancellazione e il blocco dei dati da un lato, e l'opposizione al trattamento per motivi legittimi, dall'altro.

L'articolo 24[47] riunisce in considerazione dell'omogeneità di disciplina, le disposizioni che autorizzano il trattamento dei dati personali in assenza di

[46] ZENO ZENCOVICH, *Commento agli articoli 20 e 21 in* AA. VV. (a cura di) GIANNANTONIO, LOSANO, ZENO ZENCOVICH, *La tutela dei dati personali- Commentario alla legge 675/1996*, Padova, 1999.

[47] Articolo 24 codice *privacy*: "Casi nei quali può essere effettuato il trattamento senza consenso": «Il consenso non è richiesto, oltre che nei casi previsti nella Parte II, quando il trattamento:
a) è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria; b) è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato; c) riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i

consenso, facendo tuttavia salve alcune particolari ipotesi in cui il consenso resta necessario per la comunicazione dei dati e soprattutto per la loro diffusione.

Pertanto, si ritiene che tale disposizione non integri tanto un'eccezione alla regola del consenso, quanto piuttosto contiene un adattamento di tale regola alla particolarità del trattamento o dei dati, o alla connessione del trattamento a specifiche attività[48].

Tornando alla disposizione *de quo*, la previsione di una serie di casi in cui il trattamento può avvenire anche in assenza del consenso dell'interessato, pone il problema della qualificazione penalistica di tali situazioni,

limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati; d) riguarda dati relativi allo svolgimento di attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale; e) è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2; f) con esclusione della diffusione, è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000,n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale; g) con esclusione della diffusione, è necessario, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato; h) con esclusione della comunicazione all'esterno e della diffusione, è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, in riferimento a soggetti che hanno con essi contatti regolari o ad aderenti, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, e con modalità di utilizzo previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13; i) è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 6, comma 2, del decreto legislativo29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati. i-bis) riguarda dati contenuti nei curricula, nei casi di cui all'articolo 13, comma 5-bis. i-ter) con esclusione della diffusione e fatto salvo quanto previsto dall'art. 130 del presente codice, riguarda la comunicazione di dati tra società, enti o associazioni con società controllanti, controllate o collegate ai sensi dell'articolo 2359 del codice civile ovvero con società sottoposte a comune controllo, nonché tra consorzi, reti di imprese e raggruppamenti e associazioni temporanei di imprese con i soggetti ad essi aderenti, per le finalità amministrativo contabili, come definite all'articolo 34, comma 1-ter, e purché queste finalità siano previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa di cui all'articolo 13».

[48] Tali attività derogatorie possono essere raggruppate in tre categorie: la prima riconducibile alle finalità del trattamento (art. 24 lett. a, e, g, i); la seconda ricollegata alla regola del consenso alla provenienza delle informazioni (art. 24 lett. c); la terza riguarda i dati trattati nell'ambito di determinate attività, come quelle contrattuali, economiche, investigative, di organizzazioni senza scopo di lucro (art. 24 lett b, d, f, h).

nell'alternativa tra elementi negativi del fatto che ne escludono la tipicità e cause di giustificazione che privano la fattispecie del carattere dell'antigiuridicità.

A favore della prima alternativa, si afferma che l'individuazione in un apposito articolo di casi in cui è escluso l'obbligo di richiedere il consenso in capo all'interessato, costituirebbe valido argomento per considerare il trattamento effettuato ai sensi dell'articolo 24 come condotta di cui il diritto penale si disinteressa[49]. Autorevole dottrina[50] afferma che «ai fini della rilevanza penale, laddove sussista un valido consenso non si può ritenere in radice realizzato il fatto tipico; il consenso, pertanto, non pare operare quale causa di giustificazione, ai sensi e per gli effetti cui all'articolo 50 codice penale, poiché è necessaria l'assenza di un valido consenso ai fini della medesima sussistenza del fatto di reato».

Altra dottrina[51], invece, sostiene che «il trattamento di cui all'articolo 24, priverebbe la fattispecie integrata ai sensi del combinato disposto degli articoli 167 e 23, siccome coperta dalle scriminanti dell'esercizio del diritto o dell'adempimento del dovere».

La soluzione che sembra doversi accogliere è quella che ritiene la mancanza di un valido consenso da parte dell'interessato (che riguardi l'intero trattamento o una o più operazioni dello stesso) sia necessaria ai fini della configurazione del reato *de quo*, in quanto essendo il consenso, vero e proprio elemento negativo della fattispecie e rilevante quale scriminante.

Le altre fattispecie contemplate dal I comma della norma che punisce il trattamento illecito di dati, riguardano la violazione degli articoli 123, che detta la disciplina relativa ai dati di traffico, dell'articolo 126 che detta il regime dei dati relativi all'ubicazione, dell'articolo 129 riguardante gli elenchi degli abbonati ed infine dell'articolo 130, che riguarda le comunicazioni indesiderate.

---

[49] SCALISI A., Il diritto alla riservatezza, Milano, 2002, p. 511;

[50] MANNA A., *La protezione penale dei dati personali nel diritto italiano*, Riv. trim. dir. pen. Ec, 1993.

[51] CORASANITI G., *Sanzioni penali e depenalizzazione degli illeciti nella normativa a tutela dei dati personali*, in Danno e responsabilità, n.7/2002 p. 517.

Prevedendosi, per quel che attiene i dati relativi al "traffico", l'articolo 123[52] prevede la cancellazione dei dati non più necessari ai fini della comunicazione, consente il trattamento in caso di contestazione della fatturazione e ne disciplina la conservazione; prevede inoltre le condizioni specifiche che ne autorizzano il trattamento, il contenuto dell'informativa che deve essere fornita all'abbonato o all'utente e i soggetti abilitati al trattamento.

Imponendo poi l'articolo 126[53] l'anonimato per i «dati relativi all'ubicazione diversi dai dati relativi al traffico», ovvero nell'ipotesi diversa, il consenso

[52] Articolo 123 codice *privacy*: "Dati relativi al traffico": «I dati relativi al traffico riguardanti contraenti ed utenti trattati dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico sono cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione elettronica, fatte salve le disposizioni dei commi 2, 3 e 5. Il trattamento dei dati relativi al traffico strettamente necessaria fini di fatturazione per il contraente, ovvero di pagamenti in caso di interconnessione, è consentito al fornitore, a fini di documentazione in caso di contestazione della fattura o per la pretesa del pagamento, per un periodo non superiore a sei mesi, salva l'ulteriore specifica conservazione necessaria per effetto di una contestazione anche in sede giudiziale. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico può trattare i dati di cui al comma 2 nella misura e per la durata necessarie a fini di commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, solo se il contraente o l'utente cui i dati si riferiscono hanno manifestato il proprio consenso, che è revocabile in ogni momento. Nel fornire l'informativa di cui all'articolo 13 il fornitore del servizio informa il contraente o l'utente sulla natura dei dati relativi al traffico che sono sottoposti a trattamento e sulla durata del medesimo trattamento ai fini di cui ai commi 2 e 3. Il trattamento dei dati personali relativi al traffico è consentito unicamente ad incaricati del trattamento che operano ai sensi dell'articolo 30sotto la diretta autorità del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni e che si occupano della fatturazione o della gestione del traffico, di analisi per conto di clienti, dell'accertamento di frodi, o della commercializzazione dei servizi di comunicazione elettronica o della prestazione dei servizi a valore aggiunto. Il trattamento è limitato a quanto è strettamente necessario per lo svolgimento di tali attività e deve assicurare l'identificazione dell'incaricato che accede ai dati anche mediante un'operazione di interrogazione automatizzata. L'Autorità per le garanzie nelle comunicazioni può ottenere i dati relativi alla fatturazione o al traffico necessari ai fini della risoluzione di controversie attinenti, in particolare, all'interconnessione o alla fatturazione».

[53] Articolo 126 codice *privacy*: "Dati relativi all'ubicazione": «I dati relativi all'ubicazione diversi dai dati relativi al traffico, riferiti agli utenti o agli contraenti di reti pubbliche di comunicazione o di servizi di comunicazione elettronica accessibili al pubblico, possono essere trattati solo se anonimi o se l'utente o il contraente ha manifestato previamente il proprio consenso, revocabile in ogni momento, e nella misura e per la durata necessari per la fornitura del servizio a valore aggiunto richiesto. Il fornitore del servizio, prima di richiedere il consenso, informagli utenti e gli contraenti sulla natura dei dati relativi all'ubicazione diversi dai dati relativi al traffico che saranno sottoposti al trattamento, sugli scopi e sulla durata di quest'ultimo, nonché sull'eventualità che i dati siano trasmessi ad un terzo per la prestazione del servizio a valore aggiunto. L'utente e il contraente che manifestano il proprio consenso al trattamento dei dati relativi all'ubicazione, diversi dai dati relativi al traffico, conservano il diritto di richiedere, gratuitamente e mediante una funzione semplice, l'interruzione temporanea del trattamento di tali dati per ciascun collegamento alla rete o per ciascuna trasmissione di comunicazioni. Il trattamento dei dati relativi all'ubicazione diversi dai dati relativi al traffico, ai sensi dei commi 1, 2 e 3, è consentito unicamente ad incaricati del trattamento che operano ai sensi dell'articolo 30, sono la diretta autorità del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni o del terzo che fornisce il servizio a valore aggiunto. Il

dell'utente o dell'abbonato, oltre che stabilendo anche in relazione ad essi, il contenuto dell'informativa che deve essere fornita all'abbonato o all'utente ed i soggetti abilitati al trattamento.

L'articolo 129[54] prescrive l'osservanza del provvedimento che il Garante ha il dovere di adottare, in cooperazione con l'Autorità per le garanzie nelle comunicazioni e in conformità alla normativa comunitaria, in ordine alle «modalità di inserimento e di successivo utilizzo dei dati personali relativi agli abbonati negli elenchi cartacei o elettronici a disposizione del pubblico». Si nota quindi come si tratti di una norma penale in bianco, integrata dal provvedimento del Garante.

Ed infine l'articolo 130[55] vietando le c.d. "comunicazioni indesiderate", rende necessario il consenso per l'uso di sistemi automatizzati di chiamata per l'invio di materiale pubblicitario, ricerche di mercato o comunicazioni commerciali ed impone l'identificazione del mittente.

La violazione della norma configura un reato, anche esso proprio, del commerciante o del pubblicitario, al cui connotazione appare tuttavia non scevra da problemi. La norma mira ad evitare l'invadenza di messaggi automatizzati pubblicitari, e, dato ciò, non si comprende la ragione per cui,

---

trattamento è limitato a quanto è strettamente necessario per la fornitura del servizio a valore aggiunto e deve assicurare l'identificazione dell'incaricato che accede ai dati anche mediante un'operazione di interrogazione automatizzata».

[54]Articolo 129 codice *privacy*: "Elenchi di contraenti": «Il Garante individua con proprio provvedimento, in cooperazione con l'autorità per le garanzie nelle comunicazioni ai sensi dell'articolo 154,comma 3, e in conformità alla normativa comunitaria, le modalità di inserimento e di successivo utilizzo dei dati personali relativi agli contraenti negli elenchi cartacei o elettronici a disposizione del pubblico, anche in riferimento ai dati già raccolti prima della data di entrata in vigore del presente codice. Il provvedimento di cui al comma 1 individua idonee modalità per la manifestazione del consenso all'inclusione negli elenchi e, rispettivamente, all'utilizzo dei dati per le finalità di cui all'articolo 7, comma 4, lettera b), in base al principio della massima semplificazione delle modalità d'inclusione negli elenchi a fini di mera ricerca del il contraente per comunicazioni interpersonali, e del consenso specifico ed espresso qualora il trattamento esuli da tali fini, nonché in tema di verifica, rettifica o cancellazione dei dati senza oneri».

[55] Articolo 130 codice *privacy*: "Comunicazioni indesiderate": «Fermo restando quanto stabilito dagli articoli 8 e 21 del decreto legislativo 9 aprile 2003, n. 70, l'uso di sistemi automatizzati di chiamata o di comunicazione di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è consentito con il consenso del contraente o utente. La disposizione di cui al comma 1 si applica anche alle comunicazioni elettroniche, effettuate per le finalità ivi indicate, mediante posta elettronica, telefax, messaggi del tipo Mms (Multimedia Messaging Service) o Sms (Short Message Service) o di altro tipo. Fuori dei casi di cui ai commi 1 e 2, ulteriori comunicazioni perle finalità di cui ai medesimi commi effettuate con mezzi diversi da quelli ivi indicati, sono consentite ai sensi degli articoli 23 e 24, nonché ai sensi di quanto previsto dal comma 3-bis del presente articolo».

posto che il dato personale violato sarebbe il numero telefonico o la casella di posta elettronica, si sia stabilito di presidiare con la sanzione penale e non con la semplice sanzione amministrativa, tale condotta ed escludere il caso di messaggi pubblicitari effettuati tramite personale della ditta, spesso non meno invadenti di quelli invitai tramite mezzi automatizzati[56].

L'ultima parte del primo comma prevede un trattamento sanzionatorio più severo nel caso in cui il trattamento illecito si sostanzi nella "comunicazione" o "diffusione" a terzi degli stessi dati, condotte i cui contorni si ricavano dall'articolo 4 comma 1 lett l. e lett. m del codice *privacy*.

Consiste la condotta di "comunicazione" nel «dare conoscenza a uno o più soggetti determinati, diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione».

La condotta di "diffusione" consiste invece nel «dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione».

Ricordate le definizioni di tali operazioni, al riguardo, si rileva, come l'equiparazione da un punto di vista sanzionatorio di due condotte molto diverse tra loro, possa essere indice di una violazione del principio di ragionevolezza, con conseguente sospetto di incostituzionalità della norma; infatti, pur non essendo dubitabile che la diffusione di dati sia una condotta sicuramente più grave rispetto alla comunicazione, atteso che i destinatari della prima sono una pluralità indeterminata e non un singolo o più soggetti determinati come nella comunicazione, le due differenti aggressioni allo stesso bene giuridico sono punite ex art. 167, con la medesima pena.

Nonostante si tratti di una previsione già contenuta nella legge 675/96, in dottrina si discute circa la qualificazione giuridica del trattamento illecito che si sostanzi nella comunicazione o diffusione di dati, non essendo pacifico se tale condotta debba considerarsi circostanza aggravante o titolo autonomo di reato.

[56] CORRIAS LUCENTE G., *Il codice dei dati personali. Temi e problemi* (a cura di) CARDARELLI F., SICA S., ZENO ZENCOVICH V., Milano, 2004.

Se si optasse per la natura di mera circostanza aggravante, dovrebbe concludersi che anche la punibilità della comunicazione o diffusione di dati personali sia condizionata dalla presenza di un effettivo nocumento ai danni dell'interessato, ma ciò comporterebbe una forzatura del dettato normativo e un netto contrasto col tenore letterale della norma che riferisce l'inciso «se dal fatto derivi nocumento», solo al primo periodo del primo comma dell'articolo 167 e non anche al secondo.

Perciò, sembra più corretto affermare che tale previsione configuri una vera e propria fattispecie autonoma di reato, non riscontrandosi un rapporto di *genus ad species* rispetto all'ipotesi contemplata dal primo periodo del primo comma dell'articolo 167.

Pertanto, si ritiene corretto[57] interpretare la norma come espressione di due sotto fattispecie, e, precisamente: il trattamento illecito di dati personali, dal quale derivi un nocumento (*ex* articolo 167, comma 1, I periodo), ed il trattamento illecito di dati realizzato mediante comunicazione o diffusione (*ex* articolo 167, comma 2, II periodo).

È evidente come quest'ultima fattispecie si ponga in rapporto di progressione criminosa prima, e sanzionatoria dopo, rispetto alla prima e all'interesse tutelato, in quanto avente un grado di offensività maggiore rispetto quella che caratterizza il trattamento illecito.

Il secondo comma dell'articolo 167 del D.lgs. 196/2003 prevede anch'esso fattispecie eterogenee, a cui è riservato un disvalore maggiore, essendo, le condotte descritte dalla norma richiamata, punite con una pena maggiore rispetto a quella stabilita per le condotte previste dal primo comma, consistente nella reclusione da uno a tre anni.

La prima fattispecie contemplata riguarda la violazione dell'articolo 17[58] del Codice, il quale regolamenta il trattamento che presenta rischi specifici.

---

[57] CUFFARO V., D'ORAZIO R., RICCIUTO V., *Il codice del trattamento dei dati personali*, Torino, 2007.

[58] Articolo 17 codice *privacy*: "Trattamento che presenta rischi specifici": «Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti. Le misure e gli accorgimenti di cui al comma 1 sono prescritti dal Garante in applicazione dei principi sanciti dal presente codice, nell'ambito di una verifica preliminare all'inizio del trattamento,

Parte della dottrina[59] ha criticato tale fattispecie criminosa, ritenendo che, la fattispecie che viene a compimento dal combinato disposto degli articoli 17 e 167, potrebbe essere viziata da illegittimità costituzionale in quanto non rispettosa dei principi di legalità e tassatività della norma penale.

L'articolo 17 è rubricato "Trattamento che presenta rischi specifici" e appresta una tutela particolare per dei dati diversi da quelli sensibili e giudiziari, riferendosi ai dati relativi ai diritti e alle libertà fondamentali il cui trattamento può comportare appunto, rischi specifici. Fino a qui, *nulla quaestio*. Se non fosse che, le misure per evitare che tali rischi abbiano a concretizzarsi, sono genericamente individuate in prescrizioni del Garante nel rispetto dei principi del Codice, sia preliminarmente, *ab initio* trattamento, che *in itinere* con un eventuale interpello del titolare.

Le difficoltà e i dubbi di conformità con la Costituzione nascono sia dall'indeterminatezza dei beni che si vogliono tutelare più incisivamente (il richiamo a libertà, diritti fondamentali e dignità dell'interessato è oltremodo generico), che delle condotte da seguire per evitare di incorrere nelle sanzioni penali.

In altri termini, si contesta alla disposizione, la natura di norma penale in bianco, non in grado di orientare correttamente il comportamento del destinatario.

A tal proposito la dottrina ricorda, richiamando la giurisprudenza della Corte Costituzionale[60] che, affinché i principi della riserva di legge e di tassatività siano rispettati, è necessario che la legge determini sufficientemente non solo la condotta, ma anche l'oggettività del reato e cioè l'integrale sostanza della fattispecie criminosa[61]. Tali dunque dovranno essere i parametri ai fini della valutazione della legittimità costituzionale della norma in questione.

Ancora, è interessate un'altra osservazione.

---

effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare».

[59] CIRILLO G. P. *La tutela della privacy nel sistema del nuovo codice sulla protezione dei dati personali*, Padova, 2004.

[60] Sentenza Corte cost. n. 36/1964 e sentenza Corte cost. 168/1971

[61] RAMACCI F., *Corso di diritto penale*, Torino, 1991, vol. I, p. 72.

Appare evidente che il parametro della violazione consista nelle misure specifiche adottate dall'Autorità. Una norma orientata prettamente alla tutela delle funzioni del Garante è inserita in una fattispecie, invece, destinata alla tutela sostanziale dei dati da trattamento illecito.

La collocazione appare impropria[62]. Meglio sarebbe stato inserire tale previsione nella fattispecie che tutela le funzioni del Garante, lasciando intatta la natura del delitto di trattamento illecito come diretta violazione di norme legislative omogenee riguardanti il nuovo diritto ai dati personali.

La seconda fattispecie prevista dall'articolo 167 al secondo comma consiste nella violazione dell'articolo 20[63] del Codice, il quale disciplina i principi applicabili al trattamento dei dati sensibili da parte dei soggetti pubblici, trattamento consentito solo se autorizzato da espressa disposizione di legge, nella quale siano specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.

Nulla quaestio, oramai, sul fatto che il vero *discrimen* tra le condotte di cui al comma 1 e quelle di cui al comma 2 risieda nella tipologia dell'oggetto del trattamento, illecito, essendosi ritenuto carico di maggior disvalore astratto un trattamento illecito che presenta rischi specifici, ovvero avente ad oggetto dati sensibili o giudiziari.

---

[62]CORRIAS LUCENTE G., *La nuova normativa penale a tutela dei dati personali* in *Il codice dei dati personali. Temi e problemi*. CARDARELLI F, SICA S., ZENO ZENCOVICH V., Milano, 2004.

[63]Articolo 20 codice *privacy*: "Principi applicabili al trattamento di dati sensibili": «Il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite. Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g), anche su schemi tipo. Se il trattamento non è previsto espressamente da una disposizione di legge i soggetti pubblici possono richiedere al Garante l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi dell'articolo 26, comma 2, il trattamento dei dati sensibili. Il trattamento è consentito solo se il soggetto pubblico provvede altresì a identificare e rendere pubblici i tipi di dati e di operazioni nei modi di cui al comma 2. L'identificazione dei tipi di dati e di operazioni di cui ai commi2 e 3 è aggiornata e integrata periodicamente».

Un'ulteriore condotta criminosa è rappresentata dalla violazione degli articoli 21[64] e 22, commi 8 e 11 del Codice.

Entrambe le norme hanno in comune i destinatari, che devono essere soggetti pubblici.

La prima norma disciplina i principi che applicabili al trattamento dei dati giudiziari.

Per quel che interessa la seconda disposizione, soffermiamo l'attenzione in particolar modo su due commi, il comma 8 e il comma 11.

L'articolo 22 comma 8[65] che titola "Principi applicabili al trattamento di dati giudiziari e sensibili" prevede che «i dati idonei a rivelare lo stato di salute non possono essere diffusi». Si pongono in funzione di elementi negativi della tipicità (o di scriminanti) le disposizioni dell'articolo 24, che legittimano, alle condizioni tassativamente indicate, la diffusione di dati inerenti alla salute, anche senza il consenso dell'interessato.

L'articolo 22 comma 11[66], collegandosi al comma precedente prevede che «in ogni caso le operazioni e i trattamenti di cui al comma 10[67], se effettuati utilizzando banche dati di diversi titolari, nonché la diffusione dei dati

[64] Articolo 21 codice *privacy*: "Principi applicabili al trattamento di dati giudiziari": «Il trattamento di dati giudiziari da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili. Il trattamento dei dati giudiziari è altresì consentito quando è effettuato in attuazione di protocolli d'intesa per la prevenzione e il contrasto dei fenomeni di criminalità organizzata stipulati con il Ministero dell'interno o con i suoi uffici periferici di cui all'articolo 15, comma 2, del decreto legislativo 30 luglio 1999, n. 300, previo parere del Garante per la protezione dei dati personali, che specificano la tipologia dei dati trattati e delle operazioni eseguibili. Le disposizioni di cui all'articolo 20, commi 2 e 4, si applicano anche al trattamento dei dati giudiziari».

[65] Articolo 22 comma 8 codice *privacy: "*Principi applicabili al trattamento di dati sensibili e giudiziari"*:* «I dati idonei a rivelare lo stato di salute non possono essere diffusi».

[66] Articolo 22 comma 11 codice *privacy*: *"*Principi applicabili al trattamento di dati sensibili e giudiziari"*:* «In ogni caso, le operazioni e i trattamenti di cui al comma 10, se effettuati utilizzando banche di dati di diversi titolari, nonché la diffusione dei dati sensibili e giudiziari, sono ammessi solo se previsti da espressa disposizione di legge. Le disposizioni di cui al presente articolo recano principi applicabili, in conformità ai rispettivi ordinamenti, ai trattamenti disciplinati dalla Presidenza della Repubblica, dalla Camera dei deputati, dal Senato della Repubblica e dalla Corte costituzionale».

[67] Articolo 22 comma 10 codice *privacy: "*Principi applicabili al trattamento di dati sensibili e giudiziari"*:* «I dati sensibili e giudiziari non possono essere trattati nell'ambito di test psico-attitudinali volti a definire il profilo o la personalità dell'interessato. Le operazioni di raffronto tra dati sensibili e giudiziari, nonché i trattamenti di dati sensibili e giudiziari ai sensi dell'articolo 14, sono effettuati solo previa annotazione scritta dei motivi».

sensibili o giudiziari sono ammessi solo se previsti da espressa disposizione di legge».

Si noti come, la precedente norma, limitava la categoria dei dati giudiziari sensibili, ai soli dati penali e fallimentari (notoriamente gli unici iscrivibili nel casellario); l'attuale norma, comporta un ampliamento, non operando invece alcuna distinzione tra dati relativi a diversi settori dell'ordinamento giudiziario, fino a comprendervi quelli relativi all'esercizio di qualsivoglia giurisdizione civile, penale o amministrativa.

L'articolo 167 comma secondo punisce inoltre la violazione dell'articolo 25[68], il quale stabilisce i divieti di comunicazione e diffusione dei dati personali nell'ambito del trattamento effettuato da privati e da enti pubblici economici. Tuttavia, in virtù del disposto *ex* articolo 18 comma 5, le disposizioni di cui all'articolo 25 in tema di comunicazione e diffusione, si applicano anche ai trattamenti effettuati da soggetti pubblici. La violazione dell'articolo 25 si avrà nel caso di diffusione o comunicazione per finalità diverse da quelle indicate dalla notificazione, o se effettuate in inottemperanza del divieto stabilito dal Garante o dall'autorità giudiziaria, o riguardino dati per i quali sia stata ordinata la cancellazione o per i quali sia decorso il termine necessario per il raggiungimento dello scopo per il quale siano stati raccolti. Le eccezioni al divieto di comunicazione e di diffusione dei dati sono stabilite dal secondo comma dell'articolo 25.

Si perpetua in tal modo l'incongruenza già presente nell'archetipo[69], generata da una disposizione che sanzionava il trattamento, in violazione di norme di disciplina della comunicazione e diffusione, a loro volta individuate dalla norma penale come condotte autonome del reato[70]. Non si comprende perciò

---

[68]Articolo 25 codice *privacy*: "Divieti di comunicazione e diffusione": «La comunicazione e la diffusione sono vietate, oltre che in caso di divieto disposto dal Garante o dall'autorità giudiziaria: a) in riferimento a dati personali dei quali è stata ordinata la cancellazione, ovvero quando è decorso il periodo di tempo indicato nell'articolo 11, comma 1, lettera e); b) per finalità diverse da quelle indicate nella notificazione del trattamento, ove prescritta. Fatta salva la comunicazione o diffusione di dati richieste, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici ai sensi dell'articolo 58, comma 2, per finalità di difesa o di sicurezza dello Stato odi prevenzione, accertamento o repressione di reati».

[69] CORRIAS LUCENTE G. p. 491 in GIANNANTONIO- LOSANO- ZENO ZENCOVICH, *La tutela dei dati personali*, Milano 1999.

[70] MANNA A., *Il quadro sanzionatorio ed amministrativo del codice sul trattamento dei dati personali*, Dir. Inf. 2003.

se il legislatore sanzionando il solo trattamento in violazione di una norma che disciplina la diffusione e comunicazione, abbia inteso coniare una fattispecie qualificata dall'anticipazione della punibilità, valida a penalizzare la sola condotta di trattamento univocamente diretta alla diffusione, prima che questa sia realizzata, ravvisando un particolare pericolo, meritevole di severa sanzione.

Il reato di trattamento illecito dei dati può essere commesso anche in caso di violazione dell'articolo 26[71] del Codice, i cui destinatari sono i soggetti privati e gli enti pubblici economici, la quale detta le garanzie per i dati

[71] Articolo 26 codice *privacy*: "Garanzie per i dati sensibili": «I dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal presente codice, nonché dalla legge e dai regolamenti. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione, ovvero successivamente, anche sulla base di eventuali verifiche, il Garante può prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare. Il comma 1 non si applica al trattamento: a) dei dati relativi agli aderenti alle confessioni religiose e ai soggetti che con riferimento a finalità di natura esclusivamente religiosa hanno contatti regolari con le medesime confessioni, effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, sempre che i dati non siano diffusi o comunicati fuori delle medesime confessioni. Queste ultime determinano idonee garanzie relativamente ai trattamenti effettuati, nel rispetto dei principi indicati al riguardo con autorizzazione del Garante; b) dei dati riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria. b-bis) dei dati contenuti nei curricula, nei casi di cui all'articolo 13, comma 5-bis. I dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante: a) quando il trattamento è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, ente od organismo, sempre che i dati non siano comunicati all'esterno o diffusi e l'ente, associazione od organismo determini idonee garanzie relativamente ai trattamenti effettuati, prevedendo espressamente le modalità di utilizzo dei dati con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;
b) quando il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere odi volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2; c) quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Se i dati sono idonei a rivelare lo stato di salute e la vita sessuale, il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;
d) quando è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'articolo 111. I dati idonei a rivelare lo stato di salute non possono essere diffusi».

sensibili. Per il trattamento di tale categoria di dati è necessario, per la legittimità delle relative operazioni, oltre che l'osservanza dei presupposti stabiliti dalla legge e dai regolamenti, il consenso scritto dell'interessato e l'autorizzazione del Garante. Si prevedono altresì i casi in cui tale regola non si applica (terzo comma) e i casi in cui i dati sensibili possono essere trattati anche senza consenso, previa autorizzazione del Garante (quarto comma).

Norma articolata, reitera l'attenzione del legislatore verso i dati sensibili, meritevoli di accentuata protezione e rispetto; ciò giustifica l'inasprimento della pena edittale.

L'applicazione della sanzione penale prevista all'articolo 167 comma II si applica anche alla violazione delle garanzie per i dati giudiziari di cui all'articolo 27[72] del Codice, nell'ambito dei trattamenti effettuati da privati o da enti pubblici economici. In questo caso le operazioni potranno essere consentite solo se autorizzate da espressa disposizione di legge o provvedimento del Garante che specifichino le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e le operazioni eseguibili.

È chiaro si tratti di un tema particolarmente sentito dal legislatore, che edita più disposizioni in materia; aggiungendo anche l'inosservanza delle disposizioni del Garante ai casi in cui sia prevista la punibilità, amplifica l'eterogeneità degli interessi tutelati dall'unica norma penale nelle singole fattispecie in cui si scompone[73].

Infine, l'ultima condotta criminosa consiste nel mancato rispetto dei principi in materia di trasferimento dei dati verso Paesi terzi, cioè non appartenenti all'Unione Europea, di cui all'articolo 45[74] del Codice. Tale operazione è

[72] Articolo 27 codice *privacy:* "Garanzie per i dati giudiziari": «Il trattamento di dati giudiziari da parte di privati o di enti pubblici economici è consentito soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili. Si applica quanto previsto dall'articolo 21, comma 1-bis».

[73] CORRIAS LUCENTE G. *La nuova normativa penale a tutela dei dati personali* in *Il codice dei dati personali temi e problemi,* CARDARELLI F., SICA S., ZENO ZENCOVICH V., Milano, 2004.

[74] Articolo 45 codice *privacy*: "Trasferimenti vietati": «Fuori dei casi di cui agli articoli 43 e 44, il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, è vietato quando l'ordinamento del Paese di destinazione odi transito dei dati non assicura un livello di tutela delle persone adeguato. Sono valutate anche le modalità del trasferimento e dei trattamenti previsti, le relative finalità, la natura dei dati e le misure di sicurezza».

vietata quando l'ordinamento del Paese di transito o di destinazione non assicuri un livello di tutela delle persone, adeguato. Ai fini della valutazione dell'adeguatezza della tutela, sono prese in considerazione anche le modalità del trasferimento e dei trattamenti previsto, le relative finalità, la natura dei dati e le misure di sicurezza.

Tale articolo evoca il precedente articolo 35 l. 675/96 in violazione dell'articolo 27; muta tuttavia la gravità della pena, ne risulta inasprito il minimo della pena edittale, senza che sia individuabile il criterio di meritevolezza del dosaggio sanzionatorio applicato dal legislatore[75].

Analizzate le condotte incriminate dalla norma, si evince come sussista copiosamente una tecnica di rinvio alle norme di disciplina, e ciò rende, non solo poco cristallina la logica del codice, ma estremamente complesso e puntiglioso il lavoro dell'interprete nel chiarire con precisione i contorni della fattispecie, costringendolo di volta in volta ad individuare il cuore della norma di disciplina la cui violazione assurge a elemento essenziale del fatto di reato di trattamento illecito di dati, ovvero, in altre parole, a selezionare, nell'ambito delle norme di disciplina, gli aspetti più pregnanti la cui inosservanza si appalesa davvero significativa sul versante penalistico.

La verità è che l'articolo 167 lascia spesso spazio a ad ampi dubbi anche –se non soprattutto– in ordine alla identificazione della linea di demarcazione tra l'area del lecito e l'area dell'illecito dal punto di vista penalistico, non essendo ragionevole ritenere che i destinatari del precetto penale siano in molti casi in grado di districarsi all'interno dei meandri di un dettato legislativo che non brilla certo per la sua limpidezza.

Descritte le condotte vietate dall'attuale previsione, è necessario esaminare le altre componenti del reato.

Aldilà delle ipotesi delittuose connesse al trattamento da parte di soggetti pubblici, il reato *de quo* è un reato comune, in cui soggetto attivo può essere chiunque commetta un illecito nel trattare dati personali[76].

---

[75] CORRIAS LUCENTE G. *La nuova normativa penale a tutela dei dati personali* in *Il codice dei dati personali temi e problemi*, CARDARELLI F., SICA S., ZENO ZENCOVICH V., Milano, 2004.

[76] Aa. Vv., Le modifiche alla normativa in materia di privacy, La Tribuna, 2002 p. 122.

Il tentativo, in quanto fattispecie di pericolo non si ritiene sia configurabile, atteso che, altrimenti si andrebbe a sanzionare il pericolo di un pericolo con l'inevitabile conseguenza di far arretrare oltremodo la soglia della punibilità, con evidente pregiudizio dei profili connessi al rispetto del principio di legalità.

L'elemento soggettivo richiesto affinché si configuri il reato in questione, è il dolo specifico –«al fine di trarne profitto per sé o per altri o di recare ad altri un danno»– presente nel primo e nel secondo comma. Sicché a integrare la fattispecie non sarà sufficiente la semplice violazione delle disposizioni richiamate nei due commi della disposizione, accompagnata da un'adeguata rappresentazione e volizione, dovendosi riscontare anche una specifica finalità consistente nel fine di trarre per sé o per altri profitto o nel recare ad altri un danno.

La funzione del dolo specifico, nell'ambito della precedente fattispecie dell'articolo 35, valeva infatti a costituire un *discrimen* tra le condotte illecite e quelle lecite, sicché rispetto all'eventuale neutralità della condotta, il dolo assumeva ruolo decisivo per l'incriminazione.

Quanto all'esame del concetto di profitto, questo si presenta particolarmente ampio, dovendosi intendere per esso qualsiasi vantaggio e/o utilità, anche privi del requisito della patrimonialità, che siano ricavabili dal soggetto attivo come conseguenza del reato.

Secondo la Cassazione penale, il profitto «deve essere inteso come qualsiasi utilità o vantaggio ovvero, pregiudizio, anche di natura non patrimoniale, essendo sufficiente che l'agente abbia operato per il soddisfacimento di un qualsiasi interesse, anche psichico»[77].

Parte della dottrina[78], a titolo esemplificativo, cita i casi di *direct marketing* e delle informazioni commerciali per connotare il profilo economico del profitto connesso alla fattispecie *de qua*, almeno nelle sue più frequenti forme di manifestazione.

[77] Cass. Pen. Sent. 2 novembre 1994, in Rivista penale, 1995 p. 1349.
[78] BUTTARELLI G., *Banche dati e tutela della riservatezza*, Milano, 1997

Si può affermare quindi che, quanto al dolo specifico di profitto, volendo proporre una sua *interpretatio* non in chiave necessariamente patrimonialistica, così che valga come sinonimo di vantaggio, sembra problematico immaginare un'ipotesi di trattamento da cui il titolare non intenda ricavare un'utilità; se invece diamo al profitto un'accezione patrimoniale, il dolo specifico, in questo caso, come nell'altro alternativo di dolo di danno, rischia di soffocare la disposizione penale, che verrebbe ad applicarsi nelle sole eventualità in cui il titolare abbia effettuato un trattamento illecito per conseguire una qualche utilità economica, o per produrre intenzionalmente un danno patrimoniale ad altri (in un settore tra l'altro in cui, da un punto di vista civilistico, il danno risarcibile non è solo quello patrimoniale ma anche quello non patrimoniale).

Si ritiene che, i termini profitto e danno debbano essere intesi nella loro massima estensione, comprendendo tutte le situazioni di pregiudizio e vantaggio anche non patrimoniale; e inoltre che, la scelta del legislatore di qualificare il dolo in termini di intenzionalità specifica, miri ad evitare il ricorso da parte del giudice, nell'ambito del giudizio di colpevolezza, al dolo eventuale.

2.2. Requisito del nocumento: configurazione come condizione obiettiva di punibilità e clausola di riserva

Le critiche formulate sulla inoffensività di talune condotte[79] e sulla destinazione del dolo specifico, sembrano recepite dal legislatore che, nel Codice, aggiunge un'ulteriore componente del reato: «se dal fatto deriva nocumento», reiterata nel primo e nel secondo comma.

Per nocumento, –a seguire l'opinione consolidata formatasi in relazione ai delitti contemplati dal codice penale a tutela della riservatezza e della libertà di corrispondenza, nonché a quelli concernenti la violazione del segreto documentale– si intende «un qualsiasi reale pregiudizio, giuridicamente

[79] BLAIOTTA, *Le fattispecie penali introdotte dalla legge sulla privacy*, in Cass. Pen., 1999. P.806.

rilevante […] patrimoniale o non patrimoniale»[80]. Ed in effetti, è proprio intorno a questo reale pregiudizio che sembra costituirsi l'effettiva dimensione offensiva dell'illecito penale di cui si tratta, come ha sostenuto la Suprema Corte. «L'inclusione di questo concetto, nella fattispecie penale, con la revisione del dolo specifico […] sembra maggiormente tipizzare un evento di danno direttamente ed immediatamente collegabile e documentabile nei confronti di soggetti i cui dati raccolti sono riferiti […]. Pertanto, devono essere senza dubbio escluse le semplici violazioni formali e irregolarità procedimentali, ma anche quelle inosservanze che producano un *vulnus* minimo all'identità personale dl soggetto e alla sua *privacy* (da intendersi nella duplice valenza positiva e negativa […]) e non determinino alcun danno apprezzabile».[81]

Definito il concetto di nocumento, resta da risolvere la questione relativa all'inquadramento sistematico dello stesso, cioè a dire se si collochi tra le condizioni di punibilità, ovvero fra gli elementi costitutivi del reato.

Come già precisato all'inizio di tale paragrafo, la vecchia formulazione della norma, prevedeva al terzo comma un cospicuo aumento di pena nel caso in cui dal trattamento illecito fosse derivato un nocumento all'interessato, e cioè alla persona cui i dati stessi si riferivano.

Il nocumento, pur essendo scomparso come circostanza aggravante, è stato però inserito con la locuzione «se dal fatto deriva nocumento», in entrambe le ipotesi di trattamento illecito. Pertanto, per la configurazione del delitto in esame non basta più un semplice e illecito trattamento di dati, sebbene effettuato con il dolo specifico di trarne un profitto per sé o altri, ovvero di recare un danno, ma è proprio necessaria la presenza di un nocumento, in capo al soggetto che subisce il trattamento dei propri dati.

Nulla quaestio sulla previgente disciplina che qualificava il nocumento come circostanza aggravante, e il delitto *de quo* come reato di pericolo presunto (o astratto), e cioè tra i reati in cui il fatto costitutivo non produce un'effettiva

[80] MANTOVANI F., Diritto alla riservatezza e libertà di manifestazione del pensiero con riguardo alla pubblicità dei fatti criminosi, in AAVV, Il diritto alla riservatezza e la sua tutela penale.
[81] Cass. Pen., sez. III, 28 maggio 2004, Barone, in Cass. Pen. 2005, 1895, con nota di PALAMARA L., *Note in tema di rilevanza penale del trattamento illecito di dati personali*.

lesione al bene tutelato ma determina solamente un pericolo di pregiudizio per il bene stesso.

Con la nuova disciplina è evidente che il legislatore abbandoni lo schema di "delitto aggravato dall'evento"[82], che comportava una sensibile anticipazione della soglia di rilevanza penale della condotta del soggetto agente, per passare a una fattispecie più aderente al principio di necessaria offensività dell'illecito penale sancito dalla Costituzione.

L'*intentio legis* appare evidente: dotare di ulteriore connotazione lesiva la fattispecie, al fine di evitare che fatti neutri in riferimento al bene giuridico possano essere penalizzati.

«La formula utilizzata si presenta bizzarra»[83]. La previsione del nocumento come fenomeno che deve verificarsi, si inserisce in una fattispecie a dolo specifico, caratterizzata, nella dogmatica e nell'uso legislativo, dalla circostanza che l'obiettivo o il fine criminalizzato si pone aldilà delle componenti della fattispecie penale. Ebbene, a leggere l'attuale norma, il nocumento che deve verificarsi coincide con una parte del dolo specifico (recare ad altri un danno) e costituisce una duplicazione, che rende dogmaticamente complesso l'inquadramento della nuova componente del reato.

La questione dell'inquadramento sistematico del nocumento non è puramente teorica, in quanto comporta notevoli effetti in ordine alla configurabilità stessa del reato ed in particolare in relazione all'elemento soggettivo.

Infatti, se si ritiene che il nocumento rappresenti un elemento costitutivo del reato –sulla base dell'assunto che esso concorra a definire l'interesse penalmente rilevante, sotteso alla fattispecie incriminatrice–, allora lo stesso deve necessariamente rientrare, accanto agli altri elementi della condotta.

Se lo si considera, viceversa, come una semplice condizione obiettiva di unibilità e cioè «un avvenimento esterno, successivo o concomitante al fatto

[82] I reati aggravati o qualificati dall'evento sono quelli che comportano l'inflizione di una pena più grave se, oltre al fatto base, si verifica un evento ulteriore.

[83] CORRIAS LUCENTE G. *Sanzioni* in GIANNANTONIO E., LOSANO M. ZENO ZENCOVICH V. (a cura di) *La tutela dei dati personali commentario alla l 675/96,* Padova, 1999.

di reato e perciò distinto sia dalla condotta criminosa che dall'evento tipico e che può essere causato da azione volontaria o involontaria del colpevole oppure di terzi»[84], la conseguenza è che il danno cagionato al soggetto interessato dall'illecito trattamento dei dati personali non deve essere necessariamente oggetto di rappresentazione e volizione da parte del soggetto agente.

Sebbene la soluzione proposta dal primo orientamento ermeneutico sembri più aderente all'esigenza di adeguamento della disciplina in esame al principio costituzionale di colpevolezza, deve rilevarsi che, a sostegno della tesi che configura il nocumento come condizione obiettiva di punibilità[85], vi sono varie osservazioni necessarie.

La prima considerazione che si impone è di natura letterale, poiché il legislatore delegato, introducendo all'interno dell'originaria fattispecie, il requisito del nocumento, ha utilizzato l'espressione «se dal fatto deriva nocumento», laddove invece avrebbe utilizzato la diversa espressione «se il fatto cagiona un nocumento», se avesse voluto configurare detto elemento alla stregua di evento nella fattispecie.

Sembra inoltre deporre nel senso della natura di condizione obiettiva di punibilità del nocumento, anche la previsione del dolo specifico, altrimenti vi sarebbe stata un'incongruità nel prevedere quale evento del reato proprio il fine (o uno dei fini) perseguito dal soggetto, che, in quanto riconducibile agli stilemi del dolo specifico non è, notoriamente, necessario che si realizzi ai fini della consumazione del reato[86].

Un'interpretazione parzialmente divergente era stata fornita da una precedente sentenza del tribunale ordinario di Roma i cui si sosteneva che il delitto di trattamento illecito di dati personali, *ab origine* reato di pericolo a dolo specifico, fosse attualmente ascrivibile alla categoria dei reati di evento. Dunque «la lesione del bene protetto non deve essere potenziale ma effettiva,

---

[84] MANTOVANI F., *Diritto penale*, Padova, 1992, pp 814-815.

[85] In questo senso è la giurisprudenza della Corte dii Cassazione: Cass. Pen., Sez. III, 28 maggio- 9 luglio 2004 n. 30134, in Riv. Pen., 2005 p.52. inoltre Cass. Pen. Sez III 26 marzo- 1 luglio 2004, n. 26680, Modena, in Riv. Pen. 2005, p.163.

[86] MANNA A., *Il quadro sanzionatorio ed amministrativo del codice sul trattamento dei dati personali*, Dir. Inf. 2003.

con la conseguenza che la tutela penale è assicurata solo nei casi in cui la commissione del fatto criminoso risulti accompagnata dall'effettivo nocumento. […] Non vi è stata alcuna *abolitio criminis* rispetto all'originaria formulazione *ex* articolo 35 legge 675/96, in quanto la nuova normativa comporta solo una diversa organizzazione della fattispecie del reato, trasformando l'evento del danno, da circostanza aggravante a elemento costitutivo del reato»[87].

Tuttavia, come osservato da attenta dottrina[88], la previsione nell'ambito della medesima fattispecie, del dolo specifico e della condizione di punibilità, non si spiegherebbe nel senso di considerare il nocumento come elemento costitutivo del reato, ma, troverebbe la sua *ratio* nella volontà del legislatore delegato di individuare nel novero delle condotte che esprimono un'offesa al bene giuridico -e come tali meritevoli di pena- quelle che rivelano, in maniera più pregnante, il bisogno di pena. In tale prospettiva sarebbe possibile riscontrare un rapporto sinergico tra condizioni obiettive di punibilità e dolo specifico.

La *ratio* delle condizioni intrinseche di punibilità, diversamente da quelle estrinseche, si individua nella necessità di qualificare e attualizzare la lesione dell'interesse protetto dalla norma incriminatrice. Perciò si rimette alla discrezionalità del legislatore, sulla base di una valutazione di opportunità di politica criminale, la scelta di attivare la reazione penale solo quando l'offesa al bene raggiunga una certa intensità, ovvero quando venga cagionata una lesione ulteriore e più intensa, ma inscindibilmente connessa con quella espressa dagli elementi costitutivi del reato.

Una delle principali questioni problematiche attiene alla compatibilità tra condizioni obiettive di punibilità e principio di colpevolezza. Vi è il rischio che il ricorso alla categoria delle condizioni di punibilità rappresenti una sorta di comodo alibi per sottrarre alla disciplina del dolo e della colpa elementi del fatto delittuoso *strictu senso* inteso. In proposito si impone un

[87] Tribunale ordinario di Roma, composizione monocratica, 30 gennaio 2004, estensore Iannello.
[88] MANNA A., *Il quadro sanzionatorio ed amministrativo del codice sul trattamento dei dati personali*, Dir. Inf. 2003.

ripensamento a seguito della storia sentenza costituzionale 364/1988. Pertanto, si può sostenere che non possono sottrarsi al «*nulla poena sine culpa*» le condizioni di punibilità c.d. intrinseche, cui fa parte il nocumento, ammettendo che esse, siano, sul piano soggettivo, almeno coperte dalla colpa[89].

È interessante in proposito riportare la tesi sostenuta da autorevole dottrina[90], secondo la quale ritiene che nella fattispecie di cui all'articolo 167 si esalti la funzione del nocumento come condizione obiettiva intrinseca di punibilità, laddove essa fornisce la misura dell'offensività del fatto: il meccanismo di tutela può raffigurarsi come una struttura a cerchi concentrici, in cui l'argine più esterno è costituito dalla protezione della *privacy*, quello più interno dal nucleo di valori salvaguardati come fondamentali, tra i quali spicca la riservatezza.

La ricostruzione nel modo seguente della struttura della norma, oltre ad essere in linea con la disciplina del codice, permette di cogliere come la sanzione penale configuri *l'ultima ratio*, laddove sia intaccato il nucleo fondamentale di valori, presidiato, tra gli altri strumenti, dalla disciplina del trattamento dei dati personali.

Tale approdo consente di percepire che l'obiettivo immediato della tutela è proprio il diritto alla protezione dei dati, posto in posizione di diritto funzionale ai valori ex art. 2 del d.lgs. 196/2003.

Il nocumento, altro non è che la certificazione dell'offensività e della lesività della condotta, ma ponendosi al di fuori della fattispecie generale e astratta, non occorre che sia coperto dal dolo[91] sicché conseguentemente può spiegare un maggiore potenziale di salvaguardia rispetto a quegli stessi valori; e se, lo si fosse concepito, viceversa, come elemento costitutivo del reato, o evento del reato, proprio le difficoltà in punto di dimostrazione del dolo ne avrebbero indebolito la tutela.

---

[89] ANGIONI, *Condizioni di punibilità e principio di colpevolezza, i*n Riv. It. Dir. Proc. Pen., 1989, p. 733.

[90] MANNA A., *Il quadro sanzionatorio ed amministrativo del codice sul trattamento dei dati personali*, Dir. Inf. 2003.

[91] Corte cost. 24 luglio 2007 n.322.

Pertanto, possiamo affermare che l'esternalizzazione del nocumento, denota una scelta di mediazione del legislatore, il quale, scostandosi dal modello di criminalizzazione forte previsto dall'art. 35 della legge 675/96, che anticipava la punizione collocando il nocumento tra le aggravanti, è passato alla formulazione di un reato -cui si applica sempre il coefficiente del dolo specifico- da punire solo laddove sia rinvenibile un connotato di indubbia offensività[92].

Come affermato dalla Corte di Cassazione, la realizzazione delle finalità è irrilevante ai fini della consumazione del reato, essendo sufficiente che il soggetto si rappresenti lo scopo al quale tende la condotta illecita[93].

Il reato è procedibile d'ufficio, non essendo prevista la querela di parte. A tale ultimo riguardo è possibile osservare che, almeno con riguardo al trattamento posto in essere senza il consenso dell'interessato, sarebbe forse stato più opportuno prevedere la procedibilità a querela di parte[94].

In entrambe le fattispecie di cui ai commi primo e secondo dell'articolo 167, il legislatore, ripropone in apertura come nel precedente articolo 35, la clausola di riserva «Salvo che il fatto costituisca più grave reato», facendo salve altre ipotesi delittuose di carattere più generale, che sanzionano reati più gravi.

Si tratta di una clausola di salvaguardia assolutamente indeterminata, che, contrariamente a quanto accade per quelle determinate, non esclude il fenomeno del c.d. "concorso apparente di norme" con tutti i problemi connessi in sede di teoria generale del diritto penale[95].

La clausola di riserva in esame è stata introdotta con un emendamento presentato dal Senatore Senese, che ha evidenziato, in particolare, l'opportunità di far salva l'applicazione delle disposizioni di cui agli articoli

---

[92] LOTIERZO R. *Del nocumento nell'illecito trattamento dei dati personali ovvero dell'esigenza di ascendere alle origini di una incriminazione*, in Cass Pen., n. 4/2013, p. 1589.

[93] Cass. Sezione II 20 novembre 1991 Romano, Mass. Cass. Pen., 1992, fasc. 4 p. 34.

[94] VENZIANI P., Beni giuridici protetti p. 169. L'Autore ritiene che la soluzione della procedibilità a querela sarebbe stata da preferire sia in funzione deflativa, sia a garanzia dell'interessato medesimo, che ben potrebbe avere ragione di evitare la pubblicità del processo: lo *strepitus fo*ri e financo la pubblicazione della sentenza di condanna potrebbero infatti risultare indesiderati alla vittima nel timore che si risolvano in un ulteriore intervento invasivo e lesivo della propria vita privata.

[95] MANTOVANI F., *Diritto penale*, Padova, 1992.

323 e 326 c.p.[96], vale a dire le fattispecie incriminatrici poste a tutela della pubblica amministrazione contro aggressioni che provengono dal suo interno.

Vero è, però, per quanto attiene ai rapporti dell'articolo 167 del codice *privacy*, con l'articolo 326[97] del codice penale, che non tutte le rivelazioni o utilizzazioni costituiscono "comunicazioni", "diffusioni", o "utilizzazioni" attinenti a un "trattamento" di dati, né che vi sia corrispondenza tra la nozione di dati personali trattati e quella di notizie d'ufficio segrete. Sicché la clausola di riserva sembra entri in gioco, nel caso di specie, solo ove il pubblico agente "comunichi", "diffonda" ovvero, "utilizzi" nell'ambito di un "trattamento" di dati quelli, tra questi, coperti da "segreto d'ufficio".

Più intricato e complesso è il rapporto tra l'articolo 167 del codice *privacy* e l'articolo 323[98] del codice penale, che disciplina l'abuso d'ufficio. Il punto di intersezione tra le due fattispecie sembra potersi rinvenire nel caso in cui il pubblico ufficiale o l'incaricato di un pubblico servizio trattando dati personali in violazione delle disposizioni della normativa del testo unico che attengono al c.d. "trattamento" pubblico degli stessi, arrechi un nocumento all'interessato, «al fine di trarne per sé o altri un ingiusto vantaggio patrimoniale o di recare a altri un danno ingiusto».

È da osservare, in conclusione che, l'articolo 323 e l'articolo 326 prevedono una pena edittale identica nel massimo, ma inferiore nel minimo a quella stabilita dall'articolo 167 comma II del codice.

---

[96] BUTTARELLI G., *Banche dati e tutela della riservatezza*, Milano, 1997, p.535.

[97] Articolo 326 codice penale: "Rivelazione e utilizzazione di segreti d'ufficio": «Il pubblico ufficiale o la persona incaricata di un pubblico servizio, che, violando i doveri inerenti alle funzioni o al servizio, o comunque abusando della sua qualità, rivela notizie di ufficio, le quali debbano rimanere segrete, o ne agevola in qualsiasi modo la conoscenza, è punito con la reclusione da sei mesi a tre anni. Se l'agevolazione è soltanto colposa, si applica la reclusione fino a un anno. Il pubblico ufficiale o la persona incaricata di un pubblico servizio, che, per procurare a sé o ad altri un indebito profitto patrimoniale, si avvale illegittimamente di notizie di ufficio, le quali debbano rimanere segrete, è punito con la reclusione da due a cinque anni. Se il fatto è commesso al fine di procurare a sé o ad altri un ingiusto profitto non patrimoniale o di cagionare ad altri un danno ingiusto, si applica la pena della reclusione fino a due anni».

[98] Articolo 323 codice penale: "Abuso d'ufficio": «Salvo che il fatto non costituisca un più grave reato il pubblico ufficiale o l'incaricato di pubblico servizio che, nello svolgimento delle funzioni o del servizio, in violazione di norme di legge o di regolamento, ovvero omettendo di astenersi in presenza di un interesse proprio o di un prossimo congiunto o negli altri casi prescritti, intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale ovvero arreca ad altri un danno ingiusto, è punito con la reclusione da uno a quattro anni».

2.3. Il caso Google Vividown e la responsabilità dell'ISP

Gli illeciti più diffusi della rete sono quelli che tipicamente possono essere compiuti, anche nella realtà offline attraverso l'uso di dati altrui, o informazioni e quindi: diffamazione, aggressione al diritto alla *privacy*, al diritto alla riservatezza, al diritto all'identità personale. A compiere tali illeciti, sono molto spesso, utenti che, celandosi dietro l'anonimato sfuggono alle responsabilità giuridiche conseguenti al loro operato e spesso sfuggono anche alle inibizioni personali che altrimenti potrebbero frenare la condotta socialmente disapprovata[99].

Per questa ragione si punta a coinvolgere nell'attività di controllo i *providers*, accollando agli stessi la responsabilità di quanto viene immesso, diffuso o scambiato in rete perché responsabili di non aver posto in essere quanto era nelle loro possibilità al fine di evitare la commissione di illeciti o la diffusione degli effetti dannosi dello stesso adottando ad esempio i c.d. "programmi filtro", in grado di controllare il contenuto dei materiali immessi in rete.

Tuttavia, considerare *l'internet provider* in qualche modo responsabile delle violazioni commesse da un qualsiasi utente tramite il suo *server* appare sproporzionato rispetto alla concreta necessità di individuare un soggetto responsabile della violazione.

Vi possono essere si delle responsabilità ma dovute principalmente all'imperizia nello svolgere una preventiva analisi del soggetto che intende immettere contenuti in rete.

Sul punto, il processo "*Google Vividown*" si pone al centro di un dibattito che lo supera, in quanto coinvolge il nostro vivere nel mondo digitale, gli stessi diritti del mondo digitale[100].

Costituisce pietra miliare la questione che ha investito i responsabili *Google Italy e di Google Inc*: quattro cittadini stranieri subiscono le vicende di un

[99] DI CIOMMO F., *Il Diritto dell'informazione e dell'informatica*, Milano, 2010 pp. 850 e ss.
[100] FRANCESCHELLI R., *Rivista di diritto industriale*, Padova, 2010 pp. 347

processo italiano con il seguente capo di imputazione: consentire che venisse immesso per la successiva diffusione a mezzo internet, attraverso le pagine di *google.it* senza alcun controllo preventivo, un filmato.

La condotta che, pertanto, ci si aspettava da loro consisteva nell'effettuare un controllo preventivo sul contenuto del filmato, prima di consentire che venisse immesso in rete.

In termini giuridici, il tema attiene alla responsabilità del *provider*[101].

Sulla sua funzione e sulla sua eventuale responsabilità si contrappongono due scuole di pensiero. La responsabilità del *provider* è vista da alcuni come l'unico strumento per la responsabilizzazione della rete. Chi la combatte, difende invece il principio della libertà della rete stessa.

Il caso ha suscitato aspre reazioni soprattutto oltre Oceano, fino a sfiorarsi l'incidente diplomatico con l'ambasciatore degli Stati Uniti in Italia, Thorne, che, dopo avere appreso del dispositivo della sentenza di primo grado, ha riferito alla stampa che il proprio Paese era "negativamente colpito" per la decisione del giudice italiano.

Soffermandoci sul fatto.

Il processo scaturisce dalla pubblicazione, risalente al settembre 2006 di un filmato sull'*host Google Video,* che ritrae un ragazzo disabile umiliato (con espressioni offensive) e maltrattato (con il lancio di oggetti) da alcuni compagni all'interno di un edificio scolastico; nella ripresa si sentono anche frasi ingiuriose nei confronti dell'associazione *Vivi Down,* un'associazione volta appunto alla tutela delle persone down.

Incredibilmente, tale filmato diveniva, per qualche tempo, il più̀ cliccato nella categoria video divertenti di *Google-Video*, allora concorrente di *Youtube* e soltanto nel novembre 2006, su richiesta della polizia postale italiana (a sua volta allertata da un cittadino giustamente indignato), il filmato veniva rimosso da *Google*.

Giudicata separatamente la posizione dei ragazzi minorenni, il processo di Milano riguardava esclusivamente quattro soggetti apicali investiti di diversi ruoli nell'ambito di società della galassia *Google Inc* i quali dovevano

[101] TOSI E. *Le responsabilità civili, I problemi giuridici di internet,* Milano 2003, 495 ss.

rispondere in concorso tra loro, del delitto di diffamazione mediante omissione ai danni del giovane e della associazione *Vivi down*, nonché di trattamento illecito dei dati personali relativi al solo ragazzo video ripreso.

Per la prima imputazione è intervenuta sentenza assolutoria. Invece, per il delitto di trattamento illecito di dati personali, il giudice di merito è pervenuto alla condanna con motivazioni che, condivisibili o meno, costituiscono la pietra miliare per discutere sulla responsabilità dell'*isp* (*internet service provider*) per fatti che ledono la *privacy* degli individui.

Contro la decisione di primo grado proponevano appello sia le difese sia la Pubblica accusa.

Le difese denunciavano l'erronea applicazione dell'articolo 167 D.Lgs. 196/2003, che, secondo la loro prospettazione, non punirebbe affatto le violazioni dell'articolo 13 del medesimo decreto, sanzionate in via amministrativa dall'articolo 161; per di più, l'articolo 13 non imporrebbe alcun dovere di informativa "sugli obblighi imposti dalla legge" in tema di *privacy*; infine, nell'appello degli imputati si rilevava la mancanza di dolo in capo ai *manager*.

All'opposto, la Pubblica accusa riproponeva nell'atto di gravame le ragioni poste a sostegno dell'azione penale e, segnatamente, le argomentazioni giuridiche da cui emergerebbe un obbligo del *provider* di impedire i reati realizzati dagli utenti della rete.

La Corte d'Appello, capovolgendo la questione, ha assolto i *manager* di *Google*[102] per il reato di illecito trattamento di dati (art. 167 D.Lgs. 196/2003), in riforma della decisione di primo grado[103], sul punto ampiamente criticata dalla dottrina[104], confermando**,** inoltre,

[102] Segnatamente, sono tratti a giudizio i due amministratori delegati di *Google Italy*, il responsabile del progetto *Google Video* per l'Europa e il responsabile della *policy* per la *privacy* per l'Europa di *Google Inc*.

[103] Si tratta di Trib. Milano, Sez. IV, 24 febbraio 2010, n. 1972.

[104] Si richiamano qui, in particolare, le critiche avanzate, seppur sotto profili diversi, da BEDUSCHI L., *Caso* Google: *libertà d'espressione in* internet *e tutela penale dell'onore e della riservatezza*, in *Corr. mer*., 2010, in particolare p. 967; LOTIERZO R., *Il caso* Google-Vivi Down *quale emblema del difficile rapporto degli* internet providers *con il codice della* privacy, in *Cass. Pen*., 2010, pp. 1288 e ss.; MANNA A., *I soggetti in posizione di garanzia*, in *Dir. info*., 2010, pp. 779 e ss. Volendo si veda anche INGRASSIA A., *Il ruolo dell'*internet service provider *nel ciberspazio: cittadino, controllore o tutore dell'ordine? Risposte attuali e scenari futuribili di una responsabilità penale dei* provider *nell'ordinamento italiano*, 8 novembre 2012, pp. 9 ss.

l''insussistenza del delitto di diffamazione, realizzato da un utente di *Google Video* e contestato agli imputati in forma omissiva, mancando in capo al *provider* una posizione di garanzia e poteri impedivi.

La corte d'appello qualifica *Google Video* come *host attivo*, cioè come *provider* che non si limita a memorizzare le informazioni degli utenti ma svolge un'attività «non neutra rispetto all'organizzazione ed alla gestione dei contenuti degli utenti, caratterizzata anche dalla possibilità di un finanziamento economico attraverso l'inserimento di inserzioni»[105]. Secondo la Corte d'Appello, però, da tale qualifica non si può in alcun modo far discendere - come vorrebbe la pubblica accusa - un obbligo di predisporre un controllo preventivo in capo al *provider*, impossibile sia sotto il profilo quantitativo, per la mole di materiale caricata in rete, che qualitativo, non esistendo un filtro che verifichi semanticamente i dati sensibili eventualmente trattati nelle riprese e la corrispondente presenza di un consenso per tali dati[106]. Peraltro, continua la Corte, non sarebbe nemmeno possibile contestare in forma omissiva al *provider* il trattamento illecito di dati, trattandosi di reato di mera condotta, incompatibile con la clausola di equivalenza di cui all'articolo 40 cpv c.p., che opera esclusivamente in relazione ai reati d'evento.

Secondo il Giudice del gravame l'articolo 167, letto in combinato disposto con l'art. 13, non prevede un obbligo di informare gli *uploader* sui doveri loro incombenti, derivanti dal Codice della *privacy*; per di più, i *manager* di *Google* non tratterebbero in alcun modo i dati contenuti nei video caricati dagli utenti: il soggetto responsabile del trattamento dei dati contenuti nelle riprese diffuse tramite *Google* resta l'*uploader*.

Contro la decisione d'appello proponeva quindi ricorso per cassazione la Procura generale, limitatamente al delitto di illecito trattamento dei dati.

---

[105] C. App. Milano, ud. 21.12.12.

[106] È interessante riportare il passaggio della decisione a p. 30: «la valutazione dei fini di un immagine all'interno di un video in grado di qualificare un dato come sensibile o meno, implica un giudizio semantico e variabile che certamente non può essere delegato ad un procedimento informatico».

La Procura Generale nel proprio ricorso aveva sostenuto che *Google* avesse trattato i dati contenuti nel video. Tale conclusione sarebbe avvalorata dall'ampia nozione di "trattamento dei dati sensibili" prevista dal D.lgs. 196/2003 e, soprattutto, dall'irrilevanza delle limitazioni di responsabilità previste nel D.lgs. 70/2003 ai fini della disciplina sanzionatoria sulla *privacy*; in particolare: (a) lo stesso Decreto sul commercio elettronico escluderebbe all'art. 1, comma II, lett. b), la sua applicabilità in materia di tutela della riservatezza[107]; (b) *Google Video* non si limitava ad ospitare filmati altrui, ma li indicizzava, traendo anche un profitto dalle inserzioni pubblicitarie: avrebbe svolto, dunque, l'attività tipica del cd. *host attivo*[108], a cui non possono applicarsi gli articoli 16 e 17 D.lgs. 70/2003, non trattandosi di una mera memorizzazione di contenuti degli utenti.

Nel rigettare l'impugnazione, la Suprema Corte, con la sentenza in esame[109], conferma preliminarmente l'assenza di una posizione di garanzia in capo agli *internet service provider*, giacché nessuna disposizione «prevede che vi sia in capo al *provider*, sia esso anche un *hosting provider*, un obbligo generale di sorveglianza dei dati immessi da terzi sul sito da lui gestito»; parimenti, sottolinea la Cassazione, nessuna norma incriminatrice punisce un ipotetico obbligo dei *provider* di ricordare agli utenti di rispettare la legge.

Entrando nel vivo della propria decisione e nell'esame delle doglianze della Procura Generale, la Cassazione compie una pregevole attività di coordinamento tra la disciplina sul commercio elettronico (D.lgs.

---

[107] 7L'art. 1, comma II, specifica: "Non rientrano nel campo di applicazione del presente decreto: (...) b) le questioni relative al diritto alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle telecomunicazioni di cui alla legge 31 dicembre 1996, n. 675, e al decreto legislativo 13 maggio 1998, n. 171, e successive modificazioni". La l. 675/1996 è stata sostituita proprio dal D.Lgs. 196/2003.

[108] Alla categoria di *host* attivo si riconducono i provider che non si limitino a memorizzare sui propri server informazioni e dati altrui, ma compiano attività ulteriori quali l'indicizzazione, il filtraggio, la selezione o l'organizzazione dei contenuti. Si veda sul punto, tra gli altri, TOSI E., La responsabilità civile per fatto illecito *degli Internet Service Provider* e dei motori di ricerca a margine dei recenti casi *Google Suggest* per errata programmazione del *software* di ricerca e di *Yahoo!* Italia per link illecito in violazione dei diritti di proprietà industriale, in Riv. dir. ind., 2012, 44 ss.

[109] Cass. pen., Sez. III, 17 dicembre 2013 n.5107.

70/2003) e quella sulla *privacy* (D.lgs. 196/2003), specificando i confini della possibile responsabilità dell'*host provider* (*rectius* dei gestori).

Il punto è di centrale importanza perché la disciplina sul commercio elettronico pone alcune limitazioni di responsabilità per il *provider* in relazione agli illeciti realizzati dagli utenti attraverso i contenuti da loro pubblicati. Segnatamente, il D.lgs. 70/2003 all'art. 17 esclude per l'*host provider* un generale dovere di sorveglianza sui contenuti degli *uploader* e all'articolo 16 afferma l'irresponsabilità del *provider* per le condotte illecite tenute dagli utenti, qualora non ne fosse a conoscenza e se, una volta avvisato dall'autorità, abbia provveduto alla rimozione dei contenuti stessi[110].

Partendo dalla decisione del tribunale di Milano.

«Troppo rumore per nulla». Con questa fin troppo nota citazione letteraria si chiude la citata sentenza del tribunale penale di Milano laddove con essa il giudice ha inteso evidenziare che il clamore mediatico suscitato dal processo in questione sarebbe stato eccessivo e ingiustificato posto che la sentenza aveva finito per applicare principi già affermati nella giurisprudenza italiana.

Il giudice di merito ha evidenziato come fosse innegabile che sul *provider* incombesse un particolare obbligo ossia quello di corretta e puntuale informazione ai terzi che consegnavano il video e quindi i dati, con specifico riferimento alle norme «che concernono la necessità di procurarsi l'obbligatorio consenso in ordine alla diffusione di dati personali sensibili».

Pertanto, partendo da questo presupposto, come in sentenza si legge, ovviamente non può sussistere responsabilità *ex* articolo 167 codice *privacy* in capo al *provider*, poiché non può esigersi in capo a chi fornisca un semplice servizio di interconnessione, un persuasivo controllo rispetto a ognuno dei dati inseriti nel sistema.

Ma ciò non esonera da responsabilità colui il quale effettui il trattamento di dati in una qualsiasi delle numerosissime forme indicate dall'art. 4 comma 1 lett. a codice *privacy*, senza il prescritto consenso qualora venga provata la

[110] Cass. Pen. Sez. III, 17 dicembre 2013 n. 5107

piena consapevolezza della sua mancanza derivata da precisi indici rivelatori, quale senz'altro l'inadempimento rispetto all'obbligo di informazione[111].

Per l'analisi della pronuncia in commento bisogna concentrare l'attenzione sugli articoli 23 e 26 che si ritengono violati.

Il limite alla luce di tali riferimenti pare che il tribunale non abbia approfondito il giudizio attorno alla tipologia dei dati divulgati (le immagini videoriprese del ragazzo) restando indifferente rispetto alle sollecitazioni di accusa e difesa, volte a stabilire se si trattasse di dati relativi allo stato di salute o meno[112].

Il principio del consenso è un caposaldo dei trattamenti che avvengono in ambito privato, ma ciò su cui insiste il tribunale e che rappresenta il *novum* della sentenza è il fatto che non si rimprovera la mancanza di un'informativa all'interessato, ma la mancata prospettazione a coloro che inviavano il video dei rischi giuridici collegati alla condotta che ponevano in essere.

La responsabilità *per omissionem* dell'internet provider basata appunto sull'asserita assenza di una corretta a puntuale informazione, si fonda sia sull'articolo 13 riporta, sia per non meglio specificate ragioni di buon senso[113].

Ma l'articolo 13 codice *privacy*[114] nel disciplinare il contenuto dell'informativa riguardante il trattamento non fa alcun cenno ad avvisi circa l'obbligo di rispettare il codice stesso.

---

[111] LOTIERZO R. in Cassazione penale 2010 p. 3995

[112] La difesa sosteneva che essendo la vittima autistica e non affetta da sindrome di down, i dati che rivelano tale sua condizione non riguardano lo stato di salute.

[113] MANNA A. *Il diritto dell'informazione e dell'informatica* 2010 p. 780

[114] Art. 13 codice privacy: «L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa: a) le finalità e le modalità del trattamento cui sono destinati i dati; b) la natura obbligatoria o facoltativa del conferimento dei dati; c) le conseguenze di un eventuale rifiuto di rispondere; d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi; e) i diritti di cui all'articolo 7; f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile. L'informativa di cui al comma 1 contiene anche gli elementi previsti da specifiche disposizioni del presente codice e può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati».

Pertanto, la *ratio decidendi* della sentenza è evidente: visto che non è possibile fondare *ex* articolo 40 cpv c.p. un obbligo di controllo penalmente rilevante giacche lo si è escluso per il delitto di diffamazione, sarebbe illogico affermarlo per l'altro reato, ecco perché il giudice di *prime cure* ritiene di individuare un diverso obbligo giuridico , di corretta e puntuale informazione che ha la funzione di evitare che colui che intende immettere in rete materiale penalmente rilevante non sia preventivamente e specificamente edotto dalla normativa a riguardo, senza che invece sia costretto a ricercarla nelle pieghe del contratto.

Seppur nella decisione si parli di "piena consapevolezza" del *provider* la consapevolezza della mancanza del consenso, pare che alla fattispecie contestata sia stato applicato il coefficiente psicologico del dolo eventuale come voluta disattenzione, nonostante si tratti di un'espressione ossimorica e contraddittoria *in re ipsa* in quanto partecipa sia della natura del dolo che di quella della colpa per cui diventa una sorta di ibrido inaccettabile a livello dogmatico.

Anche qualora si riuscisse a superare l'*impasse* dogmatico, preclusivo di ogni ulteriore analisi, si dovrebbe appurare se, nel caso di specie, sussisteva una posizione di garanzia in capo al provider «definibile come uno speciale vincolo di tutela tra un soggetto garante e un bene giuridico determinato dalla incapacità totale o parziale, del titolare a proteggerlo autonomamente[115].

Sicuramente dalla decisione del tribunale si comprende come l'esistenza di diverse tipologie di prestatori di servizi nella società dell'informazione non permette di svolgere un discorso esaustivo, ma appare, d'altro canto, principio ragionevole, quello secondo il quale, la responsabilità del *provider* «per materiali immessi interamente e autonomamente da altri deve ancorarsi necessariamente a un'effettiva previa conoscenza del contenuto illecito, nonché a una concreta rappresentazione della possibilità di realizzazione del fatto di reato e accettazione del rischio (e dunque volizione), del fatto

[115] CARCANO *Codice penale. Rassegna di dottrina e giurisprudenza* 2000 pag 31.

medesimo, non essendo sufficiente una generica conoscibilità delle informazioni diffuse per suo tramite»[116].

Al tribunale di Milano va riconosciuto il merito di aver emesso una sentenza che ha chirurgicamente individuato un problema tentando di risolverlo a diritto vigente, mentre per altro verso, invocava una buona legge in materia. Sicuramente tale sentenza con le sue argomentazioni costituirà una base per qualsiasi discussione concernete la responsabilità del *provider* per fatti di illecito trattamento di dati personali.

La sentenza della corte d'appello, che capovolge la questione, costituisce un importante tassello nella ricostruzione della disciplina giuridica del *cyberspazio* e nell'individuazione del ruolo che è ivi affidato al provider[117]. Nella vicenda *Google Video* si gioca, infatti, molto del futuro della rete: non sarebbe possibile l'accesso a milioni di pagine se l'*host provider* dovesse verificarne il contenuto prima di permetterne l'accesso agli utenti del *web*.

Per la Corte, ma il giudizio è pienamente condivisibile, il governo di *internet* e le decisioni su quali contenuti debbano accedere alla rete e quali debbano restarne fuori non possono essere lasciati ai *provider*: «demandare ad un *internet provider* un dovere/potere di verifica preventiva, appare una scelta da valutare con particolare attenzione in quanto non scevra da rischi, poiché potrebbe finire per collidere contro forme di libera manifestazione del pensiero»[118]. Come rilevato da autorevole dottrina[119] «è inquietante, in sostanza, l'idea di un privato che verrebbe incaricato di esercitare una sorta di censura per conto dell'ordinamento, avendo i mezzi tecnici ma non quelli culturali per realizzarla».

---

[116] SPAGNOLETTI la responsabilità del provider per i contenuti illeciti di internet, in Giur. Merito, 2004.

[117] INGRASSIA A, *Il ruolo dell'internet service provider,* in Giur. Merito, 2004.

[118] Così la sentenza annotata, p. 28

[119] FORNASARI G., *Il ruolo della esigibilità nella definizione della responsabilità penale del* provider, in PICOTTI L. (a cura di), *Il diritto penale dell'informatica nell'epoca di* internet, Padova, 2004, p. 431.

In definitiva, la Corte d'Appello rettifica la decisione di primo grado nelle sue linee, per così dire, di politica-criminale: anche qualora la rete fosse la «sconfinata prateria di internet dove tutto è permesso e niente può essere vietato»[120] *l'host provider* non può esserne lo sceriffo.

È fondamentale perché richiede l'effettiva conoscenza dei contenuti illeciti, e contribuisce a limitare il ricorso al dolo eventuale in chiave incriminatrice.

In sintesi, le soluzioni adottate dalla sentenza trovano conferma normativa nella cornice della normativa vigente, che esclude qualsiasi forma di automatica od accessoria responsabilità del *provider* e – seppure dedicata al settore civilistico – risulta rispettosa del principio di colpevolezza, nella sua accezione maggiormente garantista[121].

Fino ad arrivare alla suprema corte. La suprema Corte nel confermare l'assoluzione dei rappresentanti legali di *Google Italy* S.r.l., sembra mettere un punto fermo sulla controversa questione inerente alla eventuale responsabilità penale del soggetto-utente o *internet provider* che intraprende il trattamento di dati personali senza il necessario consenso dell'interessato; senza trascurare che, in alcuni passaggi iniziali della motivazione, offre un interessante e utile contributo per l'esegesi e la classificazione sistematica del delitto di trattamento illecito dei dati personali e, più in generale, di tutto il vasto quadro legislativo che regola i comportamenti del mondo del *web.*

La suprema Corte pone alla base dell'ipotesi di responsabilità personale un presupposto di carattere generale contenuto alla lett. *f)* dell'art. 4 codice *privacy* laddove viene individuata la categoria del "titolare" nella: «persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza; di indirizzo delle finalità e delle modalità di trattamento dei dati».

In questo modo, se non si accerta un concreto potere di governo sul trattamento dei dati posti in rete, il soggetto che solo materialmente gestisce

[120] L'espressione, ormai nota, è contenuta nella sentenza di primo grado del presente processo a p. 95.
[121] CORRIAS LUCENTE G., Giurisprudenza di merito 2004 pp 2523.

il fluire delle informazioni elettroniche non può essere chiamato a rispondere del contenuto delle stesse. Afferma a questo punto il giudice della legittimità che mentre la definizione di "trattamento dei dati" stabilita tassativamente all'articolo 4 del codice della *privacy* è puntuale, esaustiva e comprensiva di tutte le possibili operazioni da compiere, non è altrettanto omnicomprensiva la definizione normativa della categoria di "titolare del trattamento". Ed infatti, la qualifica soggettiva di rilievo penale trarrebbe fondamento, non dalla qualificazione legale fornita dalla legge di settore, ma dal potere decisionale che la stessa legge attribuirebbe di finalizzare il trattamento, stabilendone le modalità operative e individuando gli strumenti utilizzabili.
Ebbene, il *provider* o l'hosting *provider* non può rientrare nella categoria formale del "titolare" poiché, secondo la disciplina del commercio elettronico, egli non dispone di alcun potere di gestione del trattamento dei dati in rete, ma è titolare soltanto di un potere di successiva inibizione del loro utilizzo. In questo modo la sua eventuale responsabilità penale per un trattamento illecito dei dati opererebbe soltanto quando non avesse osservato l'obbligo di rimuovere informazioni lesive di diritti dei terzi opportunamente segnalate.
l delitto di trattamento illecito di dati rappresenta uno di quei modelli di fattispecie incriminatrice che offrono oggi maggiori spunti di riflessione sul diritto penale contemporaneo e sugli itinerari che esso sembra destinato a percorrere nell'immediato futuro. Il richiamo è a settori legislativi in cui il dato del rischio naturale diventa requisito di punibilità, si pensi anche a materie che ancora attendono una compiuta regolamentazione, come gli infortuni sul lavoro, il complesso settore dei beni ambientali, l'ambito sanitario e della salute.
Il problema di fondo è proprio rappresentato dal valore che il legislatore ha inteso attribuire alla complessa previsione dell'articolo 4 che nella sostanza intendeva svolgere un ruolo di esaustiva regolamentazione, nelle originarie intenzioni, priva di lacune operative e qualificative, oltre la quale la legge non si sarebbe applicata.

La norma incriminatrice dell'articolo 167 del d.lgs. n. 196/2003 è esattamente incastonata in un reticolo normativo che, nel renderla diversa da come appare a una prima sommaria lettura, mette in evidenza tutti i numerosi profili di controversa applicazione. Si tratta di una "norma laboratorio" che porta con sé le problematiche dei più indicativi nodi teorici del diritto penale ma che il legislatore non ha munito di quei dispositivi per risolvere le ipotesi applicative controverse.

La Corte di cassazione invece accerta in concreto che non può essere trasferito il potere di gestione dei dati a particolari soggetti e individua una lacuna normativa che fa scattare l'operatività di un'altra disposizione estranea però al tessuto legislativo originario[122].

Secondo una similitudine ormai diffusa la rete è descritta come un'autostrada informatica[123]. I *service provider* ne sarebbero i gestori. Ma se la società autostradale fosse considerata sempre e comunque responsabile per le violazioni delle autovetture che la percorrono il traffico si bloccherebbe.

L'impatto che può avere sulla coscienza individuale e collettiva nonché sulla formazione dell'opinione e della sensibilità singola e di massa, la pubblicazione o non pubblicazione di un video immesso online da un utente tramite uno dei tanti provider, sia nel bene che nel male è altissimo. Pertanto, nasce l'esigenza di parametrare in modo attento l'eventuale imposizione in capo ai *provider* di un obbligo di controllo sui contenuti immessi in rete per conto dei clienti. Anche perché continuare a sottovalutare l'importanza di un sistema di responsabilità giuridica che sia in grado di funzionare anche rispetto agli illeciti commessi *online* vuol dire sottostimare i costi sociali che *internet* determina e trascurare la potenza del mezzo telematico[124].

In dottrina[125] è stato in più occasioni messo in rilievo come, fino ancora alla metà degli anni Novanta, non esistesse giurisprudenza significativa sulla

[122] TRONCONE P. *Il caso google e non solo,* nota a Cassazione penale, sez. III, sentenza 03/02/2014, n. 5107
[123] NEGROPONTE N. *Being digital*, 1995 e GATES B. *The road ahead* 1995.
[124] DI CIOMMO, *Il diritto dell'informazione e dell'informatica* 2010 pp 850.
[125] PEZZELLA Giurisprudenza di merito 2010 p. 2232

responsabilità per la diffusione di notizie e messaggi attraverso *internet*, se non negli Stati Uniti d'America[126].

Quanto all'inquadramento della figura dell'*internet service provider* alla sua possibile punibilità a titolo di concorso come autore del reato di divulgazione in rete di contenuti illeciti, veniva condivisibilmente rilevato in dottrina già oltre un decennio orsono come la stessa «si limita a situazioni marginali, ove a tale soggetto sia attribuibile la paternità dei dati in questione o almeno la loro riconducibilità , qualora egli agisca come un moderatore di newsgroup o di una *mailing list* e quindi provveda al controllo dei messaggi pervenuti e decida in ordine alla successiva disponibilità di essi per gli utenti del servizio» che l'utilizzazione dello schema della responsabilità concorsuale risulta invece consentita nella ipotesi in cui sia dimostrabile che il *provider* abbia consapevolmente fornito l'accesso a dati illeciti da altri immessi in rete; situazione anche questa in grado di assumere una valenza assai limitata, a causa della difficolta sia di provare il dolo del *provider* in riferimento ad un reato non ancora verificatosi, sia di derivare la sua responsabilità alla consapevolezza sopravvenuta in ordine ad un reato già perfezionatosi nei suoi elementi essenziali[127].

---

[126] DEMARTINI Telematica e diritti della persona, in Dir. Inf, 1996, 855 ricorda come i casi esaminati dai giudici di questo Paese (Cubby Ine. v. Compuser-ve Inc., S.D.N.Y., 1991; Stratton Oakmont Inc. v. Prodigy Servı`ees Co., S.C. Nassau County, 1995; Stern v. Delphi Internet Serrices Corp., S.C.N.Y. County, 1995) si sono conclusi con l'affermazione della totale assenza di responsabilità per il. contenuto dei messaggi e delle notizie diffuse in capo alle organizzazioni che, anche professionalmente e con spirito commerciale, diffondono «*on line services*» , che sono tutte state equiparate dal punto di vista della responsabilità al distributore di un mezzo di comunicazione di massa, piuttosto che all'editore.

[127] SEMINARA S. *La responsabilità penale degli operatori in Internet,* in D.Inf , 1998, 751 ove si sottolinea che «appare comunque chiaro che la ridotta capacità operativa dei due criteri ora esaminati potrebbe indurre verso la costruzione di una responsabilità colposa del provider conseguente alla violazione di un obbligo giuridico di impedire eventi illeciti, similmente a quanto già dispone l'art. 57 c.p. per il direttore o vicedirettore responsabile in tema di stampa periodica rispetto ai reati commessi con il mezzo della pubblicazione». Secondo tale Autore, però , se è vero che già all'epoca taluni interventi giurisprudenziali apparivano voler estendere ai giornali c.d. telematici a disciplina amministrativa della stampa o affermare una equiparazione tra gli organi di stampa e i siti Internet, tuttavia «il tentativo di estendere analogicamente la normativa penale vigente in tema di stampa è destinato inesorabilmente a infrangersi sul principio di legalità giacche´ l'art. 1 l. 8 febbraio 1948, n. 47 tassativamente stabilisce che ″sono considerate stampe o stampati, ai fini di questa legge, tutte le riproduzioni tipografiche o comunque ottenute con mezzi meccanici o fisico-chimici, in qualsiasi modo destinate alla pubblicazione».

3. *Falsità nelle dichiarazioni e notificazioni al Garante, art. 168 D.lgs. 196/2003*

La fattispecie di cui all'articolo 168, in funzione di assistenza all'attività del Garante, sanziona la falsità nelle dichiarazioni e notificazioni allo stesso.

Tale fattispecie era prevista al vecchio articolo 37 bis della legge 675/96 introdotto nell'impianto originario dall'articolo 16 del D.lgs. 467/2001, per rispondere a esigenze di ulteriore tutela delle funzioni tutorie del Garante, facendo evolvere la figura dell'omessa o incompleta notificazione da reato a illecito amministrativo, e creando un'apposita fattispecie penale proprio per le ipotesi di false comunicazioni al Garante; oggi la norma in esame ne riproduce *in toto* il dettato normativo, salvo la previsione integrativa dell'incriminazione del mendacio commesso nelle comunicazioni dovute al Garante, ai sensi dell'articolo 39[128] del medesimo testo unico[129]. Nella Relazione della Commissione Giustizia allo schema di decreto legislativo, si legge come tale modifica sia motivata da un'integrazione, per omogeneità di materia[130].

La norma recita: «Chiunque, nella notificazione di cui all'articolo 37[131] o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un

---

[128] Art. 39 codice della privacy: «1. Il titolare del trattamento e' tenuto a comunicare previamente al Garante le seguenti circostanze: a) comunicazione di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico non prevista da una norma di legge o di regolamento, effettuata in qualunque forma anche mediante convenzione; b) trattamento di dati idonei a rivelare lo stato di salute previsto dal programma di ricerca biomedica o sanitaria di cui all'articolo 110, comma 1, primo periodo. I trattamenti oggetto di comunicazione ai sensi del comma 1 possono essere iniziati decorsi quarantacinque giorni dal ricevimento della comunicazione salvo diversa determinazione anche successiva del Garante. La comunicazione di cui al comma 1 e' inviata utilizzando il modello predisposto e reso disponibile dal Garante, e trasmessa a quest'ultimo per via telematica osservando le modalita' di sottoscrizione con firma digitale e conferma del ricevimento di cui all'articolo 38, comma 2, oppure mediante telefax o lettera raccomandata».

[129] BANI, *commento all'art. 39 legge n. 675/96* in Nuove leggi civ. commentate 1999, II p. 750 ss.
DE RADA, *commento all'art 39*, in GIANNANTONIO E., LOSANO M. ZENO ZENCOVICH V. (a cura di) *La tutela dei dati personali commentario alla l 675/96*, Padova, 1999.

[130] Relazione allo schema del Codice.

[131] Art. 37 codice privacy: «Il titolare notifica al Garante il trattamento di dati personali cui intende procedere, solo se il trattamento riguarda: a) dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica; b) dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria; c) dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale; d) dati trattati con l'ausilio di strumenti elettronici volti a definire il

procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni»[132].

Orbene, l'articolo 39 – così come il previgente articolo 27 comma 2 legge 675/96–, prevede alcuni obblighi di comunicazione al Garante ad opera del titolare del trattamento. Nonostante tali obblighi non siano autonomamente sanzionati (ma l'omissione della comunicazione preclude il successivo trattamento dei dati, pena la violazione dell'art. 167), il legislatore delegato ha ritenuto opportuno sanzionare espressamente il mendacio nella comunicazione[133].

Nel Codice di protezione dei dati personali l'oggetto materiale del reato consiste: nelle notificazioni di cui all'articolo 37 (quelle relative al trattamento); per i procedimenti in corso o gli accertamenti, nelle comunicazioni, negli atti, documenti, o dichiarazioni. Si aggiunge dunque la "comunicazione". La condotta consiste per gli accertamenti, nel dichiarare o attestare falsamente notizie o circostanze o nella produzione di atti o

profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti; e) dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché' dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie; f) dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti. Il Garante può individuare altri trattamenti suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato, in ragione delle relative modalità o della natura dei dati personali, con proprio provvedimento adottato anche ai sensi dell'articolo 17. Con analogo provvedimento pubblicato sulla *Gazzetta ufficiale* della Repubblica italiana il Garante può anche individuare, nell'ambito dei trattamenti di cui al comma 1, eventuali trattamenti non suscettibili di recare detto pregiudizio e pertanto sottratti all'obbligo di notificazione. La notificazione è effettuata con unico atto anche quando il trattamento comporta il trasferimento all'estero dei dati. Il Garante inserisce le notificazioni ricevute in un registro dei trattamenti accessibile a chiunque e determina le modalità per la sua consultazione gratuita per via telematica, anche mediante convenzioni con soggetti pubblici o presso il proprio Ufficio. Le notizie accessibili tramite la consultazione del registro possono essere trattate per esclusive finalità di applicazione della disciplina in materia di protezione dei dati personali.

[132] In argomento, vedasi FLORENZA O., *Trasgressori puniti con multe più salate*, in Guida al diritto, Il sole 24 ore, 2003, n.8 pp. 146 e ss.

[133] Trattandosi di un'innovazione, la sua compatibilità rispetto ai criteri stabiliti dalla legge delega, va valutata considerando che il Governo era tenuto, ai sensi dell'art. 4 della legge 127/01 a emanare un testo unico […] coordinandovi le norme vigenti ed apportando alle medesime le integrazioni e modificazioni necessarie al predetto coordinamento o per assicurarne la migliore attuazione».

documenti falsi. La disposizione differenzia le condotte in un binomio: falsità documentali e dichiarative.

Si noti quindi come l'oggetto materiale del reato sia indicato con un'elencazione casistica dettagliata e quasi ridondante (atti o documenti, dichiarazioni o attestazioni) intenzionata a criminalizzare qualunque veicolo della falsità.

Autorevole dottrina aveva segnalato l'incoerenza dell'assimilazione di due fattispecie tanto diverse quanto a disvalore, quali l'omessa notificazione e la notificazione infedele; quest'ultima, insieme agli altri comportamento descritti dall'attuale art. 168, sanziona un fatto considerato come avente una perdurante rilevanza penale[134].

Ma la riforma, opportuna per un verso, non appare del tutto esente da critiche, se si considera che il legislatore del 2001, così come il legislatore del codice in commento, ha inteso scorporare dal testo dell'originario articolo 34, in materia di notificazioni, la sola condotta di falso ideologico, lasciando, viceversa, la fattispecie della notificazione incompleta nel dominio del depenalizzato articolo 163[135].

È evidente che le ipotesi sono delimitate da una zona d'ombra di difficile demarcazione e, tuttavia stabilire se si è in presenza dell'una o dell'altra, è fondamentale, sol che si pensi alle conseguenze sanzionatorie che ne derivano.

Ed invero, la notificazione falsa, unitamente alle altre ipotesi delittuose delineate dal nuovo art. 168 comporta l'assoggettabilità, salvo che il fatto non costituisca più grave reato, del responsabile, alla pena della reclusione da sei mesi a tre anni, mentre per l'illecito amministrativo, questo scatta in presenza di una notificazione incompleta e sono previste le sanzioni del pagamento di una somma di denaro da diecimila a sessantamila euro, oltre alla pubblicazione dell'ordinanza ingiunzione in uno o più giornali.

---

[134] AA. VV. *Le modifiche alla normativa in materia di privacy,* La tribuna, 2002. P. 141.

[135] BUTTARELLI G. *Banche dati e tutela della riservatezza: la privacy nella società dell'informazione*, Milano, 1997: il vecchio art. 34 L 675/96 prevedeva anche l'ipotesi di notificazione infedele, laddove considerava reato il fatto di colui che, pur effettuando la notificazione, fornisse notizie incomplete o non rispondenti al vero. Si era in presenza di una nuova ipotesi di falso ideologico in scrittura privata, incentrantesi sia nel mendacio vero e proprio che sulla parziale reticenza.

La fattispecie appare chiaramente posta a tutela dell'azione del Garante e segnatamente a garantire la massima trasparenza e fedeltà delle acquisizioni dichiarative o documentali, tesa a precludere ed eventualmente a sanzionare l'utilizzazione di atti o documenti suscettibili di fuorviarne le relative determinazioni, sulla base di erronei presupposti. Pertanto, possiamo affermare come il bene giuridico protetto e tutelato da questa disposizione sia proprio la funzione di garanzia e di controllo del Garante[136].

Per quanto riguarda la struttura di detta fattispecie, notiamo come si tratti di reato comune, soggetto attivo può essere chiunque, nonostante secondo alcuni autori si tratterebbe di reato proprio, potendo essere commesso solo dal soggetto che ha l'obbligo di notificazione al Garante, cioè dal titolare del trattamento[137]. Vi è però da segnalare che l'articolo 157 indica, tra i soggetti ai quali può essere domandata l'esibizione dei documenti o la richiesta di informazioni, nell'ambito dell'espletamento dei compiti del Garante, non solo il titolare, ma anche il responsabile, l'interessato o altresì soggetti terzi rispetto alle operazioni di trattamento.

Il reato si perfeziona nel momento in cui vengono rilasciate le false dichiarazioni o in cui vengono prodotti gli atti o i documenti falsificati.

Il dolo generico, sotteso all'illecito in esame, richiede la consapevolezza in capo all'agente dell'*immutatio veri,* ossia della falsità delle notizie e dei documenti o delle attestazioni utilizzate e la relativa idoneità in concreto a rivestire un'apparenza ingannevole per fatti e circostanze il cui accertamento o la cui esistenza assuma rilevanza nel contesto procedimentale, senza necessità dell'ulteriore elemento dell'*animus nocendi o decipiendi*[138].

La *ratio* di ritenere sufficiente il dolo generico consiste nell'insistere sulla necessità che la condotta in esame sia realmente idonea a ledere il bene interesse oggetto di protezione penale, valorizzando così maggiormente il

[136] CORASANITI G., *Sanzioni penali e depenalizzazione degli illeciti nella normativa a tutela dei dati personali*, in Danno e responsabilità, 2002.
[137] SCALISI A., Il diritto alla riservatezza, Milano, 2002.; ZOTTA F., *Privacy,* a cura di CLEMENTE, Enc. Cendon, Padova 1999; CIRILLO G. P. *La tutela della privacy nel sistema del nuovo codice sulla protezione dei dati personali*, Padova, 2004.
[138] MANNA A., *La protezione penale dei dati personali nel diritto italiano*, Riv. trim. dir. pen. Ec, 1993.

profilo dell'offensività della condotta medesima anche sul versante del profilo psicologico[139].

La clausola di riserva relativamente indeterminata «salvo che il fatto costituisca più grave reato», viene riprodotta dalla vecchia fattispecie e impedisce qualsiasi concorso formale tra reati, confermandone la natura di reato sussidiario che cede di fronte a un reato più grave, sotto il quale possa comunque essere sussunto il fatto concreto.

Tale fattispecie delittuosa è speciale rispetto alla fattispecie generale di falso ideologico in scrittura privata, di cui all'articolo 485 c.p.[140]

Per la particolare rilevanza costituzionale degli interessi coinvolti, tale condotta è punita con la reclusione da sei mesi a tre anni, e quindi più severamente dell'ipotesi ordinaria di falso, previsto all'art. 483 c.p.[141], che prevede la reclusione fino a due anni e che costituisce l'ipotesi generale di reato per le figure come quella in esame.

4. Omissione misure minime di sicurezza, art. 169 D.lgs. 196/2003

Il reato di omessa adozione delle misure di sicurezza, è punito, a titolo contravvenzionale, dall'articolo 169, rubricato «Misure di sicurezza», quindi con una dicitura poco appropriata a un contesto penalistico e che rimanda a istituti che non vengono in rilievo in questa sede, senza alcuna indicazione dell'illiceità, quasi venga delineata una norma di disciplina.

L'articolo 169[142], testualmente recita: «Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro.

---

[139] MANNA A., *La protezione penale dei dati personali nel diritto italiano*, Riv. trim. dir. pen. Ec, 1993.

[140] Articolo 485 c.p. (oggi abr): Falsità in scrittura privata: «Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma, in tutto o in parte, una scrittura privata falsa, o altera una scrittura privata vera, è punito, qualora ne faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considerano alterazioni anche le aggiunte falsamente apposte a una scrittura vera, dopo che questa fu definitivamente formata».

[141] Articolo 483 c.p.: "Falsità ideologica commessa dal privato in atto pubblico": «Chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a due anni. Se si tratta di false attestazioni in atti dello stato civile, la reclusione non può essere inferiore a tre mesi».

[142] Oggi abrogato

All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili».

Si tratta, dunque, di una fattispecie contravvenzionale, l'unica rinvenibile all'interno del Codice.

La condotta incriminata consiste nella mancata adozione delle misure minime di sicurezza, così come previsto dall'articolo 33[143] del codice in materia di dati personali, le cui modalità di concreta predisposizione si ricavano dall'analisi dell'articolo 34[144], che disciplina le misure minime in caso di trattamento con strumenti elettronici, dell'articolo 35[145] che ne

[143] Articolo 33 codice *privacy* "Misure minime": «Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.»

[144] Articolo 34 codice *privacy* "Trattamenti con strumenti elettronici": «Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal tecnico contenuto nell'allegato B), le seguenti misure minime: a) autenticazione informatica; b) adozione di procedure di gestione delle credenziali di autenticazione; c) utilizzazione di un sistema di autorizzazione; d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici; e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici; f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi; g) tenuta di un aggiornato documento programmatico sulla sicurezza; h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari».

[145]Articolo 35 codice privacy "trattamenti senza l'ausilio di strumenti elettronici: «Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici e' consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime: a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative; b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti; c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalita' di accesso finalizzata all'identificazione degli incaricati.»

disciplina l'adozione in caso di trattamento effettuato senza l'ausilio di strumento elettronici e dall'articolo 36[146] che regola gli aggiornamenti a cui le misure di sicurezza devono essere sottoposte. Inoltre, parte della disciplina si ricava dal disciplinare tecnico dell'allegato B del codice.

In sintesi, sembrerebbe che la condotta incriminata consisterà nella mancata adozione, in via preventiva, degli standard minimi di sicurezza richiesti dalla normativa in materia, che devono essere adottati al fine di evitare la distruzione o la perdita, anche accidentale, dei dati, o i casi di accesso non autorizzato o non conforme alle finalità della raccolta.

Ma il *fulcrum* del problema inerente all'esegesi di questa disposizione consiste nell'individuare con esattezza e precisione il contenuto delle misure minime di sicurezza. Esse, in forza del rinvio contenuto nell'articolo 33 t.u., possono definirsi come quelle che il legislatore ha ritenuto necessarie e sufficienti ad escludere rischi particolarmente gravi per dati sottoposti a trattamento.

La norma, pur avendo fatto uso del termine ambiguo "adottare", per poter avere un serio contenuto precettivo deve necessariamente fare riferimento alle concrete condotte in punto di adozione delle necessarie misure di sicurezza, in via generale, ed astratta, per realizzare, permanentemente ed effettivamente, quegli accorgimenti idonei a rendere sicuro il trattamento in atto. Sicché non vi è un "prima" e un "dopo". Ma vi è un'articolata serie di condotte, modellata secondo la normativa richiamata, che vanno poste in essere incessantemente, senza soluzioni di continuità.

La previsione di una norma *ad hoc* per la materia in esame è stata motivata con l'esigenza di assicurare anche in sintonia con orientamenti giurisprudenziali internazionali in materia di diritti dell'uomo, la necessaria trasparenza alle tipologie di trattamenti effettuati per tali finalità , in relazione ai tipi di operazioni e di dati oggetto di trattamento e alle esigenze di aggiornamento e conservazione dei dati medesimi.

[146]Articolo 36 codice privacy "adeguamento": «Il disciplinare tecnico di cui all'allegato B), relativo alle misure minime di cui al presente capo, e' aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.»

È importante rilevare come, afferendo la disciplina in parola a un settore caratterizzato da una costante evoluzione tecnologica, a contenuto spiccatamente specialistico, essa rappresenta indubbiamente una delle sedi privilegiate per forme di integrazione tra fonte primaria e fonte regolamentare, anche sotto il profilo delle disposizioni penali, ove il relativo affievolimento della riserva di legge può ritenersi legittimato dal fine di assicurare maggiore duttilità e dinamicità, nonché sufficiente determinatezza della normativa.

Tuttavia, la giurisprudenza costituzionale[147], in materia di riserva di legge, ha avuto modo di chiarire come il principio di legalità non possa ritenersi eluso ove sia una legge dello Stato –anche se diversa da quella incriminatrice– a stabilire «i caratteri, i presupposti, i limiti dell'atto o del provvedimento non legislativo che concorra a determinare la condotta illecita».

Orbene, il mero rinvio operato dalla norma in esame, alla fonte regolamentare non sembra soddisfi i requisiti richiesti dalla citata giurisprudenza costituzionale, dal momento che il contenuto del detto decreto appare del tutto svincolato da ogni tipo di predeterminazione legislativa e poiché la deroga, in tal modo operata, al principio della riserva di legge, non sembra nella specie bilanciata e legittimata, da una finalizzazione della stessa garanzia di una maggiore determinatezza del precetto penale. L'utilizzo da parte del legislatore delegato della nozione di "misure minime di sicurezza", quale parametro di liceità della condotta penalmente sanzionata, comporta un inevitabile, quanto inammissibile *vulnus* al principio di precisazione della norma penale.

Come rilevato da attenta dottrina[148] in relazione al rinvio ai regolamenti contenuta nel vecchio art. 36 della legge 675/96 «sarà necessario probabilmente anche in questo settore il ricorso a clausole di riserva di carattere generale facenti riferimento, ad esempio, allo stato di evoluzione

[147] Sentenza corte cost. 113/1972. In dottrina vedasi, PALAZZO F. C. voce Legge penale, in Dig. Disc. Pen. Vol. I, Torino, 1993 p. 353 ss.

[148] VENEZIANI P., in I beni giuridici tutelati dalle norme penali in materia di riservatezza informatica e disciplina dei dati personali, tratto da Il diritto penale dell'informatica nell'epoca di internet, a cura di PICOTTI L., Padova, 2004.

della tecnica (…) o a parametri fondati su criteri di esperienza e in ogni caso sarà inevitabile un prevalente riferimento al tipo di obiettivi (impedire gli accessi, le manipolazioni, la dispersione ecc dei dati) piuttosto che alle misure concrete da adottare, difficili da descrivere ed estremamente variabili in relazione al tipo, alle dimensioni, alle modalità di accesso, ecc delle banche dati».

Si comprende come tale disciplina sia diretta a prevenire il verificarsi di pregiudizi nella sfera privata degli individui, attraverso l'imposizione ai soggetti responsabili di una serie di obblighi di protezione diretti a garantire la sicurezza delle informazioni, al fine di evitare pericolo ai diritti degli interessati. La *ratio* pertanto si rinviene sempre nella protezione della riservatezza dei dati personali, che viene tutelato attraverso il bene strumentale della sicurezza nel trattamento, sussistendo tra sicurezza e riservatezza un rapporto così stretto che la violazione dell'una può portare anche la lesione dell'altra. La sicurezza, infatti, appartiene a pieno titolo a quei mezzi preventivi di tutela che hanno un'efficacia molto maggiore rispetto a quelli che operano successivamente al verificarsi dell'evento dannoso, proprio a causa di una sostanziale impossibilità di ripristinare lo status quo ante la lesione dei diritti protetti.

Si tratta dunque, di strumenti cui è opportuno assicurare la piena ed effettiva operatività, data la loro maggiore attitudine a garantire un'efficace tutela rispetto ai mezzi meramente reattivi.

Un profilo problematico attiene alla corretta individuazione dei soggetti responsabili, e cioè dei soggetti tenuti ad attivarsi per adottare le misure di sicurezza[149], recitando testualmente l'articolo: «Chiunque essendovi tenuto». Sicuramente tale responsabilità ricade sul titolare del trattamento di dati, e ciò perché questi è il diretto destinatario delle prescrizioni di legge che impongono di predisporre tutte le misure di sicurezza necessarie. In capo al titolare del trattamento, è da precisare, sussiste sia una responsabilità *in*

[149] MANTOVANI M., *Le fattispecie penali della legge n. 675/96 e le posizioni di garanzia*, in Dir. Inf. 2000, pp. 567-595.

vigilando sia una responsabilità *in eligendo*[150]*;* egli, dunque, è responsabile penalmente anche quando demanda i propri compiti ad altri, se omette di vigilare ed effettuare verifiche periodiche. Ciò non vale ad escludere la responsabilità penale del responsabile e dell'incaricato del trattamento, poiché anche, e soprattutto, quest'ultimo può omettere di compiere date operazioni previste dal codice come necessarie per garantire la sicurezza dei dati trattati. In conclusione, sembra che vi sia la violazione della norma ogni qualvolta, da parte di chiunque rientri nella gestione di un dato trattamento, vi sia la violazione di una norma sulla sicurezza.

Questo profilo, insieme alle difficoltà sorte nell'individuare il contenuto delle «misure minime di sicurezza», determina l'inserimento della norma *de quo* nella categoria delle norme penali in bianco, il che solleva molte perplessità tra gli interpreti, soprattutto per la prospettata lesione del principio di tassatività della norma penale, insito nell'articolo 25 della Costituzione, il quale esprime l'esigenza della sufficiente determinatezza della fattispecie.

Poiché ci troviamo dinanzi a una contravvenzione, per di più avente ad oggetto una condotta omissiva, il tentativo non è ontologicamente configurabile, riferendosi l'art. 56 c.p.[151] solo ai delitti.

La norma è costruita secondo la tecnica della fattispecie omissiva propria[152], atteso che il momento consumativo coinciderà con l'inizio del trattamento non accompagnato dalle misure di sicurezza[153], a prescindere dal verificarsi di un evento in senso naturalistico; si tratta pertanto di un reato di pericolo, in quanto ai fini della punibilità non è richiesto che dal fatto derivi

---

[150] Il titolare infatti, deve scegliere i responsabili tra persone dotate di esperienza, capacità ed affidabilità, che diano idonea garanzia del pieno rispetto delle disposizioni vigenti in materia di trattamento, ivi compreso il profilo della sicurezza. In secondo luogo, il titolare è tenuto a vigilare sulla puntuale osservanza delle norme di legge e delle proprie istruzioni.

[151] Articolo 56 codice penale: Delitto tentato: «Chi compie atti idonei, diretti in modo non equivoco a commettere un delitto, risponde di delitto tentato, se l'azione non si compie o l'evento non si verifica».

[152] CIRILLO G. P. *La tutela della privacy nel sistema del nuovo codice sulla protezione dei dati personali*, Padova, 2004.

[153] Il Garante ha precisato che la data di adozione delle stesse può essere dimostrata tramite ogni fatto che sia in grado di stabilirla in modo certo, aderendo al dato normativo di cui agli artt 2702, 2704 del codice civile, che, in materia di prove documentali, recano un'elencazione non esaustiva per attribuire il carattere della certezza temporale alla formazione di documenti, in Bollettino 14/15, anno IV, 2000, p. 19.

nocumento[154]. Ciò conferma, da un lato, la volontà del legislatore di rafforzare il carattere preventivo della norma di cui all'articolo 169, realizzato attraverso un'anticipazione della soglia di punibilità, dall'altro l'impostazione, in virtù della quale il trattamento dei dati personali, è assimilata alle attività pericolose, con conseguente tutela anche sul piano civlistico, in forza del rinvio operato dall'articolo 15 del D.lgs. n. 196/2003 all'articolo 2050 del codice civile[155].

In relazione all'elemento soggettivo del reato, essendo stato l'illecito previsto come contravvenzione rispetto all'originaria previsione della legge 675/96[156], viene richiesto indifferentemente il dolo o la colpa; per cui è punito con la medesima pena sia chi volontariamente non predisponga le misure di sicurezza, sia chi non effettua tale adempimento semplicemente per negligenza, imprudenza o imperizia.

La norma ridefinisce il contenuto dell'analoga misura dell'articolo 36[157] della legge 675/96 così come modificata dal D.lgs. 467/2001. Si segnala, preliminarmente, la conferma della scelta operativa del legislatore del 2001 di qualificare la fattispecie in termini contravvenzionali, assimilandola al regime delle ipotesi contravvenzionali previste in materia di sicurezza negli ambienti di lavoro, laddove il vecchio testo dell'articolo 36 configurava un'ipotesi delittuosa punita con la pena della reclusione fino a un anno[158].

---

[154] CORASANITI G., *Sanzioni penali e depenalizzazione degli illeciti nella normativa a tutela dei dati personali,* in Danno e responsabilità, 2002,

[155] Aa. Vv. 133: il confronto tra la fattispecie di cui all'art. 169 e l'articolo 15 del Codice denota che entrambe le norme, pur affrontando tematiche del tutto differenti, l'una sul piano penalistico, l'altra disciplinando un'azione in sede civile, hanno in comune la consapevolezza che l'attività di gestione dei dati sia un'attività oggettivamente pericolosa. Di conseguenza, si avrà l'applicazione dell'art. 2050 c.c. 3, in via ulteriore, del principio dell'inversione dell'onere della prova.

[156] Nell'art. 36 della legge 675/96 l'omessa adozione di misure necessarie alla sicurezza dei dati era considerato come delitto punito con la reclusione sino a un anno sia per l'ipotesi dolosa che per quella colposa. Per l'ipotesi dolosa era però prevista una vera e propria circostanza aggravante costituita dall'aver provocato un effettivo nocumento, che comportava un innalzamento della pena sia nel minimo che nel massimo e cioè da due mesi a due anni di reclusione.

[157] Chiunque, essendovi tenuto, omette di adottare le misure necessarie a garantire la sicurezza dei dati personali, in violazione delle disposizioni dei regolamenti di cui ai commi 2 e 3 dell'articolo 15, è punito con la reclusione sino ad un anno. Se dal fatto deriva nocumento, la pena è della reclusione da due mesi a due anni. 2. Se il fatto di cui al comma 1 è commesso per colpa si applica la reclusione fino ad un anno.

[158] Così facendo, il legislatore ha altresì risolto il profilo di incostituzionalità' dal quale era manifestamente affetta l-originaria fattispecie di reato (che prevedeva un identico trattamento sanzionatorio per il fatto doloso come per quello colposo).

L'articolo 169 testo 196/2003, viceversa contempla la pena dell'arresto fino a due anni o il pagamento di un'ammenda da diecimila a cinquantamila euro. La struttura del comma 2 dell'art 169, inserito dal comma 1 dell'articolo 14 del D.lgs. 467/01 nel corpo dell'originario articolo 36, costituisce un naturale sviluppo della configurazione della fattispecie di omessa adozione delle misure di sicurezza in termini contravvenzionali.

In particolare, si è previsto un meccanismo di estinzione del reato –che ricalca quelli previsti nella legislazione sugli infortuni sul lavoro– subordinato al pagamento di una somma pari al quarto del massimo dell'ammenda stabilita dal comma 1, qualificabile dunque in euro 10320,00 circa, oltre che all'adempimento delle prescrizioni fissate dal Garante.

Nello specifico, è prevista una sorta di oblazione, definita da una parte della dottrina come una sorta di ravvedimento operoso[159].

La norma stabilisce che, all'autore del reato, all'atto dell'accertamento o, nei casi complessi anche con successivo atto del Garante, vengano impartite le prescrizioni necessarie a regolarizzare il trattamento. Il termine entro il quale deve avvenire detta regolarizzazione non deve eccedere il tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà nell'adempimento, ma comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento della prescrizione, impartita dall'Autorità, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione. L'adempimento e il pagamento estinguono il reato. Viceversa, qualora l'autore del reato non si conformi alle prescrizioni del Garante, questi dovrà darne comunicazione alla competente procura della Repubblica, affinché riprenda il proprio corso il procedimento penale *medio tempore* sospeso.

Sicché, per avervi estinzione del reato, non sarà sufficiente che si verifichi una delle due condizioni indicate dal comma 2, le quali, a tal fine, dovranno ricorrere ed essere soddisfatte entrambe[160].

---

[159] ACCIAI R., *Le nuove norme in materia di privacy*, Santarcangelo di Romagna, 2003, p. 77.

[160] CORASANITI G., *Sanzioni penali e depenalizzazione degli illeciti nella normativa a tutela dei dati personali*, in Danno e responsabilità, 2002

La materia, proprio in forza della duttilità e della complessa determinatezza e specificazione delle misure di sicurezza, capaci di essere individuate, non nel concreto, ma soltanto attraverso clausole valutative, e data anche questa particolare procedura per l'estinzione del reato, meglio si collocherebbe nel settore degli illeciti amministrativi. Di fatti, si ritengono condivisibili le istanze di quella parte della dottrina[161] che, anche alla luce dei dubbi di costituzionalità suggerisce una trasformazione di detta contravvenzione in una semplice violazione amministrativa, in aderenza ai principi di frammentarietà, sussidiarietà ed *extrema ratio* del diritto penale, che giustificano il ricorso alla sanzione penale laddove questo sua strettamente necessario perché gli altri strumenti sanzionatori offerti dall'ordinamento, di natura civile, amministrativa, disciplinare, o altro, appaiono insufficienti.

La criminalizzazione non è stata neppure imposta dalla normativa europea; secondo il raffronto operato dalla dottrina[162], la Direttiva 95/46/CE non menziona il concetto di "misure minime" e non ne impone l'adozione; suggerisce, invece, l'apprestamento di misure individuate non già in un'ottica burocratizzata di comunicazioni e controlli, ma in riferimento a parametri obiettivamente individuabili: il tipo tecnico di trattamento prescelto, la qualificazione del dato da proteggere, le caratteristiche del sistema e delle applicazioni di elaborazione. Si nota quindi una radicalmente diversa impostazione tra il Testo Unico e la Direttiva, rispetto alla quale la normativa italiana, appare, ancora una volta, *overbreadth*, in quanto divaricata sensibilmente a causa delle formalità amministrative improprie, poste per di più in rapporto integrativo della stessa norma penale, e comunque obiettivamente determinanti una significativa incertezza tra gli operatori.

[161] MANNA A., *Il quadro sanzionatorio ed amministrativo del codice sul trattamento dei dati personali*, Dir. Inf. 2003.
[162] CORASANITI G., *Sanzioni penali e depenalizzazione degli illeciti nella normativa a tutela dei dati personali* in Pardolesi, Diritto alla riservatezza e circolazione dei dati personali, Milano 2003.

5. L'inosservanza di provvedimenti del Garante, art. 170 D.lgs. 196/2003

«Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 26 comma 2[163], 90[164], 150, commi 1[165] e 2[166], e 143, comma 1, lettera c) [167], è punito con la reclusione da tre mesi a due anni».

Tale fattispecie delittuosa era già contemplata e disciplinata nella sua fisionomia e nei suoi assi portanti, dall'art. 37[168] della legge n. 675/96, salvo che per l'ulteriore incriminazione per il caso di inosservanza dell'autorizzazione adottata dall'autorità, ai sensi dell'art. 90 t.u. in relazione al trattamento dei dati genetici, in ragione della «particolare delicatezza della materia disciplinata»[169].

---

[163]Articolo 26 comma 2 codice privacy: «Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione, ovvero successivamente, anche sulla base di eventuali verifiche, il Garante può prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare».

[164] Articolo 90 codice privacy: «1 Il trattamento dei dati genetici da chiunque effettuato è consentito nei soli casi previsti da apposita autorizzazione rilasciata dal Garante sentito il Ministro della salute, che acquisisce, a tal fine, il parere del Consiglio superiore di sanità.

2. L'autorizzazione di cui al comma 1 individua anche gli ulteriori elementi da includere nell'informativa ai sensi dell'articolo 13, con particolare riguardo alla specificazione delle finalità perseguite e dei risultati conseguibili anche in relazione alle notizie inattese che possono essere conosciute per effetto del trattamento dei dati e al diritto di opporsi al medesimo trattamento per motivi legittimi.

3. Il donatore di midollo osseo, ai sensi della legge 6 marzo 2001, n.52, ha il diritto e il dovere di mantenere l'anonimato sia nei confronti del ricevente sia nei confronti di terzi».

[165] Art. 150 comma 1 codice privacy: «1. Se la particolarità del caso lo richiede, il Garante può disporre in via provvisoria il blocco in tutto o in parte di taluno dei dati, ovvero l'immediata sospensione di una o più operazioni del trattamento. Il provvedimento può essere adottato anche prima della comunicazione del ricorso ai sensi dell'articolo 149, comma 1, e cessa di avere ogni effetto se non è adottata nei termini la decisione di cui al comma 2. Il medesimo provvedimento è impugnabile unitamente a tale decisione».

[166] Articolo 150 comma 2 codice privacy: «Assunte le necessarie informazioni il Garante, se ritiene fondato il ricorso, ordina al titolare, con decisione motivata, la cessazione del comportamento illegittimo, indicando le misure necessarie a tutela dei diritti dell'interessato e assegnando un termine per la loro adozione. La mancata pronuncia sul ricorso, decorsi sessanta giorni dalla data di presentazione, equivale a rigetto».

[167] Art. 143 lett. c codice privacy: « c) dispone il blocco o vieta, in tutto o in parte, il trattamento che risulta illecito o non corretto anche per effetto della mancata adozione delle misure necessarie di cui alla lettera b), oppure quando, in considerazione della natura dei dati o, comunque, delle modalità del trattamento o degli effetti che esso può determinare, vi è il concreto rischio del verificarsi di un pregiudizio rilevante per uno o più interessati;»

[168]Art. 37 l. 675/96: 1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi dell´articolo 22, comma 2, *o degli articoli 29, commi 4 e 5, e 31, comma 1, lettera l)*, è punito con la reclusione da tre mesi a due anni.

[169] Così la Relazione al d.lgs. 196/2003, p.63.

L'illecito di cui all'articolo 170 integra un tipico "delitto di infedeltà"[170], che trova riscontro nella disciplina dell'attività di altre autorità garanti.

La disposizione punisce, con la reclusione da tre mesi a due anni (identica pena prevista dall'articolo 37 della l. 675/96), tre condotte: la prima riguarda il mancato rispetto delle indicazioni che si accompagnano o seguono il rilascio dell'autorizzazione al trattamento dei dati sensibili, e cioè di quelle informazioni che, a causa della loro maggiore capacità offensiva e dei rischi discriminatori che ne scaturiscono, sono soggette a una disciplina più rigorosa rispetto ai dati comuni; la seconda riguarda l'inosservanza delle prescrizioni contente nella decisione finale del ricorso; e la terza l'inosservanza delle misure cautelari infra-procedimentali.

Non è chiara la ragione di questa unificazione legislativa, visto che l'insieme dei provvedimenti del Garante oggetto della disposizione, non sono riconducibili a una stessa tipologia: da una parte, infatti, si incontrano provvedimenti di autorizzazione al trattamento di c.d. dati sensibili e di dati genetici; dall'altra, invece, ci si imbatte in provvedimenti che il Garante adotta, in via definitiva o cautelare, in sede di ricorso o di reclamo proposto dall'interessato.

Già a livello intuitivo si coglie, invero, l'omogeneità della prima tipologia di provvedimenti richiamati, con altri che il Garante può adottare disciplinando le condizioni di liceità del trattamento dati. Poco chiaro, pertanto, il motivo per cui essi non siano stati più correttamente richiamati nella fattispecie di "trattamento illecito", a meno di non ritenere che al legislatore, anche in questo caso, formulando i contorni della figura criminosa, sia sfuggita di mano la tecnica del rinvio alla normativa di disciplina, sì da generare un'ulteriore ipotesi incriminatrice priva di razionalità e sistematicità.

Quanto alla struttura della norma, notiamo come venga adottata la consueta tecnica redazionale del rinvio a norme extra-penali. Parte della dottrina ha affermato che sia costruita sul modello dell'articolo 388 c.p. che incrimina la mancata esecuzione dolosa di un provvedimento del giudice[171]. Altra

[170] MANNA A., La protezione penale dei dati personali nell'ordinamento italiano, in Atti del quinto congresso int.le "Informatica e attività giuridica".

[171] IMPERIALI R., *Codice della Privacy,* Il sole 24 ore Pirola, Firenze, 2004,

dottrina[172] invece ritiene che la norma vada raffrontata con l'articolo 650 c.p., che disciplina l'inosservanza dei provvedimenti dell'Autorità, anche se ciò potrebbe esporre quest'articolo alle medesime critiche in ordine al rispetto dei principi di determinatezza e tassatività della fattispecie e del principio di riserva di legge[173], in quanto norma penale in bianco destinata a essere integrata, nel caso de quo, dal provvedimento del Garante[174].

Il rilievo che il contenuto precettivo della fattispecie sia individuabile a posteriori attraverso l'emissione del successivo provvedimento del Garante, ha consentito, di rilevare che la norma sarebbe costituzionalmente illegittima, esattamente come l'articolo 650 c.p., mantenuto però nel sistema dalla Consulta con sentenza non convincente.[175]

Sicuramente la norma in termini di determinatezza non rappresenta un esemplare, ma l'illegittimità costituzionale è conseguenza eccessiva; esiste infatti una profonda differenza tra l'articolo 170 codice *privacy* e l'articolo 650 del codice penale: tutti i provvedimenti tutelati dal codice di protezione sono atti che raggiungono il destinatario direttamente, che è posto in condizione di conoscerli ed eseguirli; non tutti i provvedimenti legalmente dati all'autorità presentano tale caratteristica, essendo riconducibili alla tipologia dei provvedimenti indicati all'articolo 650, anche atti di natura generale, non necessariamente conosciuti dal destinatario. Perciò si ritiene che l'assimilazione appaia più propria con l'articolo 388 c.p., il quale presidia l'autorità elle decisioni giudiziarie, in settori particolarmente sensibili, con l'intervento supplementare della sanzione penale.[176]

---

[172] CIRILLO G. P. *La tutela della privacy nel sistema del nuovo codice sulla protezione dei dati personali*, Padova, 2004.

[173] In tal senso, sebbene in relazione all'analoga formulazione dell'art. 37 della L. 675/1996, VENEZIANI P. *beni giuridici tutelati dalle norme penali in materia di riservatezza informatica e disciplina dei dati personali*, tratto da *Il diritto penale dell'informatica nell'epoca di internet,* a cura di PICOTTI L., Padova, 2004.

[174] RAMACCI L., *Diritto penale dell'ambiente,* Padova, 2009; ANTOLISEI F., Manuale di diritto penale. Parte speciale II 1997

[175] MANNA A., *La protezione penale dei dati personali nel diritto italiano*, in Rivista trimestrale di diritto penale dell'economia, 1993

[176] CORRIAS LUCENTE G. *Sanzioni* in GIANNANTONIO E., LOSANO M. ZENO ZENCOVICH V. (a cura di) *La tutela dei dati personali commentario alla l 675/96,* Padova, 1999

La *ratio* dell'articolo 170 si può rinvenire nel buon funzionamento e nell'efficacia dell'azione dell'Autorità Garante, pertanto il bene giuridico tutelato dalla norma in esame, che sanziona una mera disobbedienza, si individua proprio nella funzione di controllo del Garante per la protezione dei dati personali[177].

L'elemento soggettivo che viene richiesto per la realizzazione del reato è certamente il dolo, per cui l'inosservanza dovrà essere oggetto di rappresentazione e volizione da parte del soggetto attivo, non essendo sufficiente, per il delitto *de quo*, una semplice inosservanza o negligenza colposa.

Il reato si perfeziona nel momento in cui si sia consumato l'inutile decorso del termine fissato per l'osservanza del provvedimento, o nel caso in cui alla comunicazione dell'atto dell'autorità segua il comportamento vietato, ad esempio, nel caso di blocco o sospensione delle operazioni di trattamento, il soggetto obbligato continui le attività interdette.

La norma in esame prevede una tutela di tipo frammentario, in quanto non vengono penalmente sanzionate tutte le disobbedienze di provvedimenti al Garante, ma solo quelle considerate dal legislatore di una certa gravità; ed infatti si noti come siano presidiate dalla sola sanzione amministrativa le condotte che hanno l'effetto di ostacolare l'attività istruttoria del Garante, quali l'omessa informazione o esibizione di documenti richiesti dal Garante, prevista dall'articolo 164.

6. Le altre fattispecie, art. 171 D.lgs. 196/2003

L'articolo 171 statuisce: «La violazione delle disposizioni di cui agli articoli 113 comma 1 e 114 è punita con le sanzioni di cui all'articolo 38 della legge 20 maggio 1970, n. 300».

Prima facie si può osservare quanto appaia bizzarra la genericità della rubrica, che titolandosi «altra fattispecie», suscita l'idea che vi siano

[177] MANNA A. in a cura di FIORAVANTI L., in cui si sostiene che la norma sia posta a presidio della c.d. "funzione di trasparenza" del trattamento dei dati.

collocate norme eterogenee, prive di una componente unificatrice, quanto invece, non risulta dall'analisi della fattispecie, la quale punisce due condotte poste a tutela dei lavoratori.

Nello specifico, l'articolo 171 punisce il trattamento effettuato in violazione delle disposizioni di cui agli articoli 113 (Raccolta di dati e pertinenza)[178] e 114 (Divieto di controllo a distanza e telelavoro)[179] del testo unico. Tali ultime norme fanno riferimento, rispettivamente, agli articoli 8 e 4 della legge 300/1970 meglio nota come Statuto dei lavoratori; esse prevedono testualmente che «resta fermo quanto disposto» dai suddetti articoli[180].

L'articolo 8[181] dello statuto dei lavoratori fa espresso divieto al datore di lavoro di effettuare, sia ai fini dell'assunzione[182], sia nel corso dello svolgimento del rapporto di lavoro, indagini sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini dell'attitudine professionale del lavoratore.

Del pari, l'articolo 4[183] dello stesso statuto vieta al datore di lavoro di utilizzare impianti audiovisivi e altre apparecchiature per finalità di controllo a distanza dei lavoratori.

---

[178] Art. 113 codice privacy: «Resta fermo quanto disposto dall'articolo 8 della legge 20 maggio 1970, n. 300».

[179] Art. 114 codice privacy: «Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n. 300».

[180] DE ANGELIS, Controlli datoriali sulle telefonate dei lavoratori con il telefono aziendale; tutela della privacy e sanzioni disciplinari, in Giur. Piemontese, 2004 pp. 131- 147; Stenico, L'esercizio del potere di controllo informatico del datore di lavoro sugli strumenti tecnologici di ultima generazione in Riv. Giur. Lavoro, 2003 pp. 117 e ss.

[181] Art. 8 Statuto dei lavoratori: «È fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore».

[182] Cass. Pen. Sez III, 10 novembre 1998- 27 gennaio 1999, n.1133, Daubreè in Danno e resp., 1999 pp. 892 e ss.

[183] Art. 4 Statuto dei lavoratori: «Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione delle sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi».

Il reato di cui all'articcolo 171 deve considerarsi un reato proprio, potendo essere commesso solo da colui che ha la qualifica di datore di lavoro.

Il bene giuridico sotteso alla tutela penale si individua nella riservatezza del prestatore di lavoro e della sua libertà sindacale a non essere soggetto ad alcun tipo di controllo diretto sul posto di lavoro e *a fortiori* a non discriminato per nessun motivo.

La condotta materiale del datore di lavoro consiste nel porre in essere comportamenti diretti alle violazioni dei divieti suddetti, con dolo, ma è sufficiente anche la colpa, essendo ciò indifferente per la configurazione del reato, atteso il fatto che si tratti di un illecito contravvenzionale; il tentativo si ritiene escluso.

Le sanzioni penali previste per il datore di lavoro che pone in essere una condotta antisindacale, con il richiamo all'articolo 38[184] dello statuto dei lavoratori consistono nell'ammenda da 150 a 1500 euro o nell'arresto da 15 giorni ad un anno; nei casi più gravi, non ulteriormente specificati e rimessi all'interpretazione giurisprudenziale, le due pene possono essere applicate congiuntamente e quando il giudice ritiene le violazioni gravi ad essere può aggiungersi la pubblicazione della sentenza penale di condanna nei modi stabiliti dall'articolo 36 del codice penale. In tal caso, dunque, la pubblicazione della sentenza di condanna avviene per una contravvenzione e quindi al di fuori dei casi previsti dall'articolo 172 codice privacy.

Pertanto, si tratta di una contravvenzione punita con pena alternativa (salvi i casi più gravi puniti con pena congiunta), sicché può, di regola, trovare applicazione l'oblazione ex articolo 162 bis[185] codice penale. Normale deve

[184] Art. 38 Statuto dei lavoratori: «Le violazioni degli articoli 2, 5, 6, e 15, primo comma lettera a), sono punite, salvo che il fatto non costituisca più grave reato, con l'ammenda da lire 300.000 a lire 3.000.000 o con l'arresto da 15 giorni ad un anno. Nei casi più gravi le pene dell'arresto e dell'ammenda sono applicate congiuntamente. Quando per le condizioni economiche del reo, l'ammenda stabilita nel primo comma può presumersi inefficace anche se applicata nel massimo, il giudice ha facoltà di aumentarla fino al quintuplo. Nei casi previsti dal secondo comma, l'autorità giudiziaria ordina la pubblicazione della sentenza penale di condanna nei modi stabiliti dall'articolo 36 del codice penale».

[185] Art. 162 bis c.p.: «Nelle contravvenzioni per le quali la legge stabilisce la pena alternativa dell'arresto o dell'ammenda, il contravventore può essere ammesso a pagare, prima dell'apertura del dibattimento, ovvero prima del decreto di condanna, una somma corrispondente alla metà del massimo dell'ammenda stabilita dalla legge per la contravvenzione commessa, oltre le spese del procedimento».

ritenersi quindi il ricorso da parte della pubblica accusa al procedimento per decreto penale di condanna.

Quello che si realizza nell'art. 171 è un mero trapianto di norme, conseguente all'identità lesiva e di materia identificata dal legislatore, poiché anche lo Statuto dei lavoratori vieta il trattamento di taluni dati personali pertinenti ai lavoratori ne sanzionava la violazione.

Nonostante la tecnica legislativa del richiamo delle norme di disciplina risulti singolare e anomala (in quanto una disposizione del codice conferma la validità di una precedente disposizione, senza abrogarla), si ritiene che l'obiettivo perseguito dal legislatore sia stato quello di creare un unicum all'interno del Codice di protezione dei dati personali, al fine di dare attuazione e compimento agli articoli 4 e 8 dello statuto dei lavoratori che presentano un chiaro e preciso contenuto precettivo[186].

Un interessante provvedimento del Garante disciplina l'introduzione dei sistemi di videosorveglianza, attraverso l'installazione di telecamere su alcune linee di bus e tram e presso le fermate, per finalità di contenimento della criminalità. In tale provvedimento, il Garante ha affermato che l'attivazione dei sistemi, la localizzazione delle telecamere e le modalità di ripresa andranno fissate in aderenza ai principi fissati dalla legge, proprio in particolare nel rispetto dei principi di pertinenza e non eccedenza dei dati raccolti rispetto agli scopi perseguiti. L'attività di videocontrollo dovrà essere effettuata in modo tale da evitare non solo riprese particolareggiate troppo intrusive della riservatezza dei passeggeri, ma anche e soprattutto in modo da impedire la violazione delle previsioni di cui all'articolo 4 della legge n. 300/1970, in riferimenti alla posizione di guida degli autisti[187].

7. Le pene accessorie, art. 172 D.lgs. 196/2003

L'articolo 172 Codice *Privacy* chiude il Capo II, Parte III, dedicata alle sanzioni, contemplando e disciplinando la misura accessoria della

[186] MANNA A. il quadro sanzionatorio ed amministrativo sul codice sul trattamento dei danni personali, Dir. Inf, 2003.

[187] Provvedimento del Garante, 23 marzo 1999, in Bollettino n. 8, 57.

pubblicazione della sentenza di condanna, nei seguenti termini: «La condanna per uno dei delitti previsti dal presente codice importa la pubblicazione della sentenza», la disposizione trova il suo precedente normativo, riproducendone la lettera, nell'articolo 38[188] legge n. 675/96, il quale imponeva la pena accessoria della pubblicazione della sentenza di condanna per tutti i delitti previsti dalla legge medesima.

Ab origine la pena accessoria riguardava tutti i reati previsti dalla 675/96 allora prefigurati come delitti; ora non riguarda le contravvenzioni di cui agli articoli 169 e 170.

Notiamo come la disposizione preveda la pena accessoria da applicarsi *ex lege* tutte le volte in cui l'imputato venga condannato per uno dei delitti previsti dal codice, indipendentemente dal comportamento criminoso tenuto in concreto e, senza che il giudice possa valutarne l'opportunità caso per caso, al fine di limitare l'irrogazione ai soli casi più gravi.

Atteso che tale pena accessoria vada sempre irrogata, poiché sembra sfuggire al beneficio della sospensione condizionale ex articolo 163 c.p.[189], la dottrina è divisa su quale potrebbe esserne la *ratio*. C'è chi ritiene che miri a rafforzare la tutela penalistica accordata alla normativa in materia di protezione dei dati personali[190]; chi invece pone l'accento sulla sua portata deterrente con evidenti riflessi anche sul piano della tutela dei consumatori, i quali potranno beneficiare, nelle loro scelte di consumo dei beni, di un maggior spettro di informazioni[191].

Nulla quaestio sul fatto che tale obbligatorietà susciti non poche perplessità, poiché, *in primis* potrebbe esporsi a dubbi di legittimità costituzionale con riferimento all'articolo 27 comma 3 della Costituzione e in secondo luogo potrebbe essere controproducente per la vittima del reato; infatti comportando la generale divulgazione degli esiti di una vertenza, essa

[188]Articolo 38 l. 675/96: «La condanna per uno dei delitti previsti dalla presente legge importa la pubblicazione della sentenza».

[189]BUTTARELLI G. Banche dati p. 540, il quale ritiene, viceversa, che tale pena accessoria oltre a non avere una concreta efficacia dissuasiva (la considerazione assume rilievo per le piccole imprese), potrebbe fruire del beneficio della sospensione condizionale della pena;

[190] CIRILLO G. P. *La tutela della privacy nel sistema del nuovo codice sulla protezione dei dati personali*, Padova, 2004.

[191] IMPERIALI R., *Codice della Privacy*, Il sole 24 ore Pirola, Firenze, 2004.

potrebbe risultare indesiderata alla vittima che, dopo aver subito un illecito trattamento di dati protetti, si vedrebbe costretta a subire un ulteriore trattamento invasivo e lesivo della propria sfera privata[192].

Ma non da ultimo, interessante l'analisi di quella parte della dottrina che ritiene altresì nell'attuale sistema penale, tale misura accessoria sarebbe distribuita troppo indiscriminatamente: «siamo lontani dall'impostazione del codice Rocco del 1930, che prevedeva questa pena accessoria -vera e propria gogna moderna-, solo in casi marginali: l'esposizione del condannato e della sua famiglia, di riflesso, al disprezzo dell'opinione pubblica, era riservata alla condanna alla pena di morte o all'ergastolo, e alla condanna per pochi altri reati. La dignità –e, paradossalmente la riservatezza– del condannato, era protetta al massimo grado»[193].

Per quanto riguarda le modalità attraverso le quali avverrà la pubblicazione della sentenza di condanna, queste andranno individuate tenuto conto delle regole generali stabilite dall'articolo 36 c.p.[194] e dall'articolo 536 c.p.p.[195], dovendo avvenire per estratto e per una sola volta in uno o più giornali individuati dal giudice, il quale può anche disporne la pubblicazione per intero.

8. Conclusioni

Quel che resta del Codice *privacy* alla luce della recente innovazione legislativa, sono i principi informatori, che hanno ispirato nel corso del tempo il legislatore, alla tutela ed alla relativa disciplina del dato personale.

---

[192]VENEZIANI P., in I *beni giuridici tutelati dalle norme penali in materia di riservatezza informatica e disciplina dei dati personali*, tratto da Il diritto penale dell'informatica nell'epoca di internet, a cura di PICOTTI L., Padova, 2004.

[193] SGUBBI F. *Profili penalistici in Riv Trim dir e proc civ*, 1998 II.

[194]Articolo 36 c.p.: «La sentenza di condanna alla pena di morte o all'ergastolo è pubblicata mediante affissione nel Comune ove è stata pronunciata, in quello ove il delitto fu commesso, e in quello ove il condannato aveva l'ultima residenza. La sentenza di condanna è inoltre pubblicata, per una sola volta, in uno o più giornali designati dal giudice. La pubblicazione è fatta per estratto, salvo che il giudice disponga la pubblicazione per intero; essa è eseguita d'ufficio e a spese del condannato.
La legge determina gli altri casi nei quali la sentenza di condanna deve essere pubblicata. In tali casi la pubblicazione ha luogo nei modi stabiliti nei due capoversi precedenti».

[195]Articolo 536 c.p.p.: «Nei casi previsti dall'articolo 36 del codice penale, il giudice stabilisce nel dispositivo se la sentenza deve essere pubblicata per intero o per estratto e designa il giornale o i giornali in cui deve essere inserita».

Atteso che, la nuova legislazione è prevalentemente strutturata sulla base di ragioni ed esigenze di tutela che non sono più soltanto quelle nazionali, ma rispondono ad interessi, forme di tutela e di protezione di più ampio respiro europeo.
La conseguente struttura a macchia di leopardo del D.lgs. n. 101/2018 rende quasi impossibile tentare una esposizione sistematica degli interventi e delle interpolazioni rispetto al precedente sistema sanzionatorio e consente solo alcune indicazioni di sintesi per chiarire al lettore come la recente innovazione legislativa sia intervenuta sul testo previgente del Codice *privacy* 2003.

CAPITOLO III
LE NOVITÀ INTRODOTTE DAL DECRETO LEGISLATIVO 101/2018 E I PROFILI CRITICI DELLA DISCIPLINA

SOMMARIO: -1. *Introduzione. -2. Apparato sanzionatorio amministrativo. -3. Apparato sanzionatorio penale; .3.1. Trattamento illecito di dati personali ex articolo 167; -3.2. Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala, articolo 167-bis d.lgs. 196/2003; -3.3. Acquisizione fraudolenta di dati personali, articolo 167-ter d.lgs. 196/2003; -3.4. Osservazioni sui nuovi articoli 168, 170, 171, 172 Codice privacy. -4. Fattispecie penali e amministrative: rischio di violazione del ne bis in idem?. -5. La tutela del dato personale e la responsabilità degli enti ex d.lgs. 231/2001.*

1. Introduzione

Dopo un lungo e travagliato *iter* legislativo, il 4 settembre è stato pubblicato nella Gazzetta Ufficiale n. 205 il decreto legislativo 101 del 10 agosto 2018 contenente le disposizioni per l'adeguamento della normativa nazionale ai principi del Regolamento europeo 2016/679/UE relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati).

La miscela combinata del Regolamento 679/2016 (*GDPR*), che ha sostituito la Direttiva n. 95/46 e del decreto legislativo 101/2018 (il Decreto) che ha modificato il decreto legislativo 196/2003 (Codice *privacy*) è stata definita in sede di primo commento come "esplosiva"[1].

Preliminarmente è opportuno tener presente che l'attuale quadro normativo in materia di protezione dei dati personali in Italia si compone del *GDPR* e del codice *privacy* (D.lgs. 196/2003 come novellato dal Decreto) – che non rappresenta più l'intera normativa nazionale in materia di protezione dei dati

[1] PANETTA R, *Decreto di adeguamento GDPR: come cambiano le sanzioni e gli illeciti penali del Codice Privacy*, Quotidiano giuridico, 2018.

personali, ma ne diventa accessoria rispetto al *GDPR*–; pertanto l'Italia si conferma uno dei paesi con la normativa *privacy* più complessa e articolata.

La funzione del decreto legislativo n. 101/2018 è quindi quella di armonizzare le norme enunciate dal nostro legislatore nel Codice in materia di protezione dei dati personali (D.lgs. 196/2003) con quelle introdotte dal Regolamento Europeo 2016/679 entrato in vigore il 25 maggio.

A seguito del nuovo decreto di adeguamento, il vecchio Codice *privacy* risulta non solo profondamente novellato nelle sue disposizioni ma anche fortemente modificato nella sua ispirazione di fondo, e nella sua stessa finalità.

Questo aspetto è ribadito dal fatto che il D.lgs. 101 abroga *in toto* l'articolo 2 del d.lgs. n. 196 del 2003 e lo sostituisce con un nuovo articolo 2 che specifica: «Il presente Codice reca disposizioni per l'adeguamento dell'ordinamento nazionale alle disposizioni del Regolamento».

Il contenuto di questa disposizione ripete sostanzialmente il titolo stesso del decreto 101.

Si tratta di una ripetizione consapevole e voluta, allo scopo di specificare, anche nel quadro del sistema normativo del Codice novellato, che la finalità del Codice stesso è limitata a contenere le disposizioni nazionali di adeguamento al *GDPR*[2].

Dunque, le norme in esso presenti si collocano unicamente nell'ambito specifico della competenza nazionale assegnata agli Stati dal Regolamento.

Tale decreto è stato emanato nel rispetto di quanto sancito dall'articolo 13 della legge n. 163/2017 che contiene una delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del *GDPR*.

La tecnica legislativa adottata dal legislatore è stata quella di evitare di duplicare alcune disposizioni, molto simili ma non coincidenti, presenti sia nel regolamento che nel codice, operando cosi una scelta chiara.

In effetti codice e regolamento sono informati a due filosofie diverse. Il regolamento, come è noto, è basato sulla cosiddetta *accountability*. Si è pertanto voluto dare un segnale del cambiamento intervenuto: cioè del

[2] PIZZETTI F., *I consigli per leggere e applicare bene il decreto 101/2018*, www.agendadigitale.it.

passaggio dalla direttiva 95/46/CE al regolamento 2016/679/UE. Dopo oltre vent'anni, la disciplina della protezione dei dati personali è stata oggetto di una riformulazione non formale ma sostanziale, essendo cambiato l'approccio stesso alla materia che oggi è appunto dominata dal principio dell'*accountability*.

Dunque, il provvedimento comunitario non effettua la scelta in molti casi specifici, ma la rimette al titolare del trattamento che è chiamato ad effettuare una valutazione, ad assumere una decisione e a provare di avere adottato misure proporzionate ed efficaci.

L'entrata in vigore del decreto è immediata e integrale e senza alcun periodo di applicazione "*soft*" o "di transizione" delle attività di ispezione e sanzione del Garante.

Il *GDPR* è, parametro di legittimità della normativa nazionale, in virtù del canone interpretativo desumibile dal sistema delle fonti. Da ciò ne consegue che, ogni interpretazione e applicazione della normativa nazionale, che sia in contrasto con il *GDPR* è affetta da vizio di illegittimità, tale da giustificare la richiesta di un accertamento giudiziale, in particolare da parte della Corte di Giustizia, ma che, preliminarmente, comporta l'inapplicabilità della norma italiana da parte dei giudici nazionali.

Residua una certezza di non poco conto per gli operatori: la centralità del *GDPR* e del nuovo approccio a cui quest'ultimo si ispira. Questo infatti, oltre a costituire parametro di legittimità per l'applicazione e l'interpretazione di qualunque norma afferente con il mondo della protezione dei dati personali, si approccia in maniera del tutto innovativa alla materia della *privacy*.

Si passa infatti, da un sistema individualistico della protezione dei dati, incentrato sulla regola del consenso e fatto proprio dalla versione precedente del Codice, ad un modello maggiormente sensibile a salvaguardare la funzione sociale e, con essa, la dimensione collettiva del diritto alla protezione dei dati personali.

In soccorso all'interprete che si trova dinanzi al vasto tessuto normativo che ospita la disciplina della *privacy*, soccorre l'Autorità Garante della

protezione dei dati, figura, la cui centralità si evince già nelle «Disposizioni generali», Titolo I, Parte I del Decreto.

2. Apparato sanzionatorio amministrativo

Nell'ambito della disciplina sulla protezione dei dati personali, la parte relativa alle sanzioni è quella che ha subito nel tempo i cambiamenti più rilevanti. L'apparato sanzionatorio in ambito *privacy* trae le sue origini già dalla Direttiva 95/46/CE, che non specificava il tipo e l'entità delle sanzioni previste, ma aveva affidato a ciascuno stato membro il compito di adottare le misure appropriate per garantire la piena applicazione delle disposizioni e stabilire le conseguenze delle violazioni, senza precisare se le violazioni dovessero essere penali o amministrative.

L'unico vincolo che veniva posto agli Stati era quello relativo al rispetto dei principi di effettività, proporzionalità, capacità dissuasiva e omogeneità delle sanzioni rispetto all'apparato sanzionatorio interno e quello degli altri stati membri.

Con il recepimento della Direttiva da parte della legge 675/96 fu previsto un regime sanzionatorio di tipo misto, formato dalla presenza di sanzioni di tipo civile, amministrativo e penale. La presenza di numerose e importanti fattispecie penali trovava ragione nella sfiducia verso l'effetto deterrente delle sanzioni amministrative e nella necessità di rispettare una simmetria con le disposizioni del codice penale che, qualificano i diritti della personalità come beni di carattere primario e tutelano anche esse la *privacy* da aggressioni realizzate con modalità diverse da quelle previste dal Codice e connesse al trattamento dei dati[3].

Successivamente, con l'approvazione del Codice *privacy*, (decreto legislativo 196/2003), sono state apportate delle modifiche alla disciplina già

[3] BUTTARELLI G., *Banche dati e tutela della riservatezza*, Milano, 1997.

introdotta dal decreto legislativo 467/2001[4], ma queste non hanno inciso in maniera profonda sul sistema complessivo ed hanno costituito, per lo più, dei necessari aggiustamenti.

Al contrario di quanto previsto dalla Direttiva 95/46/CE, il *GDPR*, disciplina il sistema delle sanzioni nel Capo VIII «Mezzi di ricorso, responsabilità e sanzioni» e ne individua gli importi e le situazioni in cui possono essere comminate. Nel Regolamento 2016/679/UE non sono previste, come invece accadeva nel Decreto legislativo 196/2003 fattispecie specifiche con condotte tipiche, la violazione delle quali prevede una sanzione amministrativa con una pena edittale minima ed una massima. Figure che, originariamente previste, sono state tutte abrogate dal decreto legislativo 101/2018 di adeguamento del codice *privacy* alla normativa del *GDPR*.

La *ratio* di tale abrogazione si rinviene nell'articolo 83 dello stesso Regolamento, caratterizzato da ampiezza e genericità e facente riferimento a sanzioni amministrative che vengono inflitte per le violazioni del Regolamento espressamente considerate.

L'assenza di fattispecie tipiche, rispetto al quadro sanzionatorio esistente *ex ante*, non costituisce una lacuna, ma, *a fortiori*, l'articolo 83 è portatore di una onnicomprensività tale da legittimare, ogni qualvolta vi sia una violazione del regolamento, l'intervento dell'Autorità di controllo a comminare una sanzione amministrativa pecuniaria, da valutare caso per caso.

Le norme in materia di sanzioni amministrative pecuniarie sono condensate nell'articolo 166[5] del Codice *privacy*, completamente novellato dall'intervento legislativo dell'agosto 2018.

---

[4] D.lgs. 467/2001: «Disposizioni correttive ed integrative della normativa in materia di protezione dei dati personali, a norma dell´art. 1 della legge n. 127 del 24 marzo 2001». Tale decreto ha apportato importanti modifiche all'apparato sanzionatorio precedente, tra le quali ad esempio, la trasformazione della violazione dell'obbligo di notificazione da illecito penale a illecito amministrativo.

[5] Articolo 166 Codice *privacy*, così rubricato: «Criteri di applicazione delle sanzioni amministrative pecuniarie e procedimento per l'adozione dei provvedimenti correttivi e sanzionatori», stabilisce quanto di seguito: «Sono 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, 2-quinquiesdecies, 92, comma 1, 93, comma 1, 123, comma 4, 128, 129, comma 2, e 132-ter. 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 fatto che le violazioni richiamate dall'articolo 166 siano quelle di natura amministrativa, oltre ad essere esplicitato dalla stessa rubrica dell'articolo – «Criteri di applicazione delle sanzioni amministrative pecuniarie e procedimento per l'adozione dei provvedimenti correttivi e sanzionatori»–, nonché dai vari riferimenti alle sanzioni amministrative contenuti in diversi commi di tale articolo, è peraltro confermato dai richiami all'applicabilità del capo I della legge n. 689/81 presenti al settimo comma dell'articolo, ovvero

---

Sono soggette alla sanzione amministrativa di cui all'articolo 83, paragrafo 5, del Regolamento le violazioni delle disposizioni di cui agli articoli 2-ter, 2-quinquies, comma 1, 2-sexies, 2-septies, comma 8, 2-octies, 2-terdecies, commi 1, 2, 3 e 4, 52, commi 4 e 5, 75, 78, 79, 80, 82, 92, comma 2, 93, commi 2 e 3, 96, 99, 100, commi 1, 2 e 4, 101, 105 commi 1, 2 e 4, 110-bis, commi 2 e 3, 111, 111-bis, 116, comma 1, 120, comma 2, 122, 123, commi 1, 2, 3 e 5, 124, 125, 126, 130, commi da 1 a 5, 131, 132, 132-bis, comma 2, 132-quater, 157, nonché' delle misure di garanzia, delle regole deontologiche di cui rispettivamente agli articoli 2-septies e 2-quater.

Il Garante è l'organo competente ad adottare i provvedimenti correttivi di cui all'articolo 58, paragrafo 2, del Regolamento, nonché ad irrogare le sanzioni di cui all'articolo 83 del medesimo Regolamento e di cui ai commi 1 e 2.

Il procedimento per l'adozione dei provvedimenti e delle sanzioni indicati al comma 3 può essere avviato, nei confronti sia di soggetti privati, sia di autorità pubbliche ed organismi pubblici, a seguito di reclamo ai sensi dell'articolo 77 del Regolamento o di attività istruttoria d'iniziativa del Garante, nell'ambito dell'esercizio dei poteri d'indagine di cui all'articolo 58, paragrafo 1, del Regolamento, nonché in relazione ad accessi, ispezioni e verifiche svolte in base a poteri di accertamento autonomi, ovvero delegati dal Garante.

L'Ufficio del Garante, quando ritiene che gli elementi acquisiti nel corso delle attività di cui al comma 4 configurino una o più violazioni indicate nel presente titolo e nell'articolo 83, paragrafi 4, 5 e 6, del Regolamento, avvia il procedimento per l'adozione dei provvedimenti e delle sanzioni di cui al comma 3 notificando al titolare o al responsabile del trattamento le presunte violazioni, nel rispetto delle garanzie previste dal Regolamento di cui al comma 9, salvo che la previa notifica della contestazione non risulti incompatibile con la natura e le finalità del provvedimento da adottare.

Entro trenta giorni dal ricevimento della comunicazione di cui al comma 5, il contravventore può inviare al Garante scritti difensivi o documenti e può chiedere di essere sentito dalla medesima autorità.

Nell'adozione dei provvedimenti sanzionatori nei casi di cui al comma 3 si osservano, in quanto applicabili, gli articoli da 1 a 9, da 18 a 22 e da 24 a 28 della legge 24 novembre 1981, n. 689; nei medesimi casi può essere applicata la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, sul sito internet del Garante. I proventi delle sanzioni, nella misura del cinquanta per cento del totale annuo, sono riassegnati al fondo di cui all'articolo 156, comma 8, per essere destinati alle specifiche attività di sensibilizzazione e di ispezione nonché' di attuazione del Regolamento svolte dal Garante.

Entro il termine di cui all'articolo 10, comma 3, del decreto legislativo n. 150 del 2011 previsto per la proposizione del ricorso, il trasgressore e gli obbligati in solido possono definire la controversia adeguandosi alle prescrizioni del Garante, ove impartite, e mediante il pagamento di un importo pari alla metà della sanzione irrogata.

Nel rispetto dell'articolo 58, paragrafo 4, del Regolamento, con proprio regolamento pubblicato nella Gazzetta Ufficiale della Repubblica italiana, il Garante definisce le modalità del procedimento per l'adozione dei provvedimenti e delle sanzioni di cui al comma 3 ed i relativi termini, in conformità ai principi della piena conoscenza degli atti istruttori, del contraddittorio, della verbalizzazione, nonché' della distinzione tra funzioni istruttorie e funzioni decisorie rispetto all'irrogazione della sanzione.

Le disposizioni relative a sanzioni amministrative previste dal presente codice e dall'articolo 83 del Regolamento non si applicano in relazione ai trattamenti svolti in ambito giudiziario.

alle disposizioni che descrivono, *inter alia*, la natura e le caratteristiche delle sanzioni stesse.

Tale articolo definisce in modo dettagliato i criteri di applicazione delle sanzioni amministrative pecuniarie di cui all'articolo 83 *GDPR*, nonché i provvedimenti correttivi di cui all'articolo 58 comma due *GDPR*. Il Garante è l'organo deputato ad irrogare tali sanzioni e adottare tali provvedimenti.

Al fine di meglio comprendere la struttura dell'articolo 166, è indispensabile esaminare il sostrato su cui questo si fonda, ossia il già menzionato articolo 83 *GDPR* e i *Consideranda n.* 148, 150 e 151.

Innanzitutto, la prima considerazione da fare è che, le sanzioni, tanto amministrative quanto penali, devono essere ispirate a un principio di armonizzazione tra gli stati membri, così come raccomandato dal *considerandum* n.11[6]. L'articolo 83 difatti prevede, a livello amministrativo quelle che il *considerandum* n.11 definisce «sanzioni equivalenti per le violazioni», ciò viene posto in evidenza al fine di evitare che nel comminare sanzioni a livello nazionale, vengano a crearsi squilibri tra Stati membri.

Il *considerandum* n. 148 recita: «Per rafforzare il rispetto delle norme del presente regolamento, dovrebbero essere imposte sanzioni, comprese sanzioni amministrative pecuniarie per violazione del regolamento, in aggiunta o in sostituzione di misure appropriate imposte dall'autorità di controllo ai sensi del presente regolamento. In caso di violazione minore o se la sanzione pecuniaria che dovrebbe essere imposta costituisse un onere sproporzionato per una persona fisica, potrebbe essere rivolto un ammonimento anziché imposta una sanzione pecuniaria. Si dovrebbe prestare tuttavia debita attenzione alla natura, alla gravità e alla durata della violazione, al carattere doloso della violazione e alle misure adottate per attenuare il danno subito, al grado di responsabilità o eventuali precedenti violazioni pertinenti, alla maniera in cui l'autorità di controllo ha preso conoscenza della violazione, al rispetto dei provvedimenti disposti nei

[6] *Considerandum* n.11 *GDPR*: «Un'efficace protezione dei dati personali in tutta l'Unione presuppone il rafforzamento e la disciplina dettagliata dei diritti degli interessati e degli obblighi di coloro che effettuano e determinano il trattamento dei dati personali, nonché poteri equivalenti per controllare e assicurare il rispetto delle norme di protezione dei dati personali e sanzioni equivalenti per le violazioni negli Stati membri».

confronti del titolare del trattamento o del responsabile del trattamento, all'adesione a un codice di condotta e eventuali altri fattori aggravanti o attenuanti. L'imposizione di sanzioni, comprese sanzioni amministrative pecuniarie dovrebbe essere soggetta a garanzie procedurali appropriate in conformità dei principi generali del diritto dell'Unione e della Carta, inclusi l'effettiva tutela giurisdizionale e il giusto processo».

Le note su cui occorre porre l'attenzione in relazione a tale disposizione sono varie. *In primis* osserviamo come venga detto «[…] comprese sanzioni amministrative pecuniarie […]», ciò sta a indicare che per le violazioni delle norme del *GDPR* sono previste altre sanzioni amministrative non pecuniarie o anche sanzioni penali –da qui i problemi in punto di *ne bis in idem*[7]–, che peraltro si aggiungono ad altre misure correttive *ex* articolo 58 comma 2[8] *GDPR.* Proprio in relazione a quest'ultimo ed ai poteri correttivi ivi previsti, il *considerandum* n. 148 usa l'espressione «in aggiunta o in sostituzione».

In estrema sintesi, esistono vari poteri correttivi, ai quali può accompagnarsi una sanzione che, in virtù della sua possibile adozione, deve tener conto di diversi fattori. Da una lettura del *considerandum* n. 13 si comprende come: «Per assicurare un livello coerente di protezione delle persone fisiche in tutta

[7] Cfr. Capitolo III Paragrafo 4

[8] Articolo 58 comma due *GDPR* rubricato «Poteri»: «Ogni autorità di controllo ha tutti i poteri correttivi seguenti:
a) rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente regolamento;
b) rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del presente regolamento;
c) ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal presente regolamento;
d) ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine;
e) ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali;
f) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;
g) ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19;
h) revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti;
i) infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle misure di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso; j) ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale».

l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, è necessario un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese, offra alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili e di obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento e assicuri un monitoraggio coerente del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri». Ciò in ragione che le diverse aziende avranno fatturati più o meno alti, sulla base dei quali andranno calibrate le sanzioni pecuniarie che per questo prevedono, *ex* articolo 83, solo importi massimi[9].

Ma in tal senso, anche il *considerandum* n. 148, si basa sulla stessa logica e ciò lo si evince da varie previsioni. Innanzitutto prevede che «in caso di violazione minore o se la sanzione pecuniaria che dovrebbe essere imposta costituisse un onere sproporzionato per una persona fisica, potrebbe essere rivolto un ammonimento anziché imposta una sanzione pecuniaria»; ciò appare ragionevole, non solo in quanto la persona fisica potrebbe non avere la stessa disponibilità economica di un'azienda o un ente, ma soprattutto perché spesso, in particolare per le violazioni minori, lo strumento dell'ammonimento, attraverso la conoscenza dell'infrazione e l'avviso circa le possibili conseguenze ulteriori, potrebbe essere di per se sufficiente a scongiurare il protrarsi della violazione o il verificarsi di ulteriori illeciti.

Analogamente, ispirata alla stessa *ratio* di fondo, è la previsione secondo la quale l'adozione di sanzioni e la fissazione del loro importo dovrà essere subordinata a una ponderazione basata su diversi criteri *ex* articolo 83 comma 2.

Procedendo con l'analisi di suddetto articolo 83 rubricato: «Condizioni generali per infliggere sanzioni amministrative pecuniarie», stabilisce al primo comma che: «Ogni autorità di controllo provvede affinché le sanzioni

[9] BOLOGNINI L., BISTOLFI C., PELINO E., *Il regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016

amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive». Notiamo come, tale articolo, stabilisce le condizioni generali per infliggere sanzioni amministrative pecuniarie e stabilisce sostanzialmente che ogni autorità di controllo deve provvedere affinché le sanzioni amministrative pecuniarie inflitte in relazione alle violazioni siano, in ogni singolo caso, effettive, proporzionate e dissuasive.

Le sanzioni amministrative pecuniarie sono inflitte sulla base di criteri che tengono conto della fattispecie concreta, al fine di evitare un'applicazione delle sanzioni, automatizzata e meccanica, ma di renderla equa, ponderata e relativa al frangente concreto.

Gli elementi cui si deve tener conto, stabiliti dalle lettere a) – k) del comma due dello stesso articolo 83[10], sono i seguenti: la natura, la gravità e la durata della violazione, tenuto conto della natura, l'oggetto o la finalità del trattamento, nonché il numero di interessati lesi dal danno e il livello del danno da essi subito, definibile come entità del pregiudizio; l'elemento soggettivo, l'animus con il quale il soggetto attivo ha agito, cioè il carattere doloso o colposo della violazione; le modalità della condotta, ma anche le misure adottate per attenuare il danno subito dagli interessati; il grado di

[10] Articolo 83, comma due, lett. a)- k) *GDPR*: «Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure. Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi: a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito; b) il carattere doloso o colposo della violazione; c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati; d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32; e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento; h) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi; g) le categorie di dati personali interessate dalla violazione; h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione; i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti; j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione».

responsabilità del titolare o del responsabile del trattamento –il che costituisce una novità rispetto alla previgente disciplina ex Direttiva 95/46/CE–; eventuali precedenti violazioni pertinenti. Del titolare e del responsabile del trattamento verrà operato, pertanto, uno *screening* completo, prendendo in considerazioni tutta la pregressa operatività, non solo quella strettamente connessa alla violazione, anche quella utile al fine di individuare l'anello debole che ha determinato la lesione dei diritti, pur nel rispetto dei vari adempimenti eseguiti in conformità alla disciplina di cui al Regolamento; il c.d. ravvedimento operoso; le categorie di dati personali interessate dalla violazione –anche questo rappresenta un importante *novum* rispetto alla disciplina precedente – in quanto più delicata e protetta sarà la natura del dato, più stringenti saranno le sanzioni da adottare, misurabili sull'entità del pregiudizio *in re ipsa*; le modalità con le quali l'autorità di controllo ha avuto conoscenza della violazione, al fine di valutare se vi è stato un atteggiamento collaborativo o omissivo; l'adozione di precedenti provvedimenti correttivi ex articolo 58 comma due nei confronti dello stesso contravventore, relativamente allo stesso oggetto; l'adesione ai codici di condotta; eventuali altri fattori aggravanti o attenuanti applicabili alle singole circostanze del caso concreto, saranno considerati, a titolo esemplificativo, eventuali benefici finanziari conseguiti o le perdite evitate conseguenti alla violazione, ampliando, pertanto, l'esame anche alle c.d. conseguenze dirette o indirette per l'impresa. Ciò al fine di considerare l'impatto della violazione sull'operato del titolare del trattamento anche in termini di eventuali vantaggi di natura economica derivanti dalla stessa.

Appare subito evidente come il regime sanzionatorio del Regolamento è in parte diverso rispetto a quello previsto dal Codice *privacy,* nel quale era stato previsto un minimo edittale sotto la soglia del quale non si poteva andare. L'assenza nella disciplina attuale di un minimo edittale è perfettamente rispondente al principio della dosimetria della sanzione. Dando uno sguardo al passato, si pensi come, anche casi lievi, o di poca rilevanza, sarebbero stati puniti obbligatoriamente con pena minima di euro 6000, sia se commesse da un piccolo artigiano, che da un professionista, o ancora da una società

unipersonale, o da una grande multinazionale, sia se si trattava di un recidivo, sia se era la prima violazione commessa.

Questi rischi con il Regolamento, sono stati del tutto scongiurati, in quanto oggi spetterà al Garante esercitare una grande discrezionalità ed un forte equilibrio nello scegliere la giusta misura sulla base degli elementi anzidetti, motivando la sua scelta e trovando una sorta dii scala di sanzioni per vari casi di gravità, avendo come unico limite nell'irrogazione delle sanzioni, l'effettività, la proporzionalità e la dissuasività rispetto al singolo caso.

Se, con i primi due caratteri, si è cercato di creare uno stretto legame tra conseguenze della violazione e sanzione da applicare, nel senso che tanto l'effettività quanto la proporzionalità rappresentano un ancoraggio tra evento e possibile misura della punizione, la dissuasività ha rappresentato, molto probabilmente, il criterio che ha indotto il legislatore ad inasprire l'intero assetto sanzionatorio nella misura in cui l'applicazione della sanzione debba essere percepita dall'azienda in maniera tanto pesante da indurla a non operare più attraverso determinate mancanze.

Assistiamo ad una sorta di personalizzazione delle sanzioni, il quale però è suscettibile di aprire questioni di non scarso rilievo sotto il profilo della uguaglianza formale di fronte alla legge, degli effetti perversi della combinazione tra sanzioni amministrative e sanzioni penali, della protezione dall'arbitrio della mano pubblica e quindi della tutela di alcuni diritti fondamentali, la cui considerazione non può automaticamente cedere di fronte a quella del diritto di ciascuna persona fisica alla protezione dei dati personali che la riguardano.

Per quel che concerne la misura massima della sanzione amministrativa pecuniaria che può essere inflitta, sempre l'articolo 83 al comma tre[11],

[11] Articolo 83 comma 3 *GDPR*: «Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave».

quattro[12] e cinque[13] opera una distinzione tra: la violazione degli obblighi del titolare o responsabile del trattamento, quelli dell'organismo di certificazione nonché quelli dell'organismo di controllo, per le quali è stabilita una misura massima di 10.000.000 Euro o, per le imprese, fino al 2% del fatturato mondiale annuo dell'esercizio precedente, se superiore; e le violazioni dei principi di base del trattamento, comprese le condizioni relative al consenso, dei diritti degli interessati, dei trasferimenti di dati personali e di qualsiasi obbligo o inosservanza di un ordine, per le quali è fissato un tetto massimo di 20.000.000 Euro o, per le imprese, il 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. Medesimo limite massimo sanzionatorio è anche previsto nei casi di inosservanza di un ordine, di una limitazione di trattamento, o di un ordine di sospensione dei flussi emananti dall'autorità di controllo[14].

Alla luce di quanto esposto, comprendiamo come gli importi delle sanzioni *ex* articolo 83 seguono dei valori fissi per i quali è individuata la massima somma comminabile, oppure vengono calcolati in percentuale sul fatturato delle imprese.

Si tratta di un cambio radicale di impostazione che certamente punta alla massima deterrenza e ad una concreta afflittività delle sanzioni, che

[12] Articolo 83 comma 4 *GDPR*: «In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:
a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43; 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».

[13] Articolo 83 comma 5, *GDPR*: «In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore: a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9; b) i diritti degli interessati a norma degli articoli da 12 a 22; c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49; d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX; 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 ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1».

[14] Articolo 83 comma 6, *GDPR*: «In conformità del paragrafo 2 del presente articolo, l'inosservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore».

dovranno avere un'incidenza reale sul patrimonio di chi commetta le violazioni.

Si segnala che, ad eccezione di pochissime fattispecie e delle norme relative a determinate misure di sicurezza minime, tutte le altre violazione, sino ad oggi, in Italia, non erano previste o non esponevano a sanzione pecuniaria, ma solo a provvedimenti inibitori-coercitivi.

Ai sensi del *considerandum* n. 150[15] lo scopo del *GDPR* è quello di «rafforzare e armonizzare le sanzioni amministrative applicabili».

In relazione alle sanzioni da infliggere ad autorità pubbliche e organismi pubblici, l'articolo 83 prevede la possibilità che ogni Stato membro possa prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie[16].

L'esercizio da parte dell'autorità di controllo dei poteri di comminare le sanzioni amministrative è soggetto a garanzie procedurali in conformità con le norme dell'ordinamento italiano e deve essere previsto, disciplinato ed effettivo, sia il ricorso giurisdizionale effettivo, sia il giusto processo[17].

---

[15] *Considerandum* n. 150: «Al fine di rafforzare e armonizzare le sanzioni amministrative applicabili per violazione del presente regolamento, ogni autorità di controllo dovrebbe poter imporre sanzioni amministrative pecuniarie. Il presente regolamento dovrebbe specificare le violazioni, indicare il limite massimo e i criteri per prevedere la relativa sanzione amministrativa pecuniaria, che dovrebbe essere stabilita dall'autorità di controllo competente in ogni singolo caso, tenuto conto di tutte le circostanze pertinenti della situazione specifica, in particolare della natura, gravità e durata dell'infrazione e delle relative conseguenze, nonché delle misure adottate per assicurare la conformità agli obblighi derivanti dal presente regolamento e prevenire o attenuare le conseguenze della violazione. Se le sanzioni amministrative sono inflitte a imprese, le imprese dovrebbero essere intese quali definite agli articoli 101 e 102 TFUE a tali fini. Se le sanzioni amministrative sono inflitte a persone che non sono imprese, l'autorità di controllo dovrebbe tenere conto del livello generale di reddito nello Stato membro come pure della situazione economica della persona nel valutare l'importo appropriato della sanzione pecuniaria. Il meccanismo di coerenza può essere utilizzato anche per favorire un'applicazione coerente delle sanzioni amministrative pecuniarie. Dovrebbe spettare agli Stati membri determinare se e in che misura le autorità pubbliche debbano essere soggette a sanzioni amministrative pecuniarie. Imporre una sanzione amministrativa pecuniaria o dare un avvertimento non incide sull'applicazione di altri poteri delle autorità di controllo o di altre sanzioni a norma del regolamento».

[16] Articolo 83 comma 7, *GDPR*: «Fatti salvi i poteri correttivi delle autorità di controllo a norma dell'articolo 58, paragrafo 2, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro».

[17] Per giusto processo si intende l'insieme delle forme necessarie per garantire a ciascun titolare di diritti soggettivi o interessi legittimi lesi, la facoltà di agire e difendersi in giudizio. I principi costituzionali del giusto processo si rinvengono all'articolo 111 della Costituzione.

L'esercizio del potere sanzionatorio è soggetto *ex* articolo 83 comma 8[18], a garanzie procedurali come il ricorso giurisdizionale effettivo.

Una breve osservazione deve essere fatta in relazione al *considerandum* n. 151[19], il quale sottolinea che gli Stati membri di Estonia e Danimarca hanno sistemi giurisdizionali che non consentono l'irrogazione di sanzioni amministrative pecuniarie come previsto dal *GDPR*. Del resto, è lo stesso articolo 83 al comma 9[20] a prevedere che «se l'ordinamento giuridico dello Stato membro non prevede sanzioni amministrative pecuniarie, l'azione sanzionatoria deve essere avviata dall'autorità di controllo competente e la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali». In entrambi i casi, la *ratio* è quella di far sì che l'applicazione delle sanzioni, a prescindere dal *nomen iuris* datogli, riesca a dare forza vincolante alle norme del *GDPR*.

In tema di procedimento amministrativo sanzionatorio il legislatore italiano ha emanato il decreto legislativo 101/2018 con il quale ha introdotte alcune norme di adeguamento e coordinamento tra il Codice *privacy* e il testo regolamentare, quali ad esempio l'articolo 166, il quale risulta strutturato in due parti. Mentre i commi 1 e 2 specificano quale tra le due tipologie di sanzioni previste dall'articolo 83 *GDPR* risulti applicabile alle singole

[18] Articolo 83 comma 8, *GDPR*: «L'esercizio da parte dell'autorità di controllo dei poteri attribuitile dal presente articolo è soggetto a garanzie procedurali adeguate in conformità del diritto dell'Unione e degli Stati membri, inclusi il ricorso giurisdizionale effettivo e il giusto processo».

[19] *Considerandum* n. 151: «I sistemi giudiziari di Danimarca ed Estonia non consentono l'irrogazione di sanzioni amministrative pecuniarie come previsto dal presente regolamento. Le norme relative alle sanzioni amministrative pecuniarie possono essere applicate in maniera tale che in Danimarca la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali quale sanzione penale e in Estonia la sanzione pecuniaria sia imposta dall'autorità di controllo nel quadro di una procedura d'infrazione, purché l'applicazione di tali norme in detti Stati membri abbia effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità di controllo. Le competenti autorità giurisdizionali nazionali dovrebbero pertanto tener conto della raccomandazione dell'autorità di controllo che avvia l'azione sanzionatoria. In ogni caso, le sanzioni pecuniarie irrogate dovrebbero essere effettive, proporzionate e dissuasive».

[20] Articolo 83 comma 9, *GDPR*: «Se l'ordinamento giuridico dello Stato membro non prevede sanzioni amministrative pecuniarie, il presente articolo può essere applicato in maniera tale che l'azione sanzionatoria sia avviata dall'autorità di controllo competente e la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali, garantendo nel contempo che i mezzi di ricorso siano effettivi e abbiano effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità di controllo. In ogni caso, le sanzioni pecuniarie irrogate sono effettive, proporzionate e dissuasive. Tali Stati membri notificano alla Commissione le disposizioni di legge adottate a norma del presente paragrafo al più tardi entro 25 maggio 2018 e comunicano senza ritardo ogni successiva modifica».

violazioni delle norme del Codice stesso, i commi da 3 a 10 descrivono la procedura per l'adozione dei provvedimenti correttivi e sanzionatori, individuando nel Garante l'autorità competente a tal fine.

In aggiunta alle ipotesi sanzionate dal Regolamento, il decreto legislativo introduce ulteriori condotte che danno luogo all'applicazione di sanzioni amministrative pecuniarie all'articolo 166. A titolo esemplificativo, menzioniamo: la violazione dell'obbligo di redigere un'informativa con linguaggio semplificato per i minori, ma anche la mancata adozione delle misure indicate dal Garante per i trattamenti che presentano rischi elevati per l'esecuzione di un compito di interesse pubblico.

Il procedimento di applicazione delle sanzioni e dei provvedimenti di conformazione è mutuato dalla legge 689/1981[21] ed opera nel modo seguente. L'autorità può pervenire all'adozione di un provvedimento sanzionatorio di tipo amministrativo, in tre specifiche situazioni che sono: reclamo, attività istruttoria *ex officio*, nell'ambito dell'esercizio dei poteri di indagine, o in seguito ad accessi, ispezioni e verifiche, svolti invece in virtù dei poteri di accertamento, autonomi o delegati. Dopo aver fatto le dovute valutazioni, il Garante procederà alla contestazione mediante verbale, ricevuto il quale, il responsabile o il titolare, ha trenta giorni per presentare scritti difensivi o per chiedere di essere sentito, esercitando il proprio diritto al contraddittorio.

Dopo di che, il pagamento della sanzione potrà avvenire in misura ridotta (del 50%), al fine di definire la controversia, a condizione che vi sia stato un adeguamento da parte del trasgressore, oppure si procederà all'irrogazione della sanzione principale e all'applicazione della misura accessoria della pubblicazione dell'ordinanza-ingiunzione, nell'ottica di esercitare una funzione deterrente alla commissione di ulteriori illeciti.

Una novità alquanto rilevante risulta essere quella relativa alla destinazione dei proventi delle sanzioni che andranno a finanziare la stessa autorità Garante «per essere destinati alle specifiche attività di sensibilizzazione e di ispezione nonché di attuazione del Regolamento».

[21] Si tratta della legge generale sul procedimento sanzionatorio pecuniario.

3. Apparato sanzionatorio penale

Come già osservato, tra le principali novità che il Regolamento ha introdotto, dal 25 maggio 2018 (data a partire dalla quale lo stesso è divenuto applicabile in tutti gli Stati europei), emergono in particolare i rinnovati profili sanzionatori previsti per le violazioni della normativa a tutela dei dati personali.

Le scelte amministrative appena illustrate, hanno, naturalmente, implicazioni importanti anche in ordine alla tutela penale. A fronte di un sistema amministrativo particolarmente ampio, rigoroso e caratterizzato da una forte dissuasività –tale da configurare sanzioni para-penali, secondo i criteri della sentenza Cedu 1976 *Engel* e a. c. Paesi Bassi –, è infatti ragionevole ridurre la sfera del penalmente rilevante alle sole condotte effettivamente distinte da quelle idonee a integrare illeciti amministrativi, dotate di una propria caratterizzazione e di un proprio disvalore, per non incorrere nel divieto di *bis in idem.*

La caratteristica essenziale delle fattispecie di reato previste dal decreto legislativo 196/2003 era riferibile alla loro natura *stricto sensu* sanzionatoria di norme sul trattamento dei dati personali sancite da altre disposizioni dello stesso decreto, secondo la tecnica legislativa dei continui rinvii a precetti extra-penali di settore, che portò parte della dottrina[22] a parlare di "vertigine combinatoria".

Anche con il decreto di adeguamento al *GDPR*, in Italia, le sanzioni penali continueranno ad avere un ruolo fondamentale per la salvaguardia del diritto alla protezione dei dati personali.

Prima di passare all'analisi esegetica di ogni singola fattispecie incriminatrice, prevista attualmente dal Codice *privacy*, è indispensabile menzionare l'articolo 84 *GDPR* rubricato appunto «Sanzioni» il quale recita: «Gli Stati membri stabiliscono le norme relative alle altre sanzioni per le

[22] Corrias Lucente G. *Profili penali della recente legge sul trattamento dei dati personali*, in *Studium Juris*, 1998,

violazioni del presente regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione. Tali sanzioni devono essere effettive, proporzionate e dissuasive.

Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 1 al più tardi entro il 25 maggio 2018, e comunica senza ritardo ogni successiva modifica».

L'articolo 84 del Regolamento, nello stabilire che gli Stati membri devono prevedere le norme relative alle altre sanzioni per le violazioni del presente Regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie *ex* articolo 83, il legislatore europeo ha consentito a ogni Stato di preveder, ove ritiene, norme in materia penale e condotte punite con la pena della reclusione da affiancare alle sanzioni amministrative e, se decide e procede in tal senso, deve adottare tutti i provvedimenti necessarie per assicurarne l'applicazione.

Già nella fase di adozione da parte del Governo del primo schema di decreto, sono state introdotte fattispecie penali che, nella prima fase preparatoria, erano state consapevolmente e motivamente escluse, anche per ragioni di possibile contrasto con il quadro regolatorio europeo che, come spesso precisato dalla Corte di Giustizia, non consente il *ne bis in idem* tra sanzioni amministrative, tutte rigidamente vincolate dalle previsioni del *GDPR* e sanzioni penali, che dovrebbero riguardare, in linea generale, solo profili non sanzionabili in via amministrativa.

Di fatti, le motivazioni a favore delle ipotesi di depenalizzazione *privacy* potevano essere ricondotte all'obiettivo di evitare il rischio di applicazioni estensive del principio di *ne bis in idem* tra sanzioni amministrative e penali alla luce del *Considerandum* n. 149 del *GDPR* («[…] 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») e, appunto, di una giurisprudenza oscillante in materia da parte della Corte di Giustizia dell'Unione Europea e della Corte Europea dei diritti dell'Uomo.

La scelta governativa di mantenere e ampliare alcune fattispecie di reato con le relative pene è stata peraltro sostenuta anche dalle Commissioni parlamentari, ed anche il Garante, ha mostrato il suo consenso.

Il legislatore italiano ha deciso di avvalersi della facoltà, concessa dal *GDPR ex* articolo 84 a tutti gli Stati membri, di prevedere sanzioni penali per alcune violazioni della normativa sulla *privacy*.

Sarebbe stato infatti ingenuo pensare che, nell'era del "tutto digitale" e dell'inevitabile esaltazione del ruolo dei dati personali nel contesto economico, sociale, e politico, globale, gli illeciti penali abbiano perso rilevanza, anziché guadagnarne. Si depenalizza quando una materia perde importanza, non quando ne assume all'ennesima potenza[23].

Il decreto 101/2018 di adeguamento al *GDPR* ha provveduto ad abrogare le disposizioni del decreto legislativo n. 196/2003 non più compatibili con il *GDPR* introducendone nuove, ma anche integrando e modificando le disposizioni che rimangono in vita.

Ne è venuta fuori una versione del codice molto più ridotta ma anche più coerente con la normativa comunitaria.

Le sanzioni penali previste attualmente, vanno però ad aggiungersi alle sanzioni amministrative già previste dal Regolamento e ciò costituisce la base per un rischio di violazione del divieto di *bis in idem*.

Passando alla disamina delle modifiche più significative apportate dal D.lgs. 101 in ambito sanzionatorio, potremmo partire dalle numerose abrogazioni che, a ben vedere, potremmo considerare come già avvenute, in quanto già con l'emanazione del Regolamento 2016/679, secondo il principio della gerarchia delle fonti, quelle norme dovevano semplicemente essere disapplicate.

Nella sistematica delle sanzioni penali rinvenibili nel Codice in materia di protezione dei dati personali si è ritenuto opportuno proporre l'opzione volta a depenalizzare le fattispecie di cui all'articolo 169[24] in tema di misure

[23] BOLOGNINI L. PELINO E., *Codice privacy: tutte le novità del d.lgs. 101/2018*, Milano, 2019.

[24] Articolo 169 Codice *privacy*, abrogato: «Misure di sicurezza», stabiliva: «Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il

minime di sicurezza. La depenalizzazione del reato in questione trova la sua *ratio* nel fatto che, con l'entrata in vigore del *GDPR*, le misure minime di sicurezza previste dal Codice sono abolite, e le nuove misure di sicurezza previste dal *GDPR* non presentano un livello di dettaglio tale da risultare compatibile col principio di tassatività, principio cardine del diritto penale.

L'opera di depenalizzazione posta in essere con il decreto di adeguamento è completata dall'articolo 24[25] dello stesso, il quale prevede che gli illeciti, ormai depenalizzati, commessi prima dell'entrata in vigore dello stesso – purché il procedimento penale non sia stato definito con sentenza o con decreto penale divenuti irrevocabili[26]– sono puniti con le sanzioni amministrative pecuniarie introdotte in sostituzione delle previgenti sanzioni penali.

Il decreto legislativo 101/2018 prevede ben tre fattispecie di reato relative al trattamento illecito di dati personali, la loro comunicazione e diffusione illecita e l'acquisizione fraudolenta. Gli articoli cui si fa riferimento sono l'articolo 167[27], riformulato e molto diverso rispetto al precedente, l'articolo

periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo della sanzione stabilita per la violazione amministrativa. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili»

[25] Articolo 24 d.lgs. 101/2018 rubricato: «Applicabilità delle sanzioni amministrative alle violazioni anteriormente commesse», stabilisce: «Le disposizioni del presente decreto che, mediante abrogazione, sostituiscono sanzioni penali con le sanzioni amministrative previste dal Regolamento (UE) 2016/679 si applicano anche alle violazioni commesse anteriormente alla data di entrata in vigore del decreto stesso, sempre che il procedimento penale non sia stato definito con sentenza o con decreto divenuti irrevocabili. Se i procedimenti penali per i reati depenalizzati dal presente decreto sono stati definiti, prima della sua entrata in vigore, con sentenza di condanna o decreto irrevocabili, il giudice dell'esecuzione revoca la sentenza o il decreto, dichiarando che il fatto non è previsto dalla legge come reato e adotta i provvedimenti conseguenti. Il giudice dell'esecuzione provvede con l'osservanza delle disposizioni dell'articolo 667, comma 4, del codice di procedura penale. Ai fatti commessi prima della data di entrata in vigore del presente decreto non può essere applicata una sanzione amministrativa pecuniaria per un importo superiore al massimo della pena originariamente prevista o inflitta per il reato, tenuto conto del criterio di ragguaglio di cui all'articolo 135 del codice penale. A tali fatti non si applicano le sanzioni amministrative accessorie introdotte dal presente decreto, salvo che le stesse sostituiscano corrispondenti pene accessorie».

[26] In tale caso, qualora siano intervenuti sentenza o decreto irrevocabili, questi potranno essere revocati dal giudice dell'esecuzione perché il fatto non è più previsto dalla legge come reato ex articolo 673 c.p.p.

[27] Cfr. Capitolo III par. 3.1

167-bis[28] relativo all'illecita comunicazione e diffusione di dati personali oggetto di trattamento su larga scala e l'articolo 167-ter[29] relativo all'acquisizione fraudolenta di dati personali, oggetto di trattamento su larga scala.

Riguardo l'articolo 168 «Falsità nelle dichiarazioni e notificazioni al Garante», si è ritenuto opportuno conservare l'opzione punitiva; *idem ratio* si rinviene per la permanenza dell'articolo 170 «Inosservanza di provvedimenti del Garante», seppur inquadrato negli attuali ambiti normativi, al pari si è ritenuto opportuno mantenere il 171 seppur diversamente rubricato «Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori».

Il Decreto ha introdotto o riformulato i casi in cui la violazione delle regole relative al trattamento dei dati personali sconfina in illeciti penalmente rilevanti; ad oggi, dunque, cinque articoli del Codice Privacy contengono norme incriminatrici di determinate condotte illecite di trattamento dati, mentre i restanti due articoli della Parte III, Titolo III del Codice Privacy riguardano, rispettivamente le violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori (articolo 171) e le pene accessorie (articolo 172).

3.1 Trattamento illecito di dati personali ex articolo 167

L'articolo 167, rubricato «Trattamento illecito di dati personali» è la principale fattispecie delittuosa per la quale maggiormente si è posto il problema della sua abrogazione. Nelle intenzioni della Commissione ministeriale incaricata di aggiornare il Codice avrebbe dovuto essere abolita in toto.

La previsione normativa di che trattasi, nella versione del Codice *privacy* 2003, statuiva[30] che, «chiunque al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali, in

[28] Cfr. Capitolo III par. 3.2
[29] Cfr. Capitolo III par. 3.3
[30] Cfr. Capitolo II par. 2

violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126, 130, ovvero in applicazione dell'articolo 129, è punito se dal fatto deriva nocumento». Il comma 2 puniva «chiunque, 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 relativi ai dati sensibili e giudiziari, se dal fatto deriva nocumento».

Dalla lettura del precedente dettato normativo, si comprende come, tale norma, non era assolutamente incompatibile con il regolamento, poiché dotata di funzione special-preventiva e vitale per la protezione dei dati personali.

La fattispecie di cui all'articolo 167 è stata profondamente mutata rispetto alla formulazione precedente, ma è di grande importanza che il legislatore abbia deciso di riformulare il delitto in modo da continuare a punire penalmente diverse condotte consistenti nell'arrecare nocumento all'interessato, in violazione di specifiche e limitate disposizioni normative, e abbia escluso l'opzione che conduceva alla sua eliminazione.

Se, da un lato, si è ritenuto di non poter rinunciare alle sanzioni penali previste per il trattamento illecito di dati personali, dall'altro, però, non si potrà prescindere dalla necessità di renderlo conforme al principio del *ne bis in idem*, così come raccomandato dal *considerandum* 149.

Venendo all'attuale formulazione dell'articolo 167, le condotte previste sono quelle in violazione degli articoli sui dati relativi al traffico, dati relativi all'ubicazione, dati sensibili o giudiziari, e sul trasferimento internazionale di dati.

Più nello specifico, l'articolo 167 continua ad essere rubricato «Trattamento illecito di dati» e si articola in una pluralità di commi. I primi tre, delineano le seguenti fattispecie – comma 1–: «Salvo che il fatto costituisca più grave reato, chiunque 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 o del provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi»; comma due: «Salvo che il fatto costituisca più grave reato, chiunque, al fine

di trarre per sé o per altri profitto o di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9[31] e 10[32] del Regolamento, in violazione delle disposizioni di cui agli articoli 2-*sexies* e 2-*octies*, o delle misure di garanzia di cui all'articolo 2-*septies* ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-*quinquiesdecies* arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni»; comma 3: «Salvo che il fatto costituisca più grave reato, la pena di cui al comma due si applica altresì a chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato».

Procedendo con l'esegesi della norma, risulta evidente, *prima facie*, la clausola posta all'*incipit* «Salvo che il fatto costituisca più grave reato», comune a tutte e tre le fattispecie.

[31] Articolo 9 *GDPR*: «È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1; b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato; […] g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; […]. I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti. Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute».

[32] Articolo 10 *GDPR*: «Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica».

Il legislatore ripropone in apertura tale clausola di riserva, come nella vecchia formulazione dell'articolo 167, ma prima ancora nel precedente articolo 35 L. 675/96, la cui *ratio* si rinviene nel fare salve altre ipotesi delittuose di carattere più generale, che sanzionano fattispecie più gravi.

Ciò denota la natura, ancora oggi, di reato sussidiario della fattispecie *de quo*, che viene assorbita, in forza del principio di sussidiarietà, qualora il fatto possa essere ugualmente sussunto in altra previsione penale che la contenga e che appaia, rispetto a essa, più grave.

Autorevole dottrina ricorda che «la funzione delle clausole di riserva consiste, in linea generalissima, nell'impedire l'applicazione della norma che la contiene, quando, pur realizzandosi la condotta prevista e disciplinata dalla norma in questione, essa integri anche quelli della disposizione cui la clausola rinvia. Il che equivale ad affermare che le clausole presuppongano, per poter operare, che si realizzi quella particolare situazione giuridica nella quale concorrano gli estremi di entrambe le norme collegate dalla riserva»[33].

Per ulteriori approfondimenti si rimanda a quanto già rappresentato in proposito[34].

Le fattispecie racchiuse all'interno di tale norma, risultano accomunate non solo dalla clausola posta all'*incipit*, ma anche dal soggetto attivo del reato, dall'elemento soggettivo che prevede il dolo specifico e dalla condotta, consistente nell'arrecare nocumento all'interessato, seppur con modalità differenti.

Il delitto *de quo* è un reato comune, viene punito infatti, «chiunque» commetta un illecito trattamento di dati, secondo le modalità indicate nel suddetto articolo.

Soffermandoci sulla condotta di cui al comma 1, il nocumento all'interessato viene arrecato in quanto il soggetto attivo ha agito «operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129», e ha ad oggetto la violazione delle norme poste a garanzia

[33] DE FRANCESCO G. A., Lex specialis. Specialità e interferenza nel concorso di norme penali, Milano 1980, p. 141.
[34] Cfr. Capitolo II par. 2.2

dell'interessato nei servizi di comunicazione elettronica. L'articolo 123[35] si occupa dei dati relativi al traffico, l'articolo 126[36] di quelli relativi all'ubicazione, l'articolo 130[37] delle comunicazioni indesiderate e l'articolo

[35] Articolo 123 codice *privacy* «Dati relativi al traffico»: «I dati relativi al traffico riguardanti abbonati ed utenti trattati dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico sono cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione elettronica, fatte salve le disposizioni dei commi 2, 3 e 5. Il trattamento dei dati relativi al traffico strettamente necessari a fini di fatturazione per l'contraente, ovvero di pagamenti in caso di interconnessione, è consentito al fornitore, a fini di documentazione in caso di contestazione della fattura o per la pretesa del pagamento, per un periodo non superiore a sei mesi, salva l'ulteriore specifica conservazione necessaria per effetto di una contestazione anche in sede giudiziale. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico può trattare i dati di cui al comma 2 nella misura e per la durata necessarie a fini di commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, solo se l'contraente o l'utente cui i dati si riferiscono hanno manifestato preliminarmente il proprio consenso, che è revocabile in ogni momento. Nel fornire le informazioni di cui agli articoli 13 e 14 del Regolamento il fornitore del servizio informa l'contraente o l'utente sulla natura dei dati relativi al traffico che sono sottoposti a trattamento e sulla durata del medesimo trattamento ai fini di cui ai commi 2 e 3. Il trattamento dei dati personali relativi al traffico è consentito unicamente a persone che, ai sensi dell'articolo 2 quaterdecies, risultano autorizzate al trattamento e che operano sotto la diretta autorità del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni e che si occupano della fatturazione o della gestione del traffico, di analisi per canto di clienti, dell'accertamento di frodi, o della commercializzazione dei servizi di comunicazione elettronica o della prestazione dei servizi a valore aggiunto. Il trattamento è limitato a quanto è strettamente necessario per lo svolgimento di tali attività e deve assicurare l'identificazione della persona autorizzata che accede ai dati anche mediante un'operazione di interrogazione automatizzata. L'Autorità per le garanzie nelle comunicazioni può ottenere i dati relativi alla fatturazione o al traffico necessari ai fini della risoluzione di controversie attinenti, in particolare, all'interconnessione o alla fatturazione».

[36] Articolo 126 codice *privacy:* «Dati relativi all'ubicazione»: «I dati relativi all'ubicazione diversi dai dati relativi al traffico, riferiti agli utenti o agli abbonati di reti pubbliche di comunicazione o di servizi di comunicazione elettronica accessibili al pubblico, possono essere trattati solo se anonimi o se l'utente o l'contraente ha manifestato previamente il proprio consenso, revocabile in ogni momento, e nella misura e per la durata necessari per la fornitura del servizio a valore aggiunto richiesto. Il fornitore del servizio, prima di richiedere il consenso, informa gli utenti e gli abbonati sulla natura dei dati relativi all'ubicazione diversi dai dati relativi al traffico che saranno sottoposti al trattamento, sugli scopi e sulla durata di quest'ultimo, nonché sull'eventualità che i dati siano trasmessi ad un terzo per la prestazione del servizio a valore aggiunto. L'utente e l'contraente che manifestano il proprio consenso al trattamento dei dati relativi all'ubicazione, diversi dai dati relativi al traffico, conservano il diritto di richiedere, gratuitamente e mediante una funzione semplice, l'interruzione temporanea del trattamento di tali dati per ciascun collegamento alla rete o per ciascuna trasmissione di comunicazioni. Il trattamento dei dati relativi all'ubicazione diversi dai dati relativi al traffico, ai sensi dei commi 1 , 2 e 3, è consentito unicamente a persone autorizzate al trattamento, ai sensi dell'articolo 2 quaterdecies, che operano, sono la diretta autorità del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni o del terzo che fornisce il servizio a valore aggiunto. Il trattamento è limitato a quanto è strettamente necessario per la fornitura del servizio a valore aggiunto e deve assicurare l'identificazione della persona autorizzata che accede ai dati anche mediante un'operazione di interrogazione automatizzata».

[37] Articolo 130 codice *privacy*: «Comunicazioni indesiderate»: «Fermo restando quanto stabilito dagli articoli 8 e 21 del decreto legislativo 9 aprile 2003, n. 70, l'uso di sistemi automatizzati di chiamata o di comunicazione di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è consentito con il consenso del contraente o utente. Resta in ogni caso fermo quanto previsto dall'articolo 1, comma 14, della legge 11 gennaio 2018, la disposizione di cui al comma 1 si applica anche alle comunicazioni

129[38] si occupa del provvedimento del Garante relativo alle modalità di inserimento e successivo utilizzo di dati personali relativi ai contraenti negli elenchi cartacei o elettronici a disposizione del pubblico.

Sfogliando il Regolamento, risulta evidente che, nella sua stesura, offre una definizione più dettagliata del termine "dato personale"[39] di quanto faccia il Decreto legislativo 196/2003, all'articolo 4 per esplicitare le proprie definizioni.

Ma, il Codice italiano, a differenza del Regolamento, si preoccupa di definire in maniera autonoma i dati identificativi, sensibili, giudiziari, anonimi, la comunicazione elettronica, i dati relativi al traffico e all'ubicazione.

---

elettroniche, effettuate per le finalità ivi indicate, mediante posta elettronica, telefax, messaggi del tipo Mms (Multimedia Messaging Service) o Sms (Short Message Service) o di altro tipo. Fuori dei casi di cui ai commi 1 e 2, ulteriori comunicazioni per le finalità di cui ai medesimi commi effettuate con mezzi diversi da quelli ivi indicati, sono consentite ai sensi degli articoli 6 e 7 del Regolamento nonché ai sensi di quanto previsto dal comma 3-bis. In deroga a quanto previsto dall'articolo 129, il trattamento dei dati di cui al comma 1 del predetto articolo, mediante l'impiego del telefono e della posta cartacea per le finalità di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale, è consentito nei confronti di chi non abbia esercitato il diritto di opposizione, con modalità semplificate e anche in via telematica, mediante l'iscrizione della numerazione della quale è intestatario e degli altri dati personali di cui al comma 1 del predetto articolo, in un registro pubblico delle opposizioni […]. Fatto salvo quanto previsto nel comma 1 , se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, può non richiedere il consenso dell'interessato, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni. L'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per le finalità di cui al presente comma, è informato della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente […]».

[38] Articolo 129 codice privacy: «Elenchi dei contraenti»: «Il Garante individua con proprio provvedimento, in cooperazione con l'Autorità per le garanzie nelle comunicazioni ai sensi dell'articolo 154, comma 4, e in conformità alla normativa dell'Unione europea, le modalità di inserimento e di successivo utilizzo dei dati personali relativi ai contraenti negli elenchi cartacei o elettronici a disposizione del pubblico. Il provvedimento di cui al comma 1 individua idonee modalità per la manifestazione del consenso all'inclusione negli elenchi e, rispettivamente, all'utilizzo dei dati per finalità di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale nonché per le finalità di cui all'articolo 21, paragrafo 2, del Regolamento, in base al principio della massima semplificazione delle modalità di inclusione negli elenchi a fini di mera ricerca del contraente per comunicazioni interpersonali, e del consenso specifico ed espresso qualora il trattamento esuli da tali fini, nonché in tema di verifica, rettifica o cancellazione dei dati senza oneri».

[39] Per dato personali si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Si comprende allora come la condotta in questione si riferisca alla violazione delle norme in materia di trattamento di dati relativi al traffico riguardanti contraenti ed utenti trattati dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico (articolo 123), di dati relativi all'ubicazione diversi dai dati relativi al traffico, riferiti agli utenti o ai contraenti di reti pubbliche di comunicazione o di servizi di comunicazione elettronica accessibili al pubblico (articolo 126), di comunicazioni promozionali indesiderate (articolo 130) e di elenchi di contraenti a disposizione del pubblico (si fa riferimento agli ex elenchi di abbonati telefonici *ex* articolo 129).

Si è deciso di escludere dall'ambito di illiceità penale il trattamento senza consenso dei dati personali comuni in quelle ipotesi di trattamento che il legislatore ha ritenuto (a torto o a ragione) non particolarmente rischiose per i diritti e le libertà dell'individuo[40].

L'assenza di tutela per questa violazione pare, però, stupire negativamente l'interprete[41].

La previsione di condotte illecite diverse rispetto alla fattispecie del vecchio articolo 167 determina una sorta di *abrogatio*, seppur parziale, della norma e una successione di leggi nel tempo per continuità normativa solo per una parte della fattispecie, ossia per le condotte di cui sopra (articoli 123, 126, 130), già presenti nel vecchio testo dell'articolo 167.

Al comma 2, con quest'ultimo testo, si punisce con la reclusione da uno a tre anni la condotta di trattamento illecito dei dati personali particolari (sensibili) – articolo 9– o giudiziari –articolo 10– trattati in violazione delle disposizioni nazionali di cui agli articoli 2-*sexies* (in materia di trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante), 2-*octies* (in materia di principi relativi al trattamento di dati relativi a condanne penali e reati) o delle misure di garanzia di cui all'articolo 2-*septies* (in materia di dati genetici, biometrici o relativi alla salute) ovvero

[40] BOLOGNINI L., BISTOLFI C., PELINO E., *Il regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016.
[41] BOLOGNINI L. PELINO E., *Codice privacy: tutte le novità del d.lgs. 101/2018*, Milano, 2019.

operando in violazione delle misure adottate dal Garante ai sensi dell'articolo 2-*quinquiesdecies* del Codice, in materia di trattamento che presenta rischi elevati per l'esecuzione di un compito di interesse pubblico, articolo 35 *GDPR* e per i quali il Garante può, sulla base di quanto disposto dall'articolo 36 paragrafo cinque del medesimo regolamento, e con provvedimenti di carattere generale adottati *ex officio*, prescrivere misure ed accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare.

Anche in questo caso, sembra non delinearsi il delitto se vi è stata solo una violazione generica dovuta alla mancanza di una base giuridica nel trattamento di dati sensibili/particolari (*ex* articolo 9 comma due *GDPR*), se non nei casi riferibili ai trattamenti di dati sensibili per rilevante interesse pubblico e di dati genetici, biometrici o relativi alla salute, oltre a quelli relativi a condanne penali o reati.

Una scelta discutibile che rischia di lasciare impunite condotte anche molto nocive per le vittime[42].

Il terzo comma della norma in esame, comporta l'applicazione della medesima pena di cui al comma secondo, appena analizzato, nel caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti agli articoli 45, 46 o 49 *GDPR*.

Resta da analizzare gli elementi comuni a tutte e tre le fattispecie appena analizzate, ossia il fine cui la condotta tende e l'evento che deve realizzarsi perché il reato sussista.

L'elemento soggettivo richiesto affinché si configuri il reato *de quo*, è il dolo specifico, testualmente «al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato», presente in tutte e tre le ipotesi di trattamento illecito di dati personali.

Pertanto, perché il delitto sussista, non è sufficiente che il soggetto attivo abbia la rappresentazione e la volizione di arrecare nocumento all'interessato, in violazione delle disposizioni su richiamate, ma è necessario che l'agente agisca col fine specifico di trarre un profitto o

[42] BOLOGNINI L. PELINO E., *Codice privacy: tutte le novità del d.lgs. 101/2018*, Milano, 2019.

arrecare un danno all'interessato. Al dolo specifico di profitto, è stato affiancato anche il dolo di danno per l'interessato, riprendendo più correttamente lo spirito della norma del vecchio codice *privacy* che li prevedeva entrambi e, quindi, correggendo rispetto al testo iniziale della Commissione che aveva addirittura eliminato la fattispecie, ma anche rispetto al testo pubblicato il 21 marzo che invece escludeva il dolo di danno.

È opportuno osservare che, mentre da un lato, la previsione del dolo specifico restringe l'area delle condotte penalmente rilevanti, dall'altro, la mancata indicazione dell'ingiustizia del profitto e del danno cui deve muovere la condotta criminosa, nonché la possibile natura patrimoniale del profitto stesso, contribuiscono senz'altro ad ampliare la soglia dell'area del penalmente rilevante.

Detto altrimenti, sono coperte da disvalore penale anche quei trattamenti compiuti per ottenere un ritorno in termini di immagine o di mera soddisfazione intellettuale[43].

Riguardo al concetto di profitto, valgono le considerazioni suddette[44].

Una precisazione merita di essere fatta circa il concetto di danno; l'articolo 167 vecchio testo si limitava a prevedere il fine di cagionare un danno «ad altri», la fattispecie attuale non si accontenta di un danno generico a chiunque, ma richiede che il danno sia diretto «all'interessato».

Il danno, pertanto, non può identificarsi nell'evento dannoso (cioè l'illecito trattamento dei dati) ma è necessario che si concretizzi un pregiudizio della sfera di interessi del danneggiato. La lesione non patrimoniale non può essere considerata *in re ipsa*; in altre parole, il solo fatto che vi sia stato un trattamento illecito di dati non determina, *ex se*, l'affiorare di un danno.

Siamo in presenza di un dolo consistente nella rappresentazione del fine che l'agente intende raggiungere attraverso la propria condotta, cui non deve necessariamente seguire la sua realizzazione.

È invece richiesto, per la sussistenza del delitto un effettivo nocumento, all'interessato (anche qui, non di «altri»).

---

[43] CHINÈ G., La tutela penale della privacy, in *Il trattamento dei dati personali*, vol. II, a cura di. CUFFARO V. RICCIUTO V., Torino, 1999, p. 490.

[44] Cfr. capitolo II par. 2.1

Il nocumento passa dall'essere condizione obiettiva di punibilità a elemento costitutivo del reato, che deve necessariamente sussistere, unitamente agli altri elementi della condotta, nel fuoco del dolo; e, conseguentemente, il delitto è stato trasformato da reato di pericolo concreto a reato di evento di danno direttamente ed immediatamente collegabile all'interessato. Come già osservato in relazione al nocumento[45], devono essere senza dubbio escluse le semplici violazioni formali ed irregolarità procedimentali, ma anche quelle inosservanze che producano un *vulnus* minimo all'identità personale del soggetto ed alla sua *privacy* e non determinino alcun danno patrimoniale apprezzabile.

Se, nel vecchio testo dell'articolo 167, la scelta di subordinare la punibilità del reato alla derivazione di un nocumento – ovvero alla altrettanto pregiudizievole comunicazione o diffusione di dati personali, effettuata con modalità contrarie a quanto previsto dalle disposizioni extra-penali– evidenziava, indubbiamente, l'intenzione del legislatore delegato di polarizzare la reazione repressiva anche sulla tutela di 'ben afferrabili' interessi, incentrati sul diritto individuale alla protezione della vita privata ed al controllo dei dati personali[46], nell'attuale formulazione l*'intentio legis* di perseguire tale tutela, è massima.

È interessante procedere all'analisi dei successivi commi dell'articolo 167 che recitano: «Il Pubblico ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante»; «Il Garante trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al più tardi al termine dell'attività di accertamento delle violazioni delle disposizioni di cui al presente decreto»; «Quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una

[45] Cfr. capitolo II par. 2.2

[46] MANNA A., *Prime osservazioni sul testo Unico in materia di protezione dei dati personali*, www.privacy.it

sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita».

I commi 4 e 5 si occupano di descrivere le modalità di collaborazione tra il Garante e il Pubblico Ministero nei casi di notizia delle predette ipotesi di reato.

È previsto quindi che sia il pubblico ministero, quando ha notizia dei reati di cui all'articolo 167 a informare senza ritardo il Garante. Viceversa, sarà il Garante poi, a dover trasmettere al Pubblico Ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al più tardi al termine dell'attività di accertamento delle violazioni delle disposizioni del Codice.

La mancanza di un termine (perentorio) potrebbe dare luogo a prevedibili problematiche future.

In relazione alla disposizione di cui al sesto comma del suddetto articolo, la *ratio* si rinviene nel garantire maggiore conformità al principio del *ne bis in idem*[47].

Il legislatore italiano tenendo in debito conto la raccomandazione di cui al menzionato *Considerandum* n. 149, ha introdotto la previsione secondo la quale, quando per lo stesso fatto sia stata applicata, in forza della norma del Codice *privacy* o del *GDPR*, a carico dell'imputato o dell'ente, una sanzione amministrativa pecuniaria dal Garante e questa sia già stata riscossa, la pena sia diminuita.

Interessante notare come nel caso di centri di imputazione giuridica delle sanzioni amministrative e penali che siano diversi (basti pensare all'ente, come soggetto sanzionato), sia stata preferita la scelta di far valere l'avvenuta riscossione della sanzione amministrativa all'ente come elemento diminuente della sanzione penale a carico della persona fisica imputata[48].

[47] Il garante, pur comprendendone la ratio, rileva la parziale difformità rispetto alla norma di cui all'art. 187-terdecies del d.lgs. n. 58 del 1998, che limita l'esazione della pena pecuniaria "alla parte eccedente quella riscossa dall'Autorità amministrativa"; circostanza che non ricorre nella disposizione in esame.
[48] BOLOGNINI L. PELINO E., *Codice privacy: tutte le novità del d.lgs. 101/2018*, Milano, 2019.

3.2 Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala, articolo 167-bis

L'articolo 167 bis[49] d.lgs. 196/2003 (così come modificato dal d.lgs. 101/2018) rubricato «Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala» punisce con la reclusione da uno a sei anni e salvo che il fatto costituisca più grave reato, «chiunque comunica o diffonde al fine di trarre profitto per sé o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contente dati personali oggetto di trattamento su larga scala». Tale quadro sanzionatorio si applica sia se la condivisione avvenga in violazione degli articoli 2-*ter*[50], 2-*sexies*[51] e 2-*octies*[52], sia nel caso in cui la stessa avvenga senza il necessario consenso dell'interessato, ove richiesto.

Si tratta di una fattispecie di reato del tutto nuova, che però, d'altra parte, costituisce altresì una riformulazione del reato di «comunicazione e diffusione illecita di dati personali, riferibili a un rilevante numero di persone»[53], contenuto nello schema di decreto. Tale riformulazione riduce

[49] Art 167-bis Codice *privacy*, così rubricato «Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala», stabilisce quanto segue: «Salvo che il fatto costituisca più grave reato, chiunque comunica o diffonde al fine di trarre profitto per sé o altri ovvero al fine di arrecare danno, 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, è punito con la reclusione da uno a sei anni.

Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sè o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, è punito con la reclusione da uno a sei anni, quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione.

Per i reati di cui ai commi 1 e 2, si applicano i commi 4, 5 e 6 dell'articolo 167».

[50] Art. 2-ter Codice *privacy*: 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.

[51] Art. 2-sexies Codice *privacy*: Trattamenti relativi a particolari categorie di dati trattati per motivi di interesse pubblico rilevante.

[52] Art. 2-octies Codice *privacy*: Principi relativi al trattamento di dati relativi a condanne penali e reati.

[53] L'articolo 167-bis nello schema del decreto era così rubricato: «Comunicazione e diffusione illecita di dati personali riferibili a un ingente rilevante numero di persone» e prevedeva che «il titolare o il responsabile del trattamento che comunica o diffonde, al fine di trarre profitto per sé o altri, dati personali riferibili ad un rilevante numero di persone, in violazione degli articoli 2-ter, 2-sexies e 2-octies, è punito con la reclusione da uno a sei anni. Inoltre, si prevede la reclusione da uno a sei anni, quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione».

notevolmente la portata applicativa di questa nuova fattispecie incriminatrice e potrebbe comportare alcuni problemi interpretativi.

Procedendo con l'esegesi della norma, questa sembrerebbe essere volta a stigmatizzare quella prassi relativa alla costituzione e diffusione di ampi database privati, talvolta utilizzati a fini commerciali e non sempre attraverso modalità trasparenti.

La condotta incriminata è quella di colui che comunica o diffonde, e al fine di meglio comprenderla, è opportuno richiamare le definizioni di "comunicazione" e "diffusione" di cui all'art 2-ter; 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, dalle persona autorizzate, ai sensi dell'art. 2-quaterdecies[54], al trattamento dei dati personali sotto l'autorità diretta del titolare o responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione»[55]; per "diffusione". si intende invece «il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione»[56].

In aggiunta alle condotte di comunicazione e diffusione, si noti il riferimento a un altro importante elemento costitutivo del reato, caratterizzato dal fatto che i dati personali particolari (sensibili) o giudiziari trattati in violazione e fuori dai limiti previsti dalla legge per trattamenti di interesse pubblico o necessari per motivi di interesse pubblico devono essere relativi a un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala.

---

[54] Art 2 quaterdecies Codice *privacy* così rubricato: «Attribuzione di funzioni e compiti a soggetti designati», stabilisce quanto segue: «Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta».

[55] Cfr. Articolo 2 ter, comma 4, lett. a) Codice *privacy*.

[56] Cfr. Articolo 2 ter, comma 4, lett. b) Codice *privacy*.

Perciò l'art. 167 bis è tassativo nell'indicare l'oggetto materiale sul quale la condotta di comunicazione e diffusione deve ricadere: il reato si configura solo quando la comunicazione o la diffusione riguardi un archivio automatizzato di dati personali (o una sua parte sostanziale).

L'archivio non viene definito dal decreto; tuttavia ai fini del GDPR per "archivio" si intende «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 che sia trattato in forma elettronica»[57].

Più ostica la definizione di "parte sostanziale" dell'archivio, concetto imprendibile e vago, che contribuisce al rischio di contrasto con il principio di tassatività delle norme penali insito tanto nell'articolo 167-bis che nel 167-ter. La sostanza potrebbe essere intesa come una parte, pur minima in termini quantitativi, ma riguardante elementi chiave o particolarmente sensibili dell'archivio; oppure potrebbe riguardare una dimensione quantitativa dei dati oggetto di trattamento illecito. Questa seconda tesi sembrerebbe doversi escludere in quanto, se di mera quantità si fosse trattato, sarebbe stato sufficiente il criterio della larga scala di trattamento che invece si riferisce al trattamento dei dati a monte e non, necessariamente alla parte oggetto di diffusione e comunicazione illecita[58].

Proprio in merito al concetto di "larga scala" del trattamento anche esso è un requisito oggettivo connotante della condotta, requisito ben difficile da determinare con sufficiente precisione e esposto a rischi di infrazione del principio di tassatività delle norme penali.

Così come il concetto di "archivio", neppure quello di "larga scala" viene definito dal decreto di adeguamento, ma questo neppure dal GDPR; anche se il *considerandum* n. 91[59] del GDPR fornisce utili indicazioni in quanto

[57] Cfr. Articolo 4 GDPR: «Definizioni».

[58] BOLOGNINI L. PELINO E., *Codice privacy: tutte le novità del d.lgs. 101/2018*, Milano, 2019.

[59] Considerando n. 91 GDPR: «Ciò dovrebbe applicarsi in particolare ai trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato, ad esempio, data la loro sensibilità, laddove, in conformità con il grado di conoscenze tecnologiche raggiunto, si utilizzi una nuova tecnologia su larga scala, nonché ad altri trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati, specialmente

afferma che «i trattamenti su larga scala ricomprendono tutti quei trattamenti che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato».

Qualche altra indicazione utile viene data dal Gruppo di Lavoro Articolo 29[60] e fatta propria dal Comitato Europeo per la protezione dei dati; si raccomanda di tenere conto, per definire se un trattamento sia effettuato su larga scala o meno, di fattori quali il numero di soggetti interessati dal trattamento, in termini assoluti o espressi in percentuale alla popolazione di riferimento, il volume dei dati o le diverse tipologie di dati oggetto del trattamento, la durata o la persistenza dell'attività di trattamento, la portata geografica.

Nulla, purtroppo, di così preciso da poter superare la critica di eccessiva indefinitezza del reato[61]. Sicuramente, la larga scala è da intendersi come requisito connesso non alla diffusione o alla comunicazione illecite, ma al trattamento di dati contenuti nell'archivio; la comunicazione o la diffusione potrebbero riguardare anche solo una parte sostanziale (qualitativa e non quantitativa).

Il riferimento a un concetto così ampio e poco definito di banca dati per una condotta così grave come quella della diffusone illecita secondo parte della dottrina[62] sembrerebbe azzardato e rischia di escludere gran parte dei piccoli ma gravissimi trattamenti senza consenso di quantità di dati personali che

---

qualora tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti. È opportuno altresì effettuare una valutazione d'impatto sulla protezione dei dati nei casi in cui i dati personali sono trattati per adottare decisioni riguardanti determinate persone fisiche in seguito a una valutazione sistematica e globale di aspetti personali relativi alle persone fisiche, basata sulla profilazione di tali dati, o in seguito al trattamento di categorie particolari di dati personali, dati biometrici o dati relativi a condanne penali e reati o a connesse misure di sicurezza. Una valutazione d'impatto sulla protezione dei dati è altresì richiesta per la sorveglianza di zone accessibili al pubblico su larga scala, in particolare se effettuata mediante dispositivi optoelettronici, o per altri trattamenti che l'autorità di controllo competente ritiene possano presentare un rischio elevato per i diritti e le libertà degli interessati, specialmente perché impediscono a questi ultimi di esercitare un diritto o di avvalersi di un servizio o di un contratto, oppure perché sono effettuati sistematicamente su larga scala. Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato. In tali casi non dovrebbe essere obbligatorio procedere a una valutazione d'impatto sulla protezione dei dati».

[60] Si tratta del gruppo di lavoro europeo indipendente che ha trattato questioni relative alla protezione della vita privata e dei dati personali fino al 25 maggio 2018 (entrata in vigore del GDPR).

[61] BOLOGNINI L. PELINO E., *Codice privacy: tutte le novità del d.lgs. 101/2018,* Milano, 2019.

[62] RICCIO G. M. SCORZA G. BELISARIO E., *GDPR e normativa privacy,* Milano, 2018

non arrivano a costituire una banca dati su larga scala. Si prenda in considerazione anche il rischio che corre l'autorità giudiziaria, di non poter indagare ipotesi di violazioni di piccole ma specifiche banche dati oggetto della violazione ma non oggetto di trattamento su larga scala. Sarebbe stato forse più opportuno legare la condotta alla comunicazione e diffusione illecita di dati sensibili e giudiziari, a prescindere dalla presenza di un rilevante numero di soggetti o ad un trattamento su larga scala[63].

Un'ulteriore osservazione da richiamare è quella relativa al caso in cui, qualora un titolare ritenga che i propri trattamenti non siano da considerare su larga scala, è tenuto a motivarlo ed a dimostrare, conseguentemente, nel caso in cui si proceda a controlli, che la sua valutazione si sia basata su evidenze oggettive e concrete. In questo momento, appare più che mai difficile farsi carico di tale *onus probandum*, in quanto, così come sia complesso definire quando si rientra nella larga scala, appare *a contrario*, difficile dimostrare quando non si rientri.

Tornando all'analisi della struttura di tale reato, nonostante l'apparente esteso ambito applicativo derivante dal "chiunque", individuato dall'articolo in esame come soggetto attivo del reato, la portata della fattispecie si restringe, in quanto il reato è configurabile solo qualora la diffusione o comunicazione dei dati avvenga in violazione di specifiche e limitate disposizioni normative per lo più applicabili a quei soggetti che trattano dati professionalmente o per obbligo di legge; da ciò deriva che tale fattispecie troverà applicazione in un numero molto limitato di casi.

Il comma 2 dell'articolo 167-bis, il quale va a punire la comunicazione o diffusione di un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, che avvenga non in violazione di specifiche disposizioni di legge, ma senza consenso, ove questo sia richiesto, altro non è che l'erede dell'ultimo periodo del comma uno del vecchio articolo 167[64], seppur con evidenti differenze; notiamo

[63] RICCIO G. M. SCORZA G. BELISARIO E., *GDPR e normativa privacy*, Milano, 2018

[64] Articolo 167 comma 1 codice *privacy*, vecchio testo: «Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento

infatti il trattamento su larga scala e il più limitato pericolo di violazione che richiede la mancanza della base giuridica del consenso.

Si tratta di un reato che viene punito a titolo di dolo specifico, tanto nel primo quanto nel secondo comma; accanto al profitto è stato affiancato il dolo di danno, similmente all'articolo 167, ma con la differenza che il danno da arrecarsi in questo caso non si riferisce al solo interessato, ben potrà riguardare anche terzi.

Inoltre, questo delitto non prevede la condizione obiettiva di punibilità del nocumento dell'interessato in quanto probabilmente il legislatore, nel disegnare tale fattispecie criminosa, ritiene che la nocività sia *in re ipsa*.

In virtù del rinvio contenuto al terzo comma di detto articolo, all'articolo 167 commi 4[65], 5[66] e 6[67], il pubblico ministero, quando ha notizia di questo reato, ne informa senza ritardo il Garante, il quale trasmetterà allo stesso pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere l'esistenza di un reato. Si comprende da ciò, come il pubblico ministero procedente abbia l'obbligo di informare il Garante, e sarà quest'ultimo a valutare la sussistenza degli estremi del reato; in tal modo l'obbligatorietà dell'azione penale finisce per essere subordinata al parere del Garante.

Il delitto è punito gravemente, con la reclusione da uno a sei anni, ma la pena è diminuita, ove per gli stessi fatti venga applicata anche una sanzione amministrativa.

---

di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi».

[65] Articolo 167 comma 4 Codice *privacy*: «Il Pubblico ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante».

[66] Articolo 167 comma 5 Codice *privacy*: «Il Garante trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al più tardi al termine dell'attività di accertamento delle violazioni delle disposizioni di cui al presente decreto».

[67] Articolo 167 comma 6 Codice *privacy*: «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 e' stata riscossa, la pena è diminuita».

I sei anni di reclusione (nel massimo) hanno come conseguenza *ex* art. 266 c.p.p.[68], che si possa operare, nella ricerca della prova per tali delitti, l'intercettazione di conversazioni o comunicazioni telefoniche e di altre forme di comunicazione, nonché l'intercettazione di comunicazioni tra presenti. Ed è inoltre ammesso *ex* art. 381 c.p.p.[69], l'arresto facoltativo in flagranza da parte di ufficiali e agenti di polizia giudiziaria.

3.3 Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala, articolo 167-ter

Il nuovo articolo 167 ter[70] del Codice *privacy* è rubricato «Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala» e provvede a punire con la reclusione da uno a quattro anni, «chiunque, al fine di trarre profitto per sé o per 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».

Si tratta di una fattispecie incriminatrice del tutto nuova che ha come *fulcrum* «l'acquisizione fraudolenta».

Gli elementi essenziali del delitto di cui all'art. 167-ter sono i medesimi dell'art. 167-bis, alla cui analisi si rimanda[71].

La differenza della condotta *ex* articolo 167-ter rispetto a quella di cui all'articolo 167-bis sta nel fatto che mentre l'articolo 167-bis si occupa di

[68] Art. 266 c.p.p. «Limiti di ammissibilità» al comma uno stabilisce: «L'intercettazione di conversazioni o comunicazioni telefoniche e di altre forme di telecomunicazione è consentita nei procedimenti relativi ai seguenti reati: a) delitti non colposi per i quali è prevista la pena dell'ergastolo o della reclusione superiore nel massimo a cinque anni».

[69] Art. 381 c.p.p. «Arresto facoltativo in flagranza» al comma uno stabilisce quanto segue: «Gli ufficiali e gli agenti di polizia giudiziaria hanno facoltà di arrestare chiunque è colto in flagranza di un delitto non colposo, consumato o tentato, per il quale la legge stabilisce la pena della reclusione superiore nel massimo a tre anni ovvero di un delitto colposo per il quale la legge stabilisce la pena della reclusione non inferiore nel massimo a cinque anni».

[70] Articolo 167-ter codice *privacy* così rubricato: «Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala», stabilisce quanto segue: «Salvo che il fatto costituisca più grave reato, chiunque, 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 è punito con la reclusione da uno a quattro anni.
Per il reato di cui al comma 1 si applicano i commi 4, 5 e 6 dell'articolo 167».

[71] Cfr. Capitolo III Paragrafo 3.2

punire la comunicazione o diffusione avvenuta in maniera illecita e a determinate condizioni (in violazione degli articoli 2-ter, 2-sexies, 2-octies, comma uno; o senza il consenso, comma due), in *subiecta* fattispecie si punisce non il semplice ricevente di tali informazioni, bensì, soggetto attivo deve necessariamente essere colui che, attivamente, con artifizi o raggiri, acquisisca l'archivio elettronico di dati personali oggetto di trattamento su larga scala o una sua parte sostanziale.

Resta da domandarsi cosa si intenda per «acquisizione con mezzi fraudolenti», poiché né il decreto di adeguamento, né il GDPR ne danno un'espressa definizione.

Per mezzi fraudolenti si fa comunemente riferimento a quegli strumenti subdoli per la commissione del crimine, come artifizi o raggiri, bugie, inganni, ma anche reticenza di ciò che si dovrebbe comunicare.

Pertanto, si ritiene si tratti di un'acquisizione avvenuta mediante condotte che presuppongono la malafede, o in termini penalistici, il dolo, che consistano in rappresentazioni artificiose tali da determinare una falsa rappresentazione della realtà.

Per quanto riguarda l'oggetto materiale della condotta si rimanda nuovamente alle considerazioni svolte in relazione all'articolo 167-bis[72].

Anche in tale caso per la configurabilità del delitto *de quo* è richiesto come elemento psicologico il dolo specifico dell'agente di trarre per sé o per altri profitto unito a quello di arrecare danno.

È ammesso *ex* articolo 381 c.p.p.[73] l'arresto facoltativo in flagranza di reato da parte di ufficiali e agenti di polizia giudiziaria.

E analogamente a quanto detto per l'articolo 167-bis, l'articolo 167-ter al comma 2 rinvia ai commi 4, 5 e 6 dell'articolo 167, ossia alle norme in materia di riduzione della pena in caso di pagamento della sanzione

[72] Cfr. Capitolo III Paragrafo 3.2

[73] Articolo 381 c.p.p. rubricato «Arresto facoltativo in flagranza» al comma uno stabilisce quanto segue: «Gli ufficiali e gli agenti di polizia giudiziaria hanno facoltà di arrestare chiunque è colto in flagranza di un delitto non colposo, consumato o tentato, per il quale la legge stabilisce la pena della reclusione superiore nel massimo a tre anni ovvero di un delitto colposo per il quale la legge stabilisce la pena della reclusione non inferiore nel massimo a cinque anni».

amministrativa pecuniaria e quelle relative allo scambio di informazioni fra pubblico ministero e Garante.

Per gli stessi motivi di cui al 167-bis, anche l'articolo 167-ter e il suo riferimento a «un'acquisizione fraudolenta di un archivio automatizzato o una parte sostanziale di esso contenete dati personali oggetto di trattamento su larga scala», appare ai limiti del principio di tassatività e rischia di lasciare senza indagine e quindi anche senza punizione moltissime ipotesi meritevoli invece di tutela[74].

3.4 Osservazioni sui nuovi articoli 168, 170, 171, 172 Codice privacy

L'articolo 168 è stato sostituito dalla novella[75] ed è ora rubricato: «Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante».

La norma recita: «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, è punito con la reclusione da sei mesi a tre anni», e il comma due prevede: «Fuori dei casi di cui al comma 1, è punito 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».

Chiunque dichiara o attesta il falso al Garante continua a essere sanzionato penalmente dall'articolo 168 codice *privacy,* il quale così come novellato dal decreto di adeguamento, ne mantiene sostanzialmente invariata la punibilità, ma rispetto a prima[76], la disposizione viene integrata con la previsione, al comma 2, di una nuova fattispecie di reato che punisce con la reclusione fino

[74] RICCIO G. M. SCORZA G. BELISARIO E., *GDPR e normativa privacy,* Milano, 2018.

[75] D.lgs. 101/2018

[76] Il vecchio testo dell'art. 168 codice privacy prevedeva: «Chiunque, 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, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni».

a un anno chiunque intenzionalmente cagiona un'interruzione o turba la regolarità di un procedimento o di un accertamento svolto dinanzi al Garante. Si tratta di una fattispecie che richiama l'articolo 340 c.p.[77], rubricato «Interruzione di un ufficio o servizio pubblico o di un servizio di pubblica necessità», del quale riprende anche il massimo della pena edittale, coerentemente col principio di eguaglianza. L'articolo 340 si colloca nel Libro II, Titolo II, Capo II «Dei delitti dei privati contro la pubblica amministrazione», e da ciò si evince come i due articoli condividano non solo lo stesso trattamento sanzionatorio, ma anche la stessa ratio, in quanto entrambi sono posti a garanzia del buon andamento della giustizia e della pubblica amministrazione e mirano a punire delle condotte che compromettono o ledono il regolare e ordinato andamento della pubblica amministrazione. L'articolo 168 è posto a tutela dell'azione del Garante, al fine di garantire la massima trasparenza e fedeltà nelle acquisizioni da parte dello stesso.

Entrambi sono reati comuni avente però carattere sussidiario, sottolineato dalla clausola di riserva posta all'*incipit*, in quanto tali norme si applicano solo ove la condotta non integri un'altra più grave fattispecie criminosa.

Il comma 1 ha espunto il riferimento alle «notificazioni, comunicazioni, atti, documenti o dichiarazioni resi o esibiti», previste nel vecchio testo, ma la condotta rimane la medesima. Viene infatti punita la dichiarazione o attestazione di false notizie o circostanze e la produzione di atti o documentazioni false, ossia il c.d. "mendacio documentale".

Si tratta di una fattispecie particolarmente insidiosa[78], in quanto può colpire, anche chi, ad esempio, abbia rappresentato durante un'ispezione o in risposta alle richieste del Garante, fatti non corrispondenti alla realtà o contrastanti con la documentazione fornita a margine dell'ispezione.

[77] Art. 340 c.p. rubricato: «Interruzione di un ufficio o servizio pubblico o di un servizio di pubblica necessità» che stabilisce quanto segue: «Chiunque, fuori dei casi preveduti da particolari disposizioni di legge, cagiona una interruzione o turba la regolarità di un ufficio o servizio pubblico o di un servizio di pubblica necessità, è punito con la reclusione fino a un anno. I capi, promotori od organizzatori sono puniti con la reclusione da uno a cinque anni».

[78] BOLOGNINI L. PELINO E., *Codice privacy: tutte le novità del d.lgs. 101/2018*, Milano, 2019.

Al fine di scongiurare il rischio di assoggettare a pena il fisiologico interloquire del Responsabile della Protezione Dati con l'autorità di controllo, si richiede una particolare colorazione dell'elemento soggettivo, almeno in termini di consapevolezza della falsità delle informazioni o delle documentazioni trasmesse.

Si ritiene che l'irrilevanza dell'ulteriore elemento dell'*animus nocendi,* che avrebbe escluso *ex ante* ogni possibile rischio di estendere l'area di punibilità, dipenda dalla necessità di valorizzare maggiormente il profilo dell'offensività della condotta anche sul versante del profilo psicologico.

Il comma 2 si occupa di incriminare la condotta di «chiunque, fuori dai casi di dichiarazioni o attestazioni false di notizie o circostanze o produzioni di atti o documenti falsi, in un procedimento o nel corso di accertamenti dinanzi al Garante, cagioni un'interruzione o turbi la regolarità di un procedimento, dinanzi al Garante o degli accertamenti dallo stesso svolti».

Si tratta di una norma più generale e ampia rispetto a quella di cui al comma 1, perciò suscettibile di essere criticata in relazione al rigoroso principio di tassatività caratterizzante le fattispecie penali.

La condotta interruttiva si sostanzia in una mancato svolgimento di un procedimento o di un accertamento per un periodo di tempo apprezzabile, mentre il turbamento si riferisce a un'alterazione della regolarità nel suo complesso.

Le condotte di interruzione e turbamento vengono punite a condizione che siano poste in essere «intenzionalmente»; tale avverbio implica delle considerazioni circa l'elemento soggettivo, diverse rispetto a quelle fatte per il comma uno, in quanto non è qui sufficiente la mera consapevolezza, ma è richiesto il dolo intenzionale.

La realizzazione dell'interruzione o del turbamento è il fine cui tende la condotta, non l'evento del reato, il quale rimane di mera condotta, che si perfeziona nel momento in cui le condotte di interruzione o turbamento sono poste in essere dall'agente.

Si è ritenuto opportuno conservare l'opzione punitiva giacché tale fattispecie sanziona condotte caratterizzate da apprezzabile meritevolezza di pena e contrassegnate da significativo disvalore.

Il *GDPR* non ha previsto specifiche sanzioni amministrative per condotte di questo tipo, pertanto, ciò permette *in primis*, di evitare problemi in punto di *ne bis in idem*, e consente altresì di ritenere giustificato e rispondente al canone dell'*extrema ratio* il ricorso alla sanzione penale.

Procedendo con la disamina delle ulteriori tre disposizioni osserviamo quanto segue.

L'articolo 170[79], rubricato «Inosservanza dei provvedimenti del Garante», sanziona con la reclusione da tre mesi a due anni, la condotta di chi non osserva i provvedimenti adottati dal Garante: si tratta, più nello specifico, dei provvedimenti adottati da quest'ultimo ai sensi dell'articolo 58 comma 2 lett. f del Regolamento (ossia in attuazione del proprio potere di imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento), nonché ai sensi dell'articolo 2-septies (inerente i dati genetici, biometrici o relativi alla salute) o dei provvedimenti generali di cui all'articolo 21 comma 1 del decreto di attuazione dell'articolo 13 della legge 163/2017.

L'articolo 171 rubricato «Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori», sembra essere frutto di una mera riorganizzazione interna del Codice. Lo stesso recita: «La violazione delle disposizioni di cui agli articoli 4, comma 1, e 8 della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della medesima legge».

L'attuale formulazione ha come *fulcrum* la tutela delle regole poste a tutela del controllo a distanza dei lavoratori, che necessita molto spesso di apposito accordo sindacale (articolo 4 Statuto dei Lavoratori), nonché delle norme

[79] Articolo 170 codice *privacy*: «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 è punito con la reclusione da tre mesi a due anni».

relative al divieto di indagine sulle opinioni religiose, politiche o sociali dei lavoratori, ovvero su atti non rilevanti ai fini della valutazione dell'attitudine professionale di questi ultimi (articolo 8 Statuto dei Lavoratori).

L'articolo 172[80] vecchio testo si limitava a imporre la pubblicazione della sentenza in seguito alla condanna per uno dei delitti previsti dal presente codice.

Nella formulazione attuale dell'articolo 172, così come novellato, sono state aggiunte le parole «secondo le modalità di cui all'articolo 36[81], secondo e terzo comma del codice penale».

Si ripropongono anche nella nuova versione dell'articolo, le stesse perplessità relative al testo precedente, in relazione all'applicabilità della pena accessoria *ex lege*, tutte le volte in cui l'imputato venga condannato per uno dei delitti previsti dal presente codice, indipendentemente dal comportamento criminoso tenuto in concreto e indipendentemente da qualsiasi valutazione caso per caso condotta dal giudice *a quo*, al fine di limitarne l'applicazione ai soli casi più gravi.

4. Fattispecie penali e amministrative: rischio di violazione del ne bis in idem?

In relazione alla tutela penale da accordare al trattamento di dati personali, questione su cui il *GDPR* era rimasto silente, essendo la previsione delle sanzioni penali materia di esclusiva competenza nazionale, il legislatore italiano, ha invece preso posizione.

Prima di soffermarci sulle principali disposizioni di riferimento, afferenti al novero delle fonti normative della materia – *Considerandum* n. 149 e articolo

[80] Articolo 172 codice *privacy*: «Pene accessorie», stabilisce quanto segue: «La condanna per uno dei delitti previsti dal presente codice importa la pubblicazione della sentenza, ai sensi dell'articolo 36, secondo e terzo comma, del codice penale».

[81] Articolo 36 c.p.: «Pubblicazione della sentenza penale di condanna»: «La sentenza di condanna all'ergastolo è pubblicata mediante affissione nel Comune ove è stata pronunciata, in quello ove il delitto fu commesso, e in quello ove il condannato aveva l'ultima residenza. La sentenza di condanna è inoltre pubblicata nel sito internet del Ministero della giustizia. La durata della pubblicazione nel sito è stabilita dal giudice in misura non superiore a trenta giorni. In mancanza, la durata è di quindici giorni. La pubblicazione è fatta per estratto, salvo che il giudice disponga la pubblicazione per intero; essa è eseguita d'ufficio e a spese del condannato. La legge determina gli altri casi nei quali la sentenza di condanna deve essere pubblicata. In tali casi la pubblicazione ha luogo nei modi stabiliti nei due capoversi precedenti».

84 *GDPR*– è qui da rammentare, a scanso di equivoci l'articolo 83 comma due TFUE[82], il quale prevede al massimo un potere generale di direzione e indirizzo in materia di legislazione criminale per l'Unione Europea.

Su queste basi, il *GDPR* non avrebbe potuto prevedere al suo interno specifici delitti o contravvenzioni penali.

L'articolo 84 *GDPR* recita: «Gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del presente regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione. Tali sanzioni devono essere effettive, proporzionate e dissuasive. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 1 al più tardi entro 25 maggio 2018, e comunica senza ritardo ogni successiva modifica».

Secondo tale articolo, viene riconosciuto quindi agli stati membri il potere di introdurre nuovi illeciti per le ipotesi di violazioni del Regolamento europeo,

[82] Cfr. Articolo 83 Trattato sul funzionamento dell'Unione Europea: «Il Parlamento europeo e il Consiglio, deliberando mediante direttive secondo la procedura legislativa ordinaria, possono stabilire norme minime relative alla definizione dei reati e delle sanzioni in sfere di criminalità particolarmente grave che presentano una dimensione transnazionale derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni.
Dette sfere di criminalità sono le seguenti: terrorismo, tratta degli esseri umani e sfruttamento sessuale delle donne e dei minori, traffico illecito di stupefacenti, traffico illecito di armi, riciclaggio di denaro, corruzione, contraffazione di mezzi di pagamento, criminalità informatica e criminalità organizzata. In funzione dell'evoluzione della criminalità, il Consiglio può adottare una decisione che individua altre sfere di criminalità che rispondono ai criteri di cui al presente paragrafo. Esso delibera all'unanimità previa approvazione del Parlamento europeo. Allorché il ravvicinamento delle disposizioni legislative e regolamentari degli Stati membri in materia penale si rivela indispensabile per garantire l'attuazione efficace di una politica dell'Unione in un settore che è stato oggetto di misure di armonizzazione, norme minime relative alla definizione dei reati e delle sanzioni nel settore in questione possono essere stabilite tramite direttive. Tali direttive sono adottate secondo la stessa procedura legislativa ordinaria o speciale utilizzata per l'adozione delle misure di armonizzazione in questione, fatto salvo l'articolo 76. Qualora un membro del Consiglio ritenga che un progetto di direttiva di cui al paragrafo 1 o 2 incida su aspetti fondamentali del proprio ordinamento giuridico penale, può chiedere che il Consiglio europeo sia investito della questione. In tal caso la procedura legislativa ordinaria è sospesa. Previa discussione e in caso di consenso, il Consiglio europeo, entro quattro mesi da tale sospensione, rinvia il progetto al Consiglio, ponendo fine alla sospensione della procedura legislativa ordinaria.
Entro il medesimo termine, in caso di disaccordo, e se almeno nove Stati membri desiderano instaurare una cooperazione rafforzata sulla base del progetto di direttiva in questione, essi ne informano il Parlamento europeo, il Consiglio e la Commissione. In tal caso l'autorizzazione a procedere alla cooperazione rafforzata di cui all'articolo 20, paragrafo 2 del trattato sull'Unione europea e all'articolo 329, paragrafo 1 del presente trattato si considera concessa e si applicano le disposizioni sulla cooperazione rafforzata».

in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie *ex* articolo 83[83].

L'unico limite posto dal Regolamento si rinviene al *Considerandum* n. 149 e consiste nell'evitare che la previsione di norme incriminatrici, produca violazioni sistematiche del diritto a non essere puniti due volte per il medesimo fatto di reato. Il *considerandum* n. 149 dispone: «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. Tali sanzioni penali possono altresì autorizzare la sottrazione dei profitti ottenuti attraverso violazioni del presente Regolamento. Tuttavia, 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».

L'impressione che si ha, dalla lettura di tali disposizioni, è quella di trovarsi dinanzi a una riserva quasi-direttiva lasciata agli stati membri per l'imposizione di sanzioni penali[84].

Posto che, spetta agli stati membri introdurre le norme relative alle altre «sanzioni non amministrative pecuniarie», per le violazioni del Regolamento, «adottando tutti i provvedimenti necessari per assicurarne l'applicazione» e, cioè imponendole mediante norme interne.

Tra queste altre sanzioni, rientrano *ex considerandum* 149 le sanzioni penali. Le sanzioni penali, ai sensi del predetto *considerandum* 149 dovrebbero potere essere adottate dagli stati membri non solo per violazioni del *GDPR*, ma anche per le violazioni di norme nazionali adottate in virtù e nei limiti del *GDPR*. L'uso del verbo "dovere" al condizionale, abbinato al "potere"

[83] Articolo 83 *GDPR*: «Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive […].»

[84] BOLOGNINI L., BISTOLFI C., PELINO E., *Il regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016

esclude l'obbligo ma conduce a ritenere che si tratti di una quasi direttiva, così come osservato da autorevole dottrina[85].

Inoltre, il *considerandum* n. 149, da un lato ammette che le sanzioni penali possano autorizzare la sottrazione dei profitti ottenuti attraverso la violazione del *GDPR*, il che significa che il contravventore verrà colpito anche in senso pecuniario, ma sul piano penale e non amministrativo; dall'altro, precisa che «l'imposizione di sanzioni penali per violazione di norme nazionali e di sanzioni amministrative» deve essere fondata sull'articolo 50[86] della Carta dei diritti fondamentali dell'Unione Europea, che sancisce il diritto di non essere giudicati o puniti due volte per il medesimo reato, e sull'articolo 4[87] del Protocollo n. 7 della Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle Libertà fondamentali, che prevede lo stesso diritto di cui sopra.

Si tratta del principio cristallizzato nel brocardo del "*ne bis in idem*", già ben conosciuto nell'ordinamento penale italiano *ex* articolo 649 c.p.p.[88], il quale opera *in primis* sul piano sostanziale, ma subito dopo, anche sul piano processuale e, in ottica garantistica, impedisce che il soggetto già giudicato sia nuovamente sottoposto a processo per il medesimo fatto, pur se diversamente considerato per titolo, grado o circostanze.

---

[85] BOLOGNINI L., BISTOLFI C., PELINO E., *Il regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016

[86] Articolo 50 Carta dei diritti fondamentali UE, così rubricato: «Diritto di non essere giudicato o punito due volte per lo stesso reato»: «Nessuno può essere perseguito o condannato per un reato per il quale è già stato assolto o condannato nell'Unione a seguito di una sentenza penale definitiva conformemente alla legge».

[87] Articolo 4 Protocollo addizionale n.7, così rubricato: «Diritto a non essere giudicato o punito due volte»: «Nessuno può essere perseguito o condannato penalmente dalla giurisdizione dello stesso Stato per un reato per il quale è già stato assolto o condannato a seguito di una sentenza definitiva conformemente alla legge ed alla procedura penale di tale Stato. Le disposizioni del paragrafo precedente non impediscono la riapertura del processo, conformemente alla legge ed alla procedura penale dello Stato interessato, se fatti sopravvenuti o nuove rivelazioni o un vizio fondamentale nella procedura antecedente sono in grado di inficiare la sentenza intervenuta. Non è autorizzata alcuna deroga al presente articolo ai sensi dell'articolo 15 della Convenzione».

[88] Articolo 649 c.p.p.: «L'imputato prosciolto o condannato con sentenza o decreto penale divenuti irrevocabili non può essere di nuovo sottoposto a procedimento penale per il medesimo fatto, neppure se questo viene diversamente considerato per il titolo, per il grado o per le circostanze, salvo quanto disposto dagli articoli 69 comma 2 e 345. Se ciò nonostante viene di nuovo iniziato procedimento penale, il giudice in ogni stato e grado del processo pronuncia sentenza di proscioglimento o di non luogo a procedere, enunciandone la causa nel dispositivo».

Il legislatore europeo, istruito dalle vicende processuali verificatesi nel settore del *market abuse,* è consapevole di aver previsto sanzioni amministrative particolarmente gravi che la Corte di Strasburgo, sotto la lente dei celebri *Engel criteria*, potrebbe considerare di natura sostanzialmente penale. Posto ciò, l'applicazione allo stesso soggetto della sanzione solo formalmente amministrativa di matrice comunitaria e della sanzione penale di fonte nazionale, per il medesimo fatto, contrario alla normativa *privacy* potrebbero esporre lo Stato a censure per violazione del divieto di *bis in idem*.

L'arsenale sanzionatorio penale-amministrativo insieme, ispirato da un meccanismo cumulativo è stato da tempo additato dalla dottrina come difficilmente compatibile con il principio *dell'extrema ratio* che dovrebbe guidare il ricorso al diritto criminale; oltre che poco coerente rispetto ai fondamentali canoni della proporzionalità e ragionevolezza dell'intervento penale.

Con la pronuncia Grande Stevens e altri contro Italia del 2014 la Corte di Strasburgo ha dichiarato che il sistema del doppio binario italiano (in materia di manipolazione del mercato) è incompatibile con la Convenzione Europea dei Diritti dell'Uomo, nella misura in cui risulta lesivo del diritto a un equo processo e del principio del *ne bis in idem*.

È giusto pertanto ripercorrerne le tappe.

Nella sentenza Grande Stevens[89], ad avviso dei giudici della Corte Europea, dopo che sono state comminate sanzioni dalla Consob, l'avvio di un processo penale sugli stessi fatti violerebbe il principio giuridico del *ne bis in idem,* secondo cui non si può essere giudicati due volte per lo stesso fatto. I ricorrenti, infatti, dopo essere stati sanzionati nel 2007 dalla Consob, erano stati rinviati a giudizio, per essere poi assolti in primo grado e condannati in appello.

Anche se il processo innanzi alla Consob è amministrativo, infatti, le sanzioni inflitte possono essere considerate a tutti gli effetti come penali, anziché

[89] Corte Europea dei diritti dell'uomo, 4 marzo 2014; Grande Stevens e altri contro Italia, Ric. 18640/10, 18647/10, 18663/10, 18668/10 e 18698/10

amministrative, vista l'eccessiva severità delle stesse – sia per l'importo che per le sanzioni accessorie – oltre che per le loro ripercussioni sugli interessi del condannato. In quanto sanzioni penali, devono dunque osservare le garanzie che l'articolo 6 CEDU riserva ai processi penali.

Nella sentenza A e B c. Norvegia[90], la Corte afferma che non è possibile dedurre dall'articolo 4 protocollo 7 un divieto assoluto per gli Stati di imporre una sanzione amministrativa (ancorché qualificabile come "sostanzialmente penale" ai fini delle garanzie dell'equo processo) per quei fatti di evasione fiscale in cui è possibile, altresì, perseguire e condannare penalmente il soggetto, in relazione a un elemento ulteriore rispetto al mero mancato pagamento del tributo, come una condotta fraudolenta, alla quale non potrebbe dare risposta sanzionatoria adeguata la mera procedura "amministrativa". Nell'ottica, allora, di un conveniente bilanciamento tra gli interessi dell'individuo e quelli della comunità a prevedere un approccio calibrato ad una sanzione 'integrata', frutto degli interventi di distinte autorità (amministrative e giurisdizionali), la Corte ritiene di dover valorizzare proprio il test della «*sufficiently close connection in substance and time*»[91] ricavato da parte della propria precedente giurisprudenza e riproposto alla sua attenzione dagli stessi giudici supremi norvegesi, alla presenza del quale, non sussisterebbe violazione del *ne bis in idem*.

Si tratta di un'importante pronuncia giurisprudenziale ma non di un vero e proprio *revirement*, in quanto la Corte di Giustizia il 20 marzo 2018[92], è intervenuta nuovamente sul delicato problema delle limitazioni applicate al principio del *ne bis in idem*, in considerazione della corretta interpretazione

[90] Corte EDU (grande Camera), sent. 15 novembre 2016, A e B c. Norvegia, ric. n. 24130/11 e 29758/1

[91] Il criterio della connessione sostanziale sufficientemente stretto implica che: i due procedimenti perseguono scopi complementari e hanno ad oggetto differenti aspetti della medesima condotta antisociale; l'apertura di un doppio percorso procedimentale rappresenti una conseguenza prevedibile della medesima condotta; i due procedimenti siano condotti in modo da evitare per quanto possibile ogni duplicazione nella raccolta e valutazione della prova; la determinazione della sanzione irrogata al termine del procedimento che è divenuto definitivo per secondo tenga conto della sanzione irrogata con il provvedimento divenuto definitivo per primo. Il criterio della connessione temporale sufficientemente stretto non postula una conduzione simultanea di due procedimenti, ben potendo questi ultimi svilupparsi in via consequenziale: ciò che conta è che sussista un collegamento cronologico sufficientemente stretto, tali da evitare incertezza ritardo ed eccessiva protrarsi dei tempi di definizione.

[92] Corte di Giustizia dell'Unione Europea, Grande Sezione, 20 marzo 2018,
Cause C-524/15, C-537/16, C-596/16 e C-597/16

dell'articolo 50 della Carta dei diritti fondamentali dell'Unione Europea, letto alla luce dell'articolo 4 del Protocollo n. 7 della Convenzione Europea per la Salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata a Roma il 4 novembre 1950. Con la sentenza ha infatti precisato che per comprendere la natura sostanzialmente penale delle sanzioni amministrative occorre fare riferimento ai tre criteri elaborati dalla giurisprudenza della medesima Corte e cioè alla qualificazione giuridica dell'illecito nel diritto nazionale, alla natura dell'illecito ed al grado di severità della sanzione cui l'interessato rischia di incorrere. Per l'accertamento della sussistenza dell'*idem factum*, ha altresì specificato la Corte, occorre fare riferimento esclusivamente al criterio dell'identità dei fatti materiali, intesi come un insieme di circostanze concrete, inscindibilmente collegate tra loro, che hanno condotto all'assoluzione o alla condanna definitiva dell'interessato, essendo a tal fine irrilevante la qualificazione giuridica o il *nomen iuris* dato a quel fatto dall'ordinamento nazionale.

La corte ha inoltre illustrato i motivi in base ai quali nel caso di specie la sanzione amministrativa irrogata fosse da considerarsi, invece, come sanzione penale, ed i fatti oggetto del procedimento amministrativo, sono gli stessi di quelli al vaglio del Tribunale Penale.

Più precisamente la corte ha affermato: «Ciò considerato, risulta che la normativa nazionale di cui al procedimento principale consente di celebrare un procedimento riguardante una sanzione amministrativa pecuniaria, di natura penale ai sensi dell'articolo 50 della Carta, nei confronti di una persona […] per condotte illecite che integrano una manipolazione del mercato, per le quali è già stata pronunciata a suo carico una condanna penale definitiva. Orbene, un simile cumulo di procedimenti e di sanzioni costituisce una limitazione del diritto garantito da detto articolo 50».

È comunque riconosciuta agli stati membri la facoltà di prevedere il doppio binario sanzionatorio, penale e amministrativo, per reprimere aspetti diversi di un medesimo fatto.

Le sentenze della Corte specificano che il cumulo di procedimenti e di sanzioni di natura penale e amministrativa può essere giustificato qualora tali

procedimenti e tali sanzioni siano previste dalla legge, ci sia coordinamento e quindi perseguano scopi complementari riguardanti, eventualmente, aspetti diversi del medesimo comportamento illecito, perseguano un fine di interesse generale, e purché ciò avvenga nel rispetto del principio di proporzionalità. Quest'ultimo impone che, «il cumulo di procedimenti e di sanzioni previsto da una normativa nazionale non ecceda i limiti di ciò che è idoneo e necessario al conseguimento degli scopi legittimi perseguiti da tale normativa, fermo restando che qualora sia possibile una scelta tra più misure appropriate, si deve ricorrere alla meno restrittiva e che gli inconvenienti causati dalla stessa non devono essere sproporzionati rispetto agli scopi perseguiti».

Sulla base delle considerazioni appena svolte, occorre evidenziare che la giurisprudenza delle corti europee, e segnatamente della Corte di giustizia e della Corte europea dei diritti dell'uomo, non esclude rigidamente la compatibilità con il *ne bis in idem* del doppio binario sanzionatorio. Al contrario, entrambe le corti hanno individuato una serie di parametri cui ancorare l'apprezzamento circa la sussistenza di un rapporto di integrazione ovvero di mera duplicazione tra i due procedimenti, purché il sacrificio imposto alle garanzie dell'interessato sia valutato alla luce del principio di proporzionalità, che impone il rispetto di un canone di necessità nell'ambito della tutela di un obiettivo di interesse generale.

Nonostante l'incertezza dei confini del *ne bis in idem* e la relativa flessibilità dimostrata dalle corti nell'interpretare questo principio, la scelta di escludere la previsione di sanzioni penali appare avventata e non ponderata.

Sulla base dell'articolo 83 – che dedica ampio spazio al tema delle sanzioni amministrative pecuniarie, definendone le condizioni generali per l'irrogazione – e dell'articolo 84 – che, avente carattere residuale, facoltizza la possibilità per gli Stati membri di introdurre altre sanzioni «effettive, proporzionate e dissuasive», ma che, soprattutto, si applicano «in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83» – il messaggio del *GDPR* appare chiaro: gli Stati membri conservano piena e impregiudicata discrezionalità nella scelta di ricorrere a

sanzioni di altro tipo, come quelle penali: non possono, tuttavia, sottoporre a sanzioni diverse violazioni che siano già soggette a sanzioni amministrative. È dunque evidente l'obiettivo del *GDPR:* evitare che sul medesimo presupposto si applichino sia una sanzione amministrativa sia una sanzione penale.

Le principali criticità rispetto al rischio di violazione del divieto di *bis in idem*, riguardano il reato di trattamento illecito di dati personali.

Ad una prima lettura sembra che lo Stato italiano abbia deciso di arginare il pericolo di violazioni sistemiche del divieto di doppio giudizio, da un lato ridimensionando fortemente il limite edittale massimo delle sanzioni amministrative rispetto alle indicazioni del Regolamento e dall'altro mantenendo nella fattispecie penale elementi, quali il dolo specifico di profitto e di danno e l'evento di nocumento alla persona offesa, sempre salvo il caso in cui il fatto costituisca più grave reato, che vogliono delimitare l'ambito di applicazione della norma incriminatrice ed evitare sovrapposizioni tra illecito penale e illecito amministrativo.

Le condotte previste all'articolo 167 comma 1 e comma 2 restano però soggette a sanzioni amministrative, tuttavia laddove sia riscontrabile la finalità di ottenere profitto o di cagionare un danno e sia possibile provare il nocumento del danneggiato, tali condotte potranno dare luogo a una responsabilità di natura penale.

Il meccanismo di coordinamento pare essere poco chiaro.

Vale la pena ricordare a tal proposito la tesi riferimento al denunziato eccesso di delega che colpirebbe lo schema di decreto legislativo in riferimento all'abrogazione dell'articolo 167, e alla conseguente eliminazione delle sanzioni penali.

L'articolo 13, comma 3, lett. e) della l. 163/2017, specifica che il governo è delegato ad "adeguare […] 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". Tale previsione, ben lungi dall'imporre un obbligo di criminalizzazione, codifica il potere del governo,

in sede di adozione del decreto legislativo, di adottare sanzioni penali e amministrative rispondenti ai criteri di efficacia, dissuasività e proporzionalità, potere che però, va coordinato con quanto previsto dal GDPR, che facoltizza il ricorso a sanzioni penali per dare invece certa copertura sanzionatoria (quantomeno a livello amministrativo) a determinate violazioni, elencate all'artcolo 83.

La *ratio* della delega affidata al Governo è assai ampia e sicuramente se i principi e i criteri direttivi impartiti dal legislatore delegante fossero stati più analitici e dettagliati, più ridotti sarebbero stati i margini di discrezionalità lasciati al legislatore delegato.

Particolarmente forti sono, infatti, le preoccupazioni che le istituzioni europee manifestano verso il pericolo di violazione del *ne bis in idem*, che alimenta non solo il rischio di una sovraesposizione sanzionatoria ma soprattutto e prima ancora, quello di una differente valutazione in merito all'esistenza di una violazione.

Sicuramente, non pare che il confronto con i criteri sopra ricordati restituisca indicazioni univoche e inequivoche circa il rispetto, da parte della normativa italiana in materia, del divieto di *bis in idem.* E su questo *nulla quaestio.*

Ma se l'articolo 167 fosse stato depenalizzato, ciò non avrebbe potuto trovare una giustificazione nel *considerandum* n. 149 del Regolamento. Quest'ultimo, non dispone in alcun modo che il delitto di trattamento illecito debba essere abrogato o che non possa essere prevista una condotta che sia punita sia con la pena della reclusione, sia con la sanzione amministrativa.

Ma anzi, stabilisce 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», e attenendoci alla lettera della disposizione, e perciò seguendo l'orientamento della Corte, sul rapporto tra sanzione penale e quella amministrativa, questa non è contrario alla sussistenza del *ne bis in idem* – il quale tra l'altro sussiste solo quando il giudice ritiene che la sanzione amministrativa irrogata assuma natura penale e solo quando vi sia un *idem factum* – ma anzi, riconosce agli stati membri la facoltà di prevedere

comunque il doppio binario, penale ed amministrativo, per reprimere aspetti diversi di un medesimo fatto, quando «[…] tali procedimenti e sanzioni perseguano, ai fini del conseguimento di un simile obiettivo, scopi complementari riguardanti, eventualmente, aspetti diversi del medesimo comportamento illecito interessato, circostanza che spetta al Giudice del rinvio verificare».

Il doppio binario deve pur sempre garantire il rispetto del principio di proporzionalità ed assicurare che la severità dell'insieme delle sanzioni inflitte non ecceda la gravità del reato accertato.

A sostegno di tale tesi, tornando a riflettere sull'articolo 167, le modifiche introdotte (fattispecie specifiche e diminuzione di pena) sembrano da un lato salvare il doppio binario, e dall'altro scongiurare anche in questo caso il pericolo del *ne bis in idem* sostanziale e procedurale, nel rispetto del principio di proporzionalità.

Quel che è certo è che, nel caso di una violazione del GDPR o della normativa nazionale adottata in virtù dello stesso, potranno coesistere sanzioni amministrative e penali, ma non più sanzioni penali per lo stesso fatto, e comunque la combinazione tra sanzioni non dovrebbe comportare un effetto punitivo eccessivo, poiché in tali casi si andrebbe in contrasto con quanto previsto dall'articolo 50 della Carta UE.

Certo, un intervento diretto a dare maggiore univocità e chiarezza in *subiecta* materia, sarebbe da tutti auspicabile.

5. La tutela del dato personale e la responsabilità degli enti ex D.lgs. 231/2001

Il decreto legislativo 231/2001 introduce nel nostro ordinamento la responsabilità amministrativa degli enti dipendente da reato[93] e rappresenta un'innovazione legislativa particolarmente importante, poiché sancisce il superamento dell'anacronistico brocardo e dogma «*societas delinquere et*

[93]Art. 1 d.lgs. 231/2001: «Il presente decreto legislativo disciplina la responsabilità degli enti per gli illeciti amministrativi dipendenti da reato. Le disposizioni in esso previste si applicano agli enti forniti di personalità giuridica e alle società e associazioni anche prive di personalità giuridica. Non si applicano allo Stato, agli enti pubblici territoriali, agli altri enti pubblici non economici nonché agli enti che svolgono funzioni di rilievo costituzionale».

puniri non potest», privilegiando un'esigenza di razionalizzazione della normativa alla luce dell'esistenza di un'evidente potenzialità criminale delle persone giuridiche. La *societas* delinque eccome, non solo, espia.

L'ente è responsabile per i reati commessi, dai soggetti apicali o subordinati[94] solo se commessi nel suo interesse o a suo vantaggio[95].

Al fine di evitare una distorsione del principio del «*nulla poena sine culpa*» e di costruire un'inammissibile ipotesi di responsabilità oggettiva, è prevista necessariamente per la configurabilità della responsabilità dell'ente da illecito amministrativo dipendente da reato, la sussistenza della cosiddetta "colpa di organizzazione".

Il legislatore, orientato dalla consapevolezza delle connotazioni criminologiche degli illeciti ispirati da organizzazioni complesse, ha inteso imporre agli enti l'obbligo di adottare le cautele necessarie a prevenire la commissione di alcuni reati, adottando iniziative di carattere organizzativo e gestionale[96]. Tali accorgimenti vanno consacrati in un documento, un modello che individua i rischi e delinea le misure atte a contrastarli. Non aver

---

[94] Art. 5 comma 1 lett. a) e b) d.lgs. 231/2001: «Per soggetti apicali si intende: persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso. E per subordinati: persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui sopra».

[95] Art. 5 comma 2 d.lgs. 231/2001: «L'ente non risponde se i soggetti di cui sopra hanno agito nell'interesse esclusivo proprio o di terzi».

[96] Cfr. Art. 6 d.lgs 231/2001: «1.Se il reato è stato commesso dalle persone indicate nell'articolo 5, comma 1, lettera a), l'ente non risponde se prova che:

a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;

b) il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;

c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;

d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b).

2. In relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, i modelli di cui alla lettera a), del comma 1, devono rispondere alle seguenti esigenze:

a) individuare le attività nel cui ambito possono essere commessi reati;

b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;

c) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;

d) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;

e) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello».

ottemperato a tale obbligo fonda il rimprovero, la colpa d'organizzazione, e il riscontro di tale *deficit* organizzativo consente la piana ed agevole imputazione all'ente dell'illecito penale. Grava sull'accusa l'onere di dimostrare l'esistenza dell'illecito penale in capo alla persona fisica inserita nella compagine organizzativa della *societas* e che abbia agito nell'interesse di questa; tale accertata responsabilità si estende "per rimbalzo" dall'individuo all'ente collettivo, e diventa onere dell'ente provare, per contrastare gli elementi di accusa a suo carico, le condizioni liberatorie di segno contrario di cui all'articolo sei del decreto legislativo 231 del 2001.

Il modello richiede rispetto ai reati riconducibili alle figure apicali delle organizzazioni complesse, la creazione di un organismo interno di vigilanza, che si atteggia come uno strumento informativo e di controllo, con poteri propositivi e di accertamento disciplinare. Sul versante informativo gioca un ruolo decisivo il piano delle informazioni e delle comunicazioni verso l'organismo di vigilanza.

Si comprende pertanto come gli organismi di vigilanza e controllo, nell'espletamento delle sue funzioni, entri in contatto con una pluralità di dati personali, quali, in particolare, dati sensibili e dati giudiziari e ciò impone, conseguentemente, di procedere all'individuazione dei pertinenti profili connessi con il trattamento dei dati personali, ai sensi del decreto legislativo 30 giugno 2003, n. 196.

A tal proposito è opportuno osservare, facendo un breve excursus, come la legge 18 marzo 2008 n. 48 aveva introdotto nel catalogo dei reati presupposto del decreto legislativo 231/2001 (articolo 24 bis) diversi delitti informatici, successivamente il decreto legge 14 agosto 2013 n. 93 ha disposto un'ulteriore integrazione dell'articolo 24 bis inserendovi alcuni delitti contenuti nel codice *privacy*, nello specifico: illecito trattamento di dati personali (articolo 167), falsità nelle dichiarazioni e notificazioni al garante (articolo 168) e inosservanza di provvedimenti del garante (articolo 170).

La riforma aveva un notevole impatto sugli enti, in quanto questi, sulla base di quanto suddetto, per evitare di incorrere in responsabilità, avrebbero dovuto rispettare scrupolosamente i provvedimenti generali del Garante in

tema di trattamento dati del lavoratore, uso di internet e posta elettronica; con la conseguente adozione di modelli di organizzazione e gestione del trattamento dei dati personali e la designazione di un responsabile del trattamento che sarebbe diventato un interlocutore privilegiato dell'organismo di vigilanza[97].

La legge 15 ottobre 2015 n. 119 che ha convertito il predetto decreto, ha espunto il riferimento ai delitti in materia di *privacy*. La *ratio* di ciò si rinviene nel fatto che l'introduzione di tali delitti nel catalogo dei reati presupposto, diversamente dai reati di frode informatica e contraffazione delle carte di credito, avrebbe comportato per le aziende importanti e immediate conseguenze sotto il profilo operativo, soprattutto in relazione alla responsabilità amministrativa scaturente dall'illecito trattamento dei dati[98].

La corte di cassazione[99] ha infatti osservato come «mentre l'aggiunta nell'elenco dei reati che fanno insorgere la responsabilità amministrativa degli enti della frode informatica e dell'indebito utilizzo, falsificazione, alterazione e ricettazione di carte di credito o di pagamento, non ha particolare importanza in sede applicativa, il richiamo ai delitti previsti dal codice *privacy* risulta di grande impatto, soprattutto per la configurazione della responsabilità da reato degli enti per l'illecito trattamento dei dati, violazione potenzialmente in grado di interessare l'intera platea delle società commerciali e delle associazioni private soggette alle disposizioni del d.lgs. 231/2001».

Nonostante ciò, l'obiettivo di responsabilizzazione degli enti in relazione al corretto trattamento dei dati personali viene perseguito nel nuovo regolamento europeo.

Tale normativa non solo potrebbe portare a una riformulazione dei reati previsti dal codice *privacy* ed, eventualmente, alla loro introduzione nel catalogo dei reati presupposto del decreto legislativo 231, nonché alla creazione di nuove fattispecie penali in materia di trattamento dei dati personali, anche esse potenzialmente fonte di responsabilità amministrativa

[97] ARENA M., *I delitti in materia di privacy nel d.lgs. 231/2001*, in *Filodiritto*, 2013.
[98] IORIO A. *Privacy, responsabilità da 231*, in *Il sole 24 ore*, 2013.
[99] Cass. Pen. Relazione n. III/01/2013, 22 agosto 2013.

degli enti, ma da una parte, prescrive agli stati membri di presidiare il rispetto delle nuove norme sul trattamento dei dati personali mediante l'introduzione di sanzioni amministrative pecuniarie[100], dall'altra prevede esso stesso all'articolo 83, paragrafi 4 e 5, sanzioni amministrative pecuniarie direttamente applicabili ai titolari del trattamento che non dimostrino di aver adottato misure idonee prevenire la violazione delle norme in materia di trattamento dei dati, in base a un meccanismo del tutto simile a quello previsto dal d.lgs. 231/2001[101]. L'articolo 4 GDPR definisce violazione dei dati personali «la 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».

Nello specifico, il «*data breach*» può aver luogo in tre tipologie di eventi, ovvero in caso di «*confidentiality breach*» (divulgazione o accesso non autorizzato a dati personali), di «*availability breach*» (alterazione di dati personali) o di «*integrity breach*» (modifica di dati personali).

Dall'analisi di questa norma emerge un immediato ed evidente collegamento con l'articolo 24 bis, Decreto legislativo n. 231/2001, rubricato «delitti informatici e trattamento illecito di dati» in cui sono elencati i reati rilevanti di accesso abusivo ad un sistema informatico o telematico (articolo 615-ter c.p.), detenzione e diffusione abusiva di codici di accesso a sistemi informatici (articolo 615-quater c.p.), interruzione illecita di comunicazioni informatiche o telematiche (articolo 617-quater c.p.), danneggiamento di informazioni, dati e programmi informatici (articolo 635-bis c.p.), danneggiamento di sistemi informatici o telematici (articolo 635-quater c.p.).

Le fattispecie di reato sopra indicate attengono alla sfera della protezione dei dati in ambito aziendale e, secondo il Decreto legislativo 231/2001, possono determinare a carico dell'ente elevate sanzioni pecuniarie (sino ad €. 774.550,00) e, nelle ipotesi delittuose più gravi, anche interdittive dell'attività con confisca.

---

[100] Regolamento 679 *considerandum* n. 148.

[101] LAMANUZZI M. *Diritto penale e trattamento dei dati personali. Codice della privacy, novità introdotte dal regolamento UE 2016/679 e nuove responsabilità per gli enti*, in JusOnline, 2017.

Il regolamento prevede infatti una serie di obblighi a carico del titolare del trattamento dei dati che svolge attività di impresa in forma societaria; il *considerandum* n.74 stabilisce infatti che «il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure, le quali dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento nonché del rischio per i diritti e le libertà delle persone fisiche».

Anche ove il titolare del trattamento deleghi il trattamento a un responsabile, prevede il regolamento, questi deve presentare garanzie sufficienti, ed entrambi, dovrebbero tenere un registro delle attività di trattamento effettuate sotto la loro responsabilità, nonché valutare i rischi inerenti al trattamento e attuare misure per limitarli. Il tutto è perfettamente rispondente al principio di *accountability*, *fulcrum* del regolamento che comporta un notevole cambio culturale e di approccio, ossia il passaggio da una concezione meramente formale di adempimento a un approccio sostanziale di tutela dei dati e delle persone stesse.

Tali compiti vengono conferiti al titolare del trattamento (ente in questo caso) al fine di avere una sorta di rispondenza fiduciaria ed infatti, in caso di tradimento, accanto alle sanzioni pecuniarie e reputazionali, ne deriverebbe anche la rottura della relazione fiduciaria.

Il *GDPR*, come il Decreto legislativo 231/2001, spinge le imprese ad analizzare la loro organizzazione per individuare aree di rischio e conseguenti misure tecniche ed organizzative, che dovranno essere adottate obbligatoriamente per provare l'avvenuta responsabilizzazione con l'adeguamento della struttura aziendale alle norme.

Pertanto, le imprese sono chiamate a sviluppare e collaudare procedure e sistemi di corretta gestione dei dati, nonché di rilevazione delle irregolarità idonei a prevenire le violazioni della nuova normativa europea conservandone la documentazione relativa.

Resta da chiedersi se *l'onus probandi,* ai fini dell'accertamento della responsabilità amministrativa dell'ente per le violazioni del regolamento graverà sull'ente stesso o sull'autorità di controllo, ipotesi quest'ultima, preferibile se a tale responsabilità fossero estesi i principi costituzionali vigenti in materia penale, come è avvenuto per effetto di una pronuncia delle sezioni unite con riferimento alla responsabilità amministrative *ex* 231[102].

Il *GDPR* ha posto a carico delle imprese un onere di responsabilizzazione circa il trattamento dei dati, rendendo opportuna l'adozione del modello organizzativo, che consenta di mappare i rischi e, conseguentemente, di individuare misure di sicurezza e codici di condotta per affrontare i casi di violazione dei dati personali.

[102] Cass. Pen. Sez. Un. Thyssenkrupp, 18 settembre 2014 n. 38343. Le sezioni unite si sono soffermate sule condizioni di esonero da responsabilità previste dall'art. 6 d.lgs. 231 del 2001, che sembrano fondare una vera e propria presunzione di colpa in capo all'ente, chiamandolo a provare in giudizio di aver adottato tutte quelle misure organizzative e di prevenzione idonee a evitare la commissione di reati della specie di quello verificatosi in concreto. Sebbene la responsabilità dell'ente, a detta delle sezioni unite, abbia natura amministrativa, si tratta di una responsabilità scaturente da reato e da accertare nel processo penale con le garanzie che lo connotano, pertanto, alla stessa va esteso il principio costituzionale di presunzione di innocenza (art. 27, comma 2, cost), in base al quale è compito dell'accusa provare la fondatezza dell'ipotesi accusatoria e quindi, la sussistenza di tutti gli elementi costitutivi della fattispecie di responsabilità e non dell'imputato provare la loro assenza. Ne consegue che la lettura dell'art. 6 come fonte di inversione dell'*onus probandi* non merita di essere accolta in quanto contrasta con il dettato costituzionale, non risultando particolarmente persuasive le proposte avanzate in dottrina di qualificare tale norma in termini di scusante o di causa di non punibilità. DE VERO G., *La responsabilità penale delle persone giuridiche* in GROSSO C. F., PADOVANI T., PAGLIARO A., *Trattato di diritto penale*, Milano, 2008.

CONCLUSIONI

Le due più grandi sfide per la nostra società sono il riscaldamento globale e la sicurezza dello spazio digitale[1].

I dati sono la proiezione informatica della nostra vita reale.

L'entrata in vigore del regolamento europeo 2016/679/UE o *GDPR* – secondo l'acronimo inglese–, segna una pietra miliare nello sviluppo di un quadro regolatore armonizzato a livello europeo in uno dei settori più sensibili della tutela dei diritti umani, quella dei dati personali, diventati, nell'odierna società caratterizzata dallo sviluppo sfrenato delle tecnologie, oggetto di business – talvolta anche sregolato – e di ogni genere di manipolazioni.

Il diritto alla protezione dei dati personali, diritto distinto ed autonomo rispetto al diritto alla riservatezza e al diritto all'identità personale, venne introdotto *per tabulas* dal legislatore italiano, con l'emanazione del codice *privacy*, il quale si apre con la solenne dichiarazione del diritto di chiunque alla protezione dei dati che lo riguardano[2].

La protezione dei dati personali, può in senso lato, comprendere anche la *privacy*, ma ne presuppone un *quid pluris.* Si ritiene infatti che, il rapporto intercorrente tra le due nozioni sia di specialità bilaterale o reciproca, in quanto la *privacy* tutela la vita privata anche al di fuori del contesto del trattamento dei dati, la protezione dei dati invece, tutela la correttezza del trattamento dei dati stessi, anche a prescindere della sua incidenza sulla sfera privata dell'individuo[3].

La Corte di Giustizia dell'Unione Europea ebbe cura di precisare quanto fosse necessario mantenere distinte le due nozioni, inquadrando il diritto alla *privacy* come diritto ad avere uno spazio privato immune da ingerenze, mentre il diritto alla protezione dei dati personali come il diritto a un corretto trattamento dei propri dati personali, indipendentemente dal fatto che siano dati privati.

---

[1] Così SORO A., intervista a La Stampa.

[2] L'articolo 1 codice *privacy* riproduce esattamente la disposizione contenuta nell'articolo 8 della Carta di Nizza.

[3] LAMANUZZI M. *Diritto penale e trattamento dei dati personali. Codice della privacy, novità introdotte dal regolamento UE 2016/679 e nuove responsabilità per gli enti*.

È lecito pertanto affermare che, il *discrimen* tra le due nozioni si rinviene nel bene oggetto di tutela, la sfera privata, che ha una portata esclusivamente individualistica, nel diritto alla *privacy* e l'interesse generale alla correttezza e liceità del trattamento dei dati, nel diritto alla protezione dei dati personali, che ha la duplice natura di diritto dell'individuo e interesse della collettività[4].
La salvaguardia dell'autodeterminazione informativa, il cui controllo gradua o addirittura impedisce l'invadenza degli altri nella propria sfera privata, articolata non soltanto nei vari istituti del consenso informato, ma anche nella valutazione di impatto *privacy*, è presidio essenziale per mantenere il governo sulle nostre tracce digitali, che più di ogni altro aspetto concorrono oggi a definire la nostra identità e, con essa, la nostra libertà.
Ogni violazione può avere conseguenze concrete: da un'esposizione non desiderata della nostra persona fino alla salute se, si supponga, i dati manipolati sono quelli di una cartella clinica, perché l'attacco è stato rivolto a un'azienda sanitaria.
La capacità di proteggere i dati personali dovrebbe rappresentare non tanto e non solo un obbligo giuridico quanto, piuttosto, un requisito preferenziale, un *asset* competitivo.
In questo mondo iper-connesso, caratterizzato da un'economia fondata sui dati e alimentata dall'intelligenza artificiale, i cittadini mostrano di preoccuparsi sempre di più del loro "corpo elettronico", di una esistenza sempre più affidata alla dimensione astratta del trattamento elettronico delle loro informazioni, «nella società digitale, noi siamo i nostri dati», asseriva il Professor Rodotà, «nel passaggio dall'*habeas corpus* all'*habeas data*[5] o più specificamente all' "*habeas corpus* in chiave digitale", il denominatore comune rimane il controllo, controllo sul proprio corpo, nel primo caso, controllo sui propri dati, nel secondo».
Facendo un salto a piè pari su tutta l'evoluzione dottrinaria e giurisprudenziale, è interessante osservare come la consapevolezza del valore dei propri dati costituisca il *leitmotiv* del *GDPR.*

[4] LAMANUZZI M. *Diritto penale e trattamento dei dati personali. Codice della privacy, novità introdotte dal regolamento UE 2016/679 e nuove responsabilità per gli enti*.
[5] RODOTÀ S., *Il mondo nella rete.* Quali i diritti, quali i vincoli, Roma – Bari, 2014

Il quadro normativo non si è cristallizzato nelle sole norme comunitarie, poiché anche l'Italia si è adeguata al regolamento europeo che detta nuove norme precise sulla *privacy* dei cittadini europei. Il *General data protection regulation* è stato quindi armonizzato nel nostro Paese con il decreto n.101 del 10 agosto 2018.

Se "protezione dei dati" è formula che riassume ed unifica tutte le regole sul trattamento dei dati, merita sottolineare che al termine "diritto", deve essere riconosciuto un ruolo fondante la situazione del soggetto rispetto all'attività di trattamento, nella consapevolezza che il rispetto delle regole contenute nel Codice rappresenta l'aggiornata espressione della libertà del soggetto in una società nella quale il trattamento dei dati personali assume una dimensione e un'intensità tali da non poter più essere ignorate.

Nulla quaestio sulla nebulosità che spesso attornia la protezione dei dati personali, ma ciò non deve stupire, in quanto si tratta di un concetto, e conseguentemente di un diritto, ancora fortemente in evoluzione e in corso di definizione[6] e bisogna riportare alla memoria che «i diritti umani sono diritti storici, cioè nati in certe circostanze, [...] gradualmente, non tutti in una volta e non una volta per sempre»[7].

Stante la mutevolezza e la dinamicità di *subiecta* materia, la *ratio* ispiratrice del *GDPR* si rinviene nel tentativo di dare all'Europa, ai suoi Stati e ai suoi cittadini, una normativa comune sul trattamento dei dati personali dei cittadini stessi, anche alla luce dell'innovazione tecnologica ed economica degli ultimi anni.

Il Regolamento nasce con l'obiettivo dichiarato di sviluppare uno spazio di libertà, sicurezza e giustizia, ma anche di realizzare un «clima di fiducia per lo sviluppo dell'economia digitale in tutto il mercato interno», promuovendo «la certezza giuridica e operativa tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche».

Questo stretto rapporto è, del resto, il riflesso della centralità della protezione dei dati nell'economia e nella società digitale, nelle quali si sono aperte sfide

[6] FINOCCHIARO G., prefazione in NIGER S., *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006.
[7] BOBBIO N. *L'età dei diritti,* Torino, 1990

sempre nuove per la sicurezza dei dati, sia per le imprese sia per le Pubbliche amministrazioni.

In Italia le sanzioni penali continuano – e probabilmente continueranno – ad avere un ruolo fondamentale per la salvaguardia del diritto alla protezione dei dati personali. Ciò è stato confermato dalla scelta operata dal nostro legislatore con il decreto di adeguamento al *GDPR*, che ha modificato l'arsenale sanzionatorio delineato dal previgente Codice *privacy*, lasciando però sostanzialmente inalterate svariate fattispecie incriminatrici ed introducendone di nuove.

Verrebbe da chiedersi, allora, come sia possibile che, secondo uno studio presentato da *Accenture*, l'Italia è tra i dieci Paesi al mondo più colpiti dai crimini informatici. Nell'ultimo anno, i costi del *cybercrime* sono cresciuti del 23% rispetto all'anno precedente.

Il diritto alla protezione dei dati dovrebbe essere posto al centro dell'agenda politica, nella consapevolezza che su di esso si misura la qualità della democrazia e da esso dipende la nostra libertà. Sulla protezione dati non può valere il paradigma del *nimby* (*not in my backyard*), ovvero l'attenzione a tale diritto solo quando ci riguardi (come Paese, come individui) in prima persona[8].

La disciplina è ineccepibile, ma la legge e la sola repressione sono insufficienti.

Non sempre l'apparato sanzionatorio previsto dalla legge garantisce la reale protezione degli interessi tutelati. Talvolta è necessario ricorrere a strumenti alternativi rispetto ai classici meccanismi predisposti dal legislatore. Occorre saper modulare le misure sanzionatorie in modo da consentire una piena ed effettiva tutela degli interessi in gioco.

L'autodisciplina può essere un aiuto per sciogliere questo nodo gordiano.

È vero che nella normativa sulla protezione dei dati personali il testo base è rappresentato da un Regolamento europeo, ma spesso sono le disposizioni attuative – nazionali – a fare la differenza.

[8] Così SORO A., intervista a La Stampa.

L'Italia ha una forte storia in questa materia e dovrebbe tentare di creare un *Made in Italy* nel settore della protezione dei dati, e nell'instaurare una cultura della protezione dei dati, le istituzioni hanno un ruolo fondamentale. «Etica, *accountability*, effettività ed efficacia: la rosa dei venti del *GDPR*»[9]. Il nuovo Regolamento europeo costituisce cornice normativa di una sfida epocale, ma ciò non basta, in quanto, più di ogni altra misura, quello che serve per garantire l'effettività dei diritti sanciti dal Regolamento è il promovimento di quella cultura della *privacy* e con essa del dato personale, la cui diffusione costituisce la *condicio sine qua non* al vero riconoscimento del legame profondo tra libertà, dignità e *privacy*, da sempre professato e ribadito dal Professor Rodotà.

Il *GDPR* è stata un'evoluzione o un'occasione persa? È ancora presto per dare una risposta certa. L'evoluzione e i risultati dell'applicazione della normativa sotto i diversi profili coinvolti, civile, penale ed amministrativo, serviranno a offrire il responso inconfutabile al predetto interrogativo.

[9] BUTTARELLI G., Roma, 2019.

BIBLIOGRAFIA

ACCIAI R., *Le nuove norme in materia di privacy*, Santarcangelo di Romagna, 2003, p. 77.

ALPA G., *La normativa sui dati personali. Modelli di lettura e problemi esegetici*, in Dir. Inf., 1997, pag. 705.

ANGIONI, *Condizioni di punibilità e principio di colpevolezza, i*n Riv. It. Dir. Proc. Pen., 1989, p. 733.

ARISTOTELE, *La politica*, Firenze, 1981.

AULETTA T. A., *Riservatezza e tutela della personalità*, Milano, 1978, pp. 42-43.

BELLOCCI M., MAGNANENSI S., PASSAGLIA P., RISPOLI E., (a cura di), *Tutela della vita privata: realtà e prospettive costituzionali*, Quaderno predisposto in occasione dell'incontro trilaterale delle Corti costituzioni spagnola, portoghese e italiana, Lisbona, 1–4 ottobre 2006.

BELVEDERE A., *Riservatezza e strumenti d'informazione,* in *Dizionario del dir. priv.*, Milano, 1980.

BENDICH A., P*rivacy, Poverty, and the Constitution, Berkeley*, 1966.

BERGHELLA R., BLAIOTTA P., Diritto penale dell'informatica e beni giuridici, in Cassazione Penale, 1995, 7, 1463

BLAIOTTA R., *Le fattispecie penali introdotte dalla legge sulla privacy*, in Cass. Pen., 1999, p. 806.

BOLOGNINI L. PELINO E., *Codice privacy: tutte le novità del d.lgs. 101/2018*, Milano, 2019.

BOLOGNINI L., BISTOLFI C., PELINO E., *Il regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016

BRICOLA F., *Prospettive e limiti della tutela penale della riservatezza,* in AAVV, *Il diritto alla riservatezza e la sua tutela penale,* Milano, 1970.

BUSIA G., voce *Diritto alla riservatezza,* in *Digesto Disc. Pubbl*., Torino, 2000.

BUTTARELLI G. *Banche dati e tutela della riservatezza: la privacy nella società dell'informazione*, Milano, 1997

CALAMANDREI P., *L'avvenire dei diritti di libertà*, Introduzione di RUFFINI F., *Diritti di libertà,* Firenze, 1946

CARNELUTTI F., *Diritto alla vita privata, in Riv. Trim. dir. Proc*., 1995.

CASETTA E., *Sanzione amministrativa*, in Dig. Disc. Pubbl, Torino, 1994, p. 599.

CATAUDELLA A., *Scritti giuridici*, Padova, 1991, p. 545.

CAUTADELLA S., *Accesso ai dati personali, riserbo e controllo sull'attività di lavoro*, in *Arg. Dir. Lav*. 2001, n.1;

CHIECO P., *Privacy e lavoro. La disciplina dei dati personali del lavoratore*, Bari, 2000;

CHINÈ G., La tutela penale della privacy, in *Il trattamento dei dati personali*, vol. II, CUFFARO V. RICCIUTO V., (a cura di), Torino, 1999, p. 490.

CIRILLO G. P. *La tutela della privacy nel sistema del nuovo codice sulla protezione dei dati personali,* Padova, 2004.

CORASANITI G., *Sanzioni penali e depenalizzazione degli illeciti nella normativa a tutela dei dati personali*, in Danno e responsabilità, 2002.

CORRIAS LUCENTE G. *La nuova normativa penale a tutela dei dati personali* in *Il codice dei dati personali temi e problemi,* CARDARELLI F., SICA S., ZENO ZENCOVICH V., Milano, 2004.

CORRIAS LUCENTE G. *Sanzioni* in GIANNANTONIO E., LOSANO M. ZENO ZENCOVICH V. (a cura di) *La tutela dei dati personali commentario alla l 675/96,* Padova, 1999.

CORRIAS LUCENTE G., *Il codice dei dati personali. Temi e problemi* (a cura di) CARDARELLI F., SICA S., ZENO ZENCOVICH V., Milano, 2004.

CUFFARO V., D'ORAZIO R., RICCIUTO V., *Il codice del trattamento dei dati personali*, Torino, 2007.

DE VERO G., *La responsabilità penale delle persone giuridiche* in GROSSO C. F., PADOVANI T., PAGLIARO A., *Trattato di diritto penale*, Milano, 2008.

DI CIOMMO F., *Il Diritto dell'informazione e dell'informatica*, Milano, 2010 pp. 850 e ss.

FOIS S., *Questioni sul fondamento costituzionale del diritto alla «identità personale»*, in AAVV, *L'informazione e i diritti della persona*, Jovene, Napoli, 1983, pp. 159 ss.

FORNASARI G., *Il ruolo della esigibilità nella definizione della responsabilità penale del* provider, in PICOTTI L. (a cura di), *Il diritto penale dell'informatica nell'epoca di* internet, Padova, 2004, p. 431.

FROSINI voce *telematica e informatica giuridica* in Enc dir vol XLIV, Milano 1992 p. 66.

GALOPPI, Aa Vv., Codice della privacy, 2004, Tomo II, p.2111.

GATES B. *The road ahead* 1995.

HUSTINX P. *The European Approach: Regulation through Protection Authorities*, 8 november 2005, speech at the colloquium Information technologies: servitude or liberty? Paris, 2005.

ICHINO P., *Diritto alla riservatezza e diritto al segreto nel rapporto di lavoro*, Milano, 1979

ICHINO P., *Il contratto di lavoro, vol III, Trattato di diritto civile e commerciale* Milano 2003, pag 217 ss;

IMPERIALI R., *Codice della Privacy*, Milano, 2005.

INGRASSIA A, *Il ruolo dell'internet service provider,* in Giur. Merito, 2004.

LAMANUZZI M. *Diritto penale e trattamento dei dati personali. Codice della privacy, novità introdotte dal regolamento UE 2016/679 e nuove responsabilità per gli enti*, in JusOnline, 2017.

LOTIERZO R. *Del nocumento nell'illecito trattamento dei dati personali ovvero dell'esigenza di ascendere alle origini di una incriminazione,* in Cass Pen., n. 4/2013, p. 1589.

MANNA A. *Beni della personalità e limiti della protezione penale*, Padova 1989.

MANNA A., *Il quadro sanzionatorio ed amministrativo del codice sul trattamento dei dati personali*, Dir. Inf. 2003.

MANNA A., *Il quadro sanzionatorio penale ed amministrativo del codice sul trattamento dei dati personali,* in Il diritto dell'informazione e dell'informatica, 2003, n. 4-5.

MANNA A., *Il quadro sanzionatorio penale ed amministrativo del codice sul trattamento dei dati personali,* in *Il diritto dell'informazione e dell'informatica,* 2003, 4-5, 727

MANNA A., *La protezione personale dei dati personali nell'ordinamento italiano,* in *Rivista trimestrale di diritto penale dell'economia,* 1993.

MANTOVANI F. *Brevi note a proposito della nuova legge sulla criminalità informatica* in Critica del diritto, 1994 IV.

MANTOVANI F., *Diritto alla riservatezza e libertà di manifestazione del pensiero con riguardo alla pubblicità dei fatti criminosi*, in AAVV, *Il diritto alla riservatezza e la sua tutela penale*, Milano, 1970.

MANTOVANI F., *Diritto Penale – Parte Speciale, delitti contro la persona*, Padova, 2012

MANTOVANI F., *Diritto penale*, Padova, 1992, pp 814-815.

MANTOVANI F., *Diritto penale. Parte speciale I. Delitti contro la persona,* Padova, 2011

MANTOVANI F.., *Diritto alla riservatezza e libertà di manifestazione del pensiero con riguardo alla pubblicità dei fatti criminosi*, in AAVV, *Il diritto alla riservatezza e la sua tutela penale*, Milano, 1970

MANTOVANI M., *Le fattispecie penali della legge n. 675/96 e le posizioni di garanzia*, in Dir. Inf. 2000, pp. 567-595.

MARTINOTTI G. *La difesa della privacy*, *Politica del diritto*, Bologna, 1971

MASLOW A., *Motivazione e personalità*, Roma, 2010.

MESSINETTI D. in *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali* in Enc. Dir., Milano, 1983.

MILITELLO V., *Nuove esigenze di tutela penale e trattamento elettronico delle informazioni*, in *Rivista trimestrale di diritto penale dell'economia,* 1992, 3, 374

MIRABELLI V., *Identità personale e dato personale*, in CUFFARO V., RICCIUTO V. (a cura di), Il trattamento dei dati personali, Torino, 1997.

MONDUCCI J. SARTOR G. *Il codice in materia dei dati personali*, Padova, 2004.

MORSILLO G., *La tutela penale del diritto alla riservatezza*, Milano, 1966, p. 274.

MUCCIARELLI F, *Informatica e tutela penale della riservatezza* in *Il diritto penale dell'informatica nell'epoca di internet*, PICOTTI L. Padova, 2004.

MUMFORD L., *La cultura delle città,* Torino, 2007.

NEGROPONTE N. *Being digital*, 1995

NIGER S., *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006.

ORLANDI, *Gli adempimenti per i titolari dei trattamenti,* in SICA- STANZIONE (a cura di), *La nuova disciplina della privacy,* Bologna- Roma, 2004, p. 183.

PAGLIARO A., *Bene giuridico e interpretazione della legge penale,* in *Studi in onore di Francesco Antolisei,* Volume II, Milano, 1965

PAGLIARO S. *Informatica e crimine organizzato* in Ind Pen 1990 p 414 ss.

PALAMARA L., *Note in tema di rilevanza penale del trattamento illecito di dati personali*.

PALAZZO F. C. *Bene giuridico e tipi di sanzione,* in *Indice Penale,* 1992, 1, 213

PALAZZO F. C. *Sulle funzioni delle norme definitorie*, in AA. VV., *Omnis definitio in iure periculosa? Il Problema delle definizioni legali nel diritto penale*. CADOPPI A. (studi coordinati da), Padova, 1996.

PALAZZO F. C., Considerazioni in tema di tutela della riservatezza, in Rivista italiana di diritto e procedura penale, 1975.

PALAZZO F. C., *Il principio di determinatezza nel diritto penale*, Milano, 1979.

PALAZZO F., *Considerazioni in tema di tutela della riservatezza*, in Riv. Trim. dir. e proc. pen, 1975 pp. 126.

PANETTA R., *Libera circolazione e protezione dei dati personali*, Milano, 2006.

PARDOLESI R., (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003

PARDOLESI R., *Un bilancio interlocutorio e le prospettive sulla legge Privacy*, Roma, 1998.

PARODOLESI R. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003.

PATRONO P. *Privacy e vita privata* (diritto penale), in Enc Dir XXXV, Milano 1986. P. 557.

PETRONE M. *Banche dati e tutela della privacy*. *Riflessi penalistici* in Dir Inf, 1988 p. 82.

PEZZELLA Giurisprudenza di merito 2010 p. 2232

PICOTTI L., *Profili di diritto penale sostanziale*, in *La ratifica della Convenzione sul Cybercrime del Consiglio d'Europa*, in *Diritto penale e processo*, 2008, 3, 710

PICOTTI L.,*Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004

PITT W., The Elder Lord Chattam, discorso del marzo 1763, citato in BROUGHAM H.P. *Historical Sketches of Statesmen Who Flourished in the Time of George III*, Charles Knight e Co., Londra, 1839, vol. I. 52.

PIZZORUSSO A., *I profili costituzionali di un nuovo diritto della persona*, in AAVV, *Il diritto alla identità personale*, 1980.

PIZZORUSSO A., *Sul diritto alla riservatezza nella Costituzione italiana*, in *Prassi e Teoria*, 1976

PULITANÒ P., *La responsabilità da "reato" degli enti: i criteri d'imputazione*, in *Rivista italiana di diritto e procedura penale*, 2002, 3, 420

RAMACCI F., *Corso di diritto penale*, Torino, 1991, vol. I, p. 72.

RAMACCI L., *Diritto penale dell'ambiente,* Padova, 2009

RAVÀ, *Istituzioni di diritto privato*, Padova, 1934

RICCIO G. M. SCORZA G. BELISARIO E., *GDPR e normativa privacy*, Milano, 2018

RODOTÀ S. *Tecnologie e diritti*, Bologna, 1995.

RODOTÀ S., *Il mondo nella rete.* Quali i diritti, quali i vincoli, Roma – Bari, 2014

RODOTÀ S., *in Intervista su Privacy e Libertà*, Bari, 2005.

RODOTÀ S., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in Riv. Crit. Dir. Priv., 1997, p. 558.

RODOTÀ S., *Tecnologie e diritti*, Bologna 1995.

RONCO M., *Vita privata (interferenze illecite nella)*, in *Novis, Digesto It.*,VII, Torino, 1987, 163

SANDULLI A. M.- BALDASSARRE A. *Profili costituzionali della statistica in Italia*, in *Dir. soc*., 1973

SCALISI A., Il diritto alla riservatezza, Milano, 2002, p. 511;

SGUBBI F. *Profili penalistici in Riv Trim dir e proc civ*, 1998 II pp. 753 ss.

SICA S.., *Danno e nocumento nell'illecito trattamento di dati personali,* in *Il diritto dell'informazione e dell'informatica*, 2004, 4-5, 714

SILEONI S., *Autori delle proprie regole. I codici di condotta per il trattamento dei dati personali e il sistema delle fonti*, Padova, 2011

SIMITIS S., *Il contesto giuridico e politico della tutela della privacy*, in Rivista critica del diritto privato, Bologna, 1997.

SOFOCLE, *Edipo re – Edipo a Colono – Antigone*, a cura di Dario Del Corno, Oscar Mondadori, 2006.

SPAGNOLETTI, *La responsabilità del provider per i contenuti illeciti di internet*, in Giur. Merito, 2004.

TORRE V. *La gestione del rischio nella disciplina del trattamento dei dati personali*, pp. 238 ss, in PICOTTI L., *Il diritto penale dell'informatica nell'epoca di internet,* Padova, 2004.

TRONCONE P. *Il caso google e non solo,* nota a Cassazione penale, sez. III, sentenza 03/02/2014, n. 5107

VANNINI *La criminalità informatica: le tipologie di compter crimes di cui alla l. n. 547/93 dirette alla tutela della riservatezza e del segreto* in Riv. Trim. dir. Pen. economia, 1994 p. 427.

VENEZIANI P., in *I beni giuridici tutelati dalle norme penali in materia di riservatezza informatica e disciplina dei dati personali,* tratto da *Il diritto penale dell'informatica nell'epoca di internet,* a cura di PICOTTI L., Padova, 2004

VILLANI C. *Il codice del trattamento dei dati personali,* a cura di CUFFARIO, D'ORAZIO, RICCIUTO, Torino, 2006

VOLTA *La tutela penale del diritto alla riservatezza, art 615 bis cp: esegesi della norma* in Riv. Pen. 1989 pp. 535.

WARREN S. D. E BRANDEIS L. D., *The Right to privacy. The implicit made explicit*, in *Harward Law Review*, 1890.

ZANGONI, *sulla tutela penale del diritto alla riservatezza* ivi 1982 pp 971 *Banche dati, telematica e diritti della persona,* (a cura di), ALPA G., BESSONE M., Padova 1984.

ZATTI P., *Il diritto alla identità e l'"applicazione diretta" dell'art. 2 Cost.*, in AAVV, *Il diritto alla identità personale*, a cura di ALPA G. e BESSONE M., Padova, 1981, pp. 55 ss.

ZENO ZENCHOVICH V., *"Personalità (diritti della)"*, in *Digesto delle discipline penalistiche*, 1995

ZOTTA D., *Le sanzioni* in CLEMENTE A. (a cura di) Privacy, Padova, 1999.