Dipartimento di Giurisprudenza

Cattedra di Diritto penale 2

LA TUTELA PENALE DEL DATO PERSONALE

RELATORE
Chiar.mo Prof.
Maurizio Bellacosa

CANDIDATO
Giovanni Tomasello
Matr. 153103

CORRELATORE
Chiar.ma Prof.
Maria Novella Masullo

Anno Accademico 2021/2022

INDICE

CAPITOLO II

LA TUTELA PENALE DEL DATO PERSONALE: DAL D.LGS. N. 101/2018 AL D. LGS N. 139/2021

CAPITOLO III

NUOVE FATTISPECIE INCRIMINATRICI DEL CODICE DELLA PRIVACY

INTRODUZIONE

Il presente elaborato mira ad approfondire la tematica della tutela penale del dato personale in un'epoca storica caratterizzata dalla crescita esponenziale dei trattamenti effettuati con strumenti informatici per la quale è nata l'esigenza di apprestare una maggiore tutela e protezione dei diritti fondamentali della persona, sia nell'ordinamento giuridico italiano sia in quello europeo anche con particolare riguardo ai trattamenti di dati personali su larga scala.

Nel primo capitolo attraverso un breve *excursus* storico verrà analizzata l'evoluzione del concetto di *privacy* partendo dal contesto storico- culturale dell'antica Grecia. Nel periodo della *polis* greca esisteva la distinzione tra vita privata e pubblica, quest'ultima era maggiormente esaltata e riservata alle persone istruite. Dovere assoluto, per il cittadino greco, era quello di partecipare attivamente alla vita pubblica della Polis, riconoscendo però allo stesso anche un ambito intimo che, però, si limitava strettamente al compimento dei propri bisogni e delle proprie necessità[1] e si poneva all'ombra del *Bios politikos*[2] che, invece, assorbiva la quasi totalità della sfera di vita del cittadino. Secondo tale prospettiva, la partecipazione attiva alla vita democratica della città si inquadrava come dovere imprescindibile del cittadino, mentre la vita privata era considerata come fine a sé stessa e pertanto ignorata. Lo stesso Aristotele definiva l'uomo come un "animale sociale-politico",[3] che necessitava di scambi sociali e culturali, poiché chi viveva maggiormente nel privato era considerato *extra societatem.*

---

[1] ARENDT H., *Vita activa. La condizione umana*, trad. it. di DAL LAGO A., Milano, 2001, 19. IGER S., *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006, XI.

[2] Concetto greco risalente agli antichi Pitagorici e successivamente ripreso da Aristotele, il vivere politico dell'uomo, inteso come uomo libero, si fonda sull'azione, *praxis*, e sul discorso, *lexis*, da cui non può che trarre origine il dominio degli affari umani.

[3] Concetto di *"politikòn zôon"* di Aristotele espresso nel trattato Politica, traduzione a cura di Federico Ferri, Bompiani editore Milano, 2016

Ancora durante il medioevo e in particolare nel feudalesimo, il concetto di privacy era completamente compresso a favore di una vita familiare basata su rapporti personali e di fiducia reciproca, senza spazio per l'individualità.[4] Ogni casa e ogni famiglia, diveniva a quel tempo una piccola società, una piccola polis, in cui la vita si estrinsecava quotidianamente come vita pubblica, cui ogni soggetto doveva attivamente partecipare ed in merito alla quale, giova ribadire, l'individualità era bandita.[5]

Nei secoli XVIII e XIX si cominciò ad intravedere l'inizio dell'importanza giuridica della tutela della sfera privata di ogni individuo come diritto inviolabile ed irrevocabile.

Nel 1890 Samuel. D. Warren e Louis. D. Brandeis, due studiosi e giuristi statunitensi pubblicarono sul Harward Law Review, un saggio dal titolo "*The Right to Privacy".* Il saggio in argomento nacque in relazione ad una vicenda strettamente personale di uno dei due autori del saggio, in particolare riguardava la vita matrimoniale e il divorzio di Samuel Warren, che fu resa pubblica su tutti i giornali e tale circostanza condizionò non poco la reputazione dei protagonisti. Da qui la necessità di creare un vero e proprio nuovo diritto della persona (*Right to privacy)* definito come "*right to be let alone*" sviluppatosi in virtù dei cambiamenti politici, sociali ed economici della società americana di fine secolo. I due giovani famosi avvocati sottolinearono l'importanza del mutamento tecnologico che gradualmente la società stava subendo e quindi l'urgente necessità di elaborare una normativa più specifica e attenta ai diritti del singolo.

I già menzionati giuristi parlavano di tutela dei pensieri, intesi come idee, opinioni personali, sentimenti ed emozioni strettamente personali.[6]

Warren e Brandeis asserirono che si trattava di un concetto rintracciabile all'interno dell'area privata del singolo, inteso come quello spazio domestico in cui rifugiarsi, ossia un posto sicuro da ingerenze esterne introducendo, così un rivoluzionario diritto alla riservatezza.

---

[4] FABRIS F., *Il diritto alla privacy*, cit., 95.
[5] DUBY G., *Potere privato, potere pubblico*, in ARIES P., DUBY G (a cura di), *La vita privata*, vol. II, RomaBari, 2001, 10.
[6] FABRIS F., *Il diritto alla privacy*, cit., 96.

Ciò comportò un cambiamento dalle logiche materialistiche alla dignità personale e alla protezione dell'inviolabilità personale come valore supremo, prima ancora del valore preminente della proprietà privata.

In questo senso il diritto alla *privacy* sebbene nasca nell'epoca borghese, si origina come un diritto dei ricchi e degli aristocratici, soltanto in seguito il diritto alla riservatezza si evolverà ulteriormente ad un livello successivo, così da spezzare nuovamente quelle catene e consentire progressivamente il raggiungimento di un nuovo e più ampio livello di tutela riconosciuto a tutti gli esseri umani e non soltanto appannaggio di pochi.

Il Codice privacy garantisce, infatti, il diritto alla protezione dei dati personali, ossia che il trattamento dei dati avvenga conformemente alle norme. Questo diritto, chiamato "*data protection*", è diventato importante a causa della sempre maggiore quantità di informazioni personali presenti nel mondo digitale, realizzando un passaggio dall'Habeas Corpus, che garantisce il controllo sul proprio corpo, all'habeas data, che garantisce il controllo sui propri dati, consentendo una autodeterminazione ed un controllo informativo. Il concetto di privacy si arricchisce dunque di contenuti ulteriori, fino ad assumere un'accezione positiva, quale controllo sulle proprie informazioni.[7]

Inoltre, la privacy è anche vista come il diritto dell'individuo a determinare liberamente le proprie scelte personali. Per un corretto inquadramento giuridico del tema saranno esaminati gli articoli della Costituzione italiana alla ricerca del fondamento del diritto alla riservatezza, all'identità personale e alla libertà di pensiero. Ciò che sarà oggetto di maggiore indagine è senz'altro l'evoluzione del diritto alla riservatezza che inizialmente intorno agli anni settanta era inteso come rispetto della vita privata, successivamente, intorno agli anni novanta se ne inizia a parlare come diritto al controllo dei propri dati personali.

A tal proposito sarà approfondita l'evoluzione di tale normativa sia a livello europeo che nazionale.

---

[7] S. RODOTÀ, *Repertorio di fine secolo*, Bari-Roma, 1992, p. 190.

La disamina della normativa si concentrerà in particolare sul Regolamento UE 2016/679 (di seguito, per brevità, GDPR), emanato con l'obiettivo di aggiornare la normativa in merito alle innumerevoli innovazioni tecnologiche che sono intervenute e che ormai sono alla base del nostro vivere quotidiano. Il D.lgs.196/2003 comunemente conosciuto come Codice della *privacy* (di seguito, per semplicità, il "Codice") recentemente revisionato – ad opera del D. lgs n. 101/2018 – per adeguare le sue disposizioni a quelle del GDPR, ed un ultimo aggiornamento al testo si deve anche al Decreto Legge n. 139/2021 (c.d. Decreto Capienze), convertito con modificazioni dalla Legge n. 205/2021. L'analisi di tale evoluzione normativa in materia di trattamento dei dati personali comporterà un assetto normativo più aderente alle esigenze della mutata società. Saranno dunque esaminate le diverse tipologie di dati personali, come espressamente disciplinati dal nuovo GDPR, affinché possano essere messi in evidenza gli obiettivi di conservazione e circolazione secondo liceità e trasparenza che la normativa si prefigge di raggiungere.

Nel secondo capitolo verranno analizzati innanzitutto i soggetti attivi operanti all'interno del trattamento dei dati personali che sono in particolare, il Titolare, il Responsabile, l'incaricato, il DPO (Data Protection Officer) ed il Garante, ciascuno con le loro competenze che consistono nella raccolta, nella gestione, nella comunicazione e nella conservazione dei dati dell'interessato chiamato anche soggetto passivo, ossia colui a cui i dati personali si riferiscono. Il titolare del trattamento dei dati è considerato il fulcro attorno al quale orbitano le scelte in relazione alle finalità da perseguire nel trattamento. La figura del titolare può essere rivestita da una persona fisica, una persona giuridica o un'autorità pubblica, la quale ha l'obbligo giuridico di attuare un'attività che garantisca mediante una dimostrazione, che il trattamento dei dati sia stato eseguito in totale conformità alle disposizioni del Regolamento e alle disposizioni nazionali.

Il titolare, inoltre, può decidere di nominare un Responsabile che consiste in un'altra figura del trattamento dei dati, mediante il quale per suo conto si occupi degli adempimenti in materia di privacy. Il Responsabile del trattamento deve fornire garanzie sufficienti per mettere in atto misure

tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

Altra figura di rilievo è il responsabile della protezione dei dati (Data Protection Officer" DPO). Secondo l'art.37 del Regolamento UE n.679 del 2016 il titolare del trattamento e il responsabile del trattamento designano un responsabile della protezione dei dati nel caso in cui il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali.

Il diritto alla privacy è più ampio e comprende il controllo delle informazioni personali e la scelta su cosa condividere o meno con terze parti. La protezione dei dati personali, che include la privacy, riguarda la protezione di qualsiasi informazione che riguardi o possa riguardare una persona identificabile.

Il diritto alla privacy tutela la vita privata in modo esclusivamente soggettivo, mentre il diritto alla protezione dei dati personali riguarda la correttezza e la liceità del trattamento dei dati personali, avendo una natura sia soggettiva che collettiva.

Il diritto alla protezione dei dati personali inizia, così a trovare una più precisa e unitaria forma di regolamentazione nella Direttiva europea 95/46/CE, del 24 ottobre 1995 (definita anche "Direttiva madre"), emanata dal Parlamento e dal Consiglio dell'Unione Europea con la finalità di tutelare le persone fisiche in ordine ad un corretto trattamento dei dati personali ed alla relativa libera circolazione di detti dati. Inoltre, la Direttiva mira ad uniformare le legislazioni nazionali dei singoli Stati aderenti all'Unione, in considerazione del fatto che sono i sistemi di trattamento dei dati personali ad essere al servizio della persona umana, della quale devono necessariamente essere rispettate le libertà ed i diritti fondamentali.

Il legislatore europeo ha dato autonomia ai legislatori nazionali per creare la propria normativa in materia di protezione dei dati personali.

Inoltre, nel secondo capitolo verranno evidenziate le ulteriori integrazioni effettuate dal D.lgs. n. 101/2018 insieme al D.L. n. 139/2021 c.d. Decreto Capienze relativamente al sistema sanzionatorio.

Il sistema sanzionatorio novellato ha l'obiettivo di creare una proporzionalità tra l'entità dell'illecito e la relativa sanzione da applicare.

In tale prospettiva il legislatore europeo non ha previsto il minimo edittale della pena stabilendo che il grado di intensità afflittiva andasse valutato volta per volta.

Nel terzo capitolo invece, saranno analizzate le nuove fattispecie penali riguardanti il trattamento dei dati personali su larga scala e in particolare gli articoli 167 *bis* e 167 *ter* del Codice, riguardanti la comunicazione, la diffusione e l'acquisizione illecita di dati personali. L'articolo 167-bis del Decreto Legislativo 96/2003, meglio conosciuto come Codice in materia di protezione dei dati personali, stabilisce le regole per il trattamento dei dati personali su larga scala da parte di organismi pubblici e privati. Questo articolo stabilisce le obbligazioni per le imprese e gli enti che effettuano trattamenti di dati personali su larga scala, come la raccolta, l'elaborazione, la conservazione e la diffusione di dati. Inoltre, prevede sanzioni per la comunicazione o diffusione illecita di dati personali da parte di organismi pubblici e privati, con pene che possono arrivare fino a sei anni di reclusione. La norma prevede due fattispecie incriminatrici: la prima è integrata da altre disposizioni non penali, la seconda si basa sull'assenza di consenso. Il consenso è un elemento essenziale per la liceità della comunicazione o diffusione dei dati personali.

Nel quadro normativo del trattamento dei dati personali a livello comunitario il regolamento ha introdotto un nuovo termine "larga scala", il quale però, nonostante la normativa comunitaria faccia più volte riferimento a tale locuzione non enuncia mai una definizione concreta e chiara, ciò accade anche in ambito nazionale nel decreto attuativo 101/2018, in cui manca una definizione ben precisa di tale terminologia.

Soltanto nel *considerandum* 91 il GDPR, viene stabilito che si possono considerare trattamenti su larga scala quelli che hanno per oggetto sia a livello regionale, nazionale che sovranazionale la gestione ed il controllo di una grande quantità di dati, che per loro natura necessitano di una particolare protezione, poiché presentano dei rischi e delle criticità dovute alla grande

quantità di interessati. Un altro riferimento normativo che può essere di ausilio in tal senso è il gruppo di lavoro articolo 29, nel quale vengono indicate le linee guida al fine di poter constatare se il trattamento dei dati personali può essere stato attuato o meno su larga scala.[8] Il Gruppo di lavoro articolo 29 attraverso l'utilizzo dell'art. 37 GDPR enuncia alcune fattispecie mediante le quali si arriva ad una specifica definizione della nozione di larga scala.

Con riferimento al concetto dei dati su "larga scala" nel terzo capitolo verrà inoltre, analizzato il recente caso di cronaca internazionale relativo al caso *Facebook/Cambridge Analytica*. Nel 2013 il fondatore della società SCL costituì un nuovo ramo di azienda denominato *Cambridge Analytica* la quale si occupava prevalentemente di consulenza politica. La società *Cambridge analytica*, attraverso l'applicazione "*Thisisyourdigitallifeche"* si era riservata in accordo con *Facebook* di poter inviare a soggetti terzi i dati raccolti dall'applicazione stessa.

I dati venivano acquisiti attraverso un test sottoposto a tutti coloro che avevano un account *Facebook* che cliccando sullo stesso e compilando tutti i dati richiesti permettevano inconsapevolmente agli sviluppatori dell'applicazione di ottenere informazioni non solo sull'utente, attraverso l'accesso all'interno del suo profilo *Facebook*, ma acquisivano anche i dati personali degli amici dell'utente. In questo modo l'archivio si riempiva anche di contatti indiretti, ossia dei dati personali degli amici degli utenti che avevano adoperato l'applicazione, ovviamente senza chiedere il loro consenso, creando uno scandalo di dimensioni paradossali, infatti in seguito, il colosso *Facebook,* fu condannato a pagare ingenti sanzioni pecuniarie.

Un ulteriore importante argomento affrontato è inoltre, il principio del *de bis in idem*. L'articolo 649 C.p.p. prevede il divieto per un soggetto di essere processato due volte per lo stesso reato, nella fattispecie che ci occupa il punto è stabilire se tale principio può essere applicato in presenza di una condotta incriminatrice che comporta l'applicazione di una sanzione penale e amministrativa, poiché il divieto riguarda soltanto la presenza di una duplice

[8] ANTONINI E., Il Trattamento illecito di dati personali nel Codice della Privacy – i nuovi confini della tutela penale, in Diritto e procedura penale 2005, 44

sanzione di natura penale. In buona sostanza, se in una stessa fattispecie è prevista l'applicazione di una normativa sanzionatoria di tipo penalistico ed una normativa sanzionatoria di tipo amministrativo se quest'ultima possiede un grado di afflittività particolarmente grave può essere considerata come una sanzione penale e come tale rientrare nel principio del *ne bis in idem*.[9] Pertanto, nell'ipotesi in cui una violazione della norma sul trattamento dei dati personali comporti l'applicazione di una doppia risposta sanzionatoria sia di natura amministrativa con l'applicazione ad esempio dell'art. 166, commi 1 e 2 del Codice *Privacy* e dell'art. 83 commi 4 e 5 del Regolamento e sia di natura penale a titolo di esempio, l'art. 167 *bis* secondo comma diffusione e comunicazione senza il consenso degli interessati dei dati personali su larga scala, non si crea una violazione del principio del *ne bis in idem* poiché si mira a raggiungere un trattamento sanzionatorio compatibile col principio di proporzionalità della pena. Il giudice penale ridurrà sensibilmente in maniera proporzionale l'entità della sanzione in presenza di una condanna intervenuta precedentemente in sede amministrativa, per tali motivi non potrà verificarsi la violazione del principio del *ne bis in idem,* in quanto viene messo in atto un meccanismo finalizzato a rendere il trattamento sanzionatorio compatibile col principio di proporzionalità.

In definitiva la protezione dei dati richiede un approccio olistico che comprenda sia la repressione legale che misure sanzionatorie modulate e proporzionate al caso specifico. La differenza tra buona e cattiva protezione dipende dalle disposizioni attuative nazionali, per tali motivi le istituzioni hanno un ruolo cruciale nel promuovere una cultura della protezione dei dati, insieme al GDPR che fornisce le regole basilari su cui bisogna partire, arricchendo sempre di più la normativa in argomento per garantire l'effettività dei diritti alla privacy.[10]

---

[9] *Ex multis*: Corte EDU, 4.3.2014, Grande Stevens e altri contro Italia; Corte EDU, 8.6.1976, Engels e altri contro Paesi Bassi; Corte di Giustizia Dell'Unione Europea, Grande Sezione, causa C-524/15, Sentenza 20.3.2018.

[10] BOLOGNINI L., BISTOLFI C., PELINO E., IL REGOLAMENTO, CIT., 120. 170 BOLOGNINI L., BISTOLFI C., PELINO E., IL REGOLAMENTO, CIT., 121. 171 PANETTA R., CIRCOLAZIONE, CIT., 17 SS.

172 PANETTA R., Circolazione, cit., 17 ss

CAPITOLO I

L'EVOLUZIONE DELLA NORMATIVA IN MATERIA DI PRIVACY

SOMMARIO: 1. Rilievi introduttivi– 2. diritto alla privacy e all'identità personale - 3. Definizione del bene della riservatezza- 3.1. (*segue*) "L'articolo 2 della Costituzione come "clausola aperta" - 3.2. (*segue)* La riservatezza come riflesso degli art. 13,14,15 e 21 della Costituzione - 4. Evoluzione della normativa italiana, dalla legge n.98 del 1974 alla legge n. 547 del 1993 sulla criminalità informatica - 5. La legge 31 dicembre 1996, n. 675"Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali - 6. Il d.lgs. n. 196 del 30 giugno 2003 "Codice in materia di protezione dei dati personali" - 7. La nozione di dato personale - 8. Il ruolo del Garante nel trattamento del dato personale - 9. La tutela dei dati personali nell'Unione europea e il Regolamento UE n. 2016/679 - 10. Altre fattispecie a tutela della riservatezza: art. 615 *ter* c.p. Accesso abusivo a sistemi informatici, 615 *quater* c.p. Detenzione e diffusione abusiva di codici di accesso, 617 *quater* c.p. Intercettazione abusiva – 11. Conclusioni.

1. Rilievi introduttivi

Per meglio comprendere il concetto di *privacy* è opportuno intraprendere un cammino a ritroso nella storia, la nozione del concetto di *privacy* risale ad antiche e nobili origini, poiché l'uomo da sempre ha cercato di proteggersi e di tutelarsi in un ambiente intimo e personale e di sottrarsi alle ingerenze esterne non autorizzate.

Abraham Maslow,[11] noto psicologo statunitense con il suo concetto sulla "piramide dei bisogni", afferma che il secondo bisogno, dopo quelli c.d. "fisiologici", c'è la tutela e la protezione della propria *privacy.*

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

In età medievale, ad esempio con il termine privacy si diede il sinonimo di familiare, invece nell'età feudale le relazioni tra individui che appartenevano al feudo- monade prendevano il nome di "senso di intimità".

Nell'Europa illuminista e pre-rivoluzionaria, ad esempio nasce la *privacy* dal diritto soggettivo dell'individuo, in un contesto sociale e istituzionale in cui la privacy non era la realizzazione di un diritto naturale, ma l'acquisizione di un privilegio da parte di un gruppo, per cui si avvertiva la necessità di tutelare la sfera privata della persona sia nelle sue componenti fisiche che psichiche.

Ancora intorno al 1890 due studiosi giuristi statunitensi Samuel. D. Warren e Louis. D. Brandeis sulla Harward Law Review, scrissero un saggio dal titolo "The Right to Privacy"[12], nel quale riconobbero per la prima volta l'esistenza di un autonomo diritto alla *privacy.*

L'excursus che sarà oggetto della trattazione nel presente capitolo inizierà dall'analisi degli articoli 2, 13,14,15, e 21 della Costituzione Italiana in ordine al contemperamento di opposti interessi come la libertà di manifestazione del pensiero e la riservatezza come diritto fondamentale riconosciuto ad ogni essere umano.

L'art. 2 Cost, prevede in particolare che lo Stato italiano tuteli 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.

L'individuo è posto al centro dell'ordinamento giuridico al fine di affermare la sua personalità, garantendo la tutela dei dritti inviolabili, sia nel contesto sociale che in quello strettamente individuale.[13]

---

[12] WARRENS 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.

[13] 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*

Cosicché il riconoscimento e la salvaguardia del bene giuridico del diritto alla *privacy* costituisce un diritto costituzionalmente protetto, nonché la massima espressione del rispetto dell'essere umano.

La società attuale è fondata ormai su l'utilizzo della rete per qualsiasi attività quotidiana sia sociale che economica, per cui la tutela del dato personale assume un'importanza fondamentale, sia nella fase dell'acquisizione, della circolazione ed infine nella fase della conservazione al fine di tutelare la riservatezza e la dignità umana.

Le prime norme introdotte dalla normativa italiana si riferiscono alla legge n.98 del 1974 e la legge n. 547 del 1993 sul tema della criminalità informatica, modificazioni ed integrazioni.

Successivamente la legge 31 dicembre 1996, n. 675 "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali nella quale si evince la mancanza di completezza ed esaustività della disciplina, infatti successivamente furono introdotte altre normative come il D.lgs 196/2003 Codice della *privacy* normativa specifica posta a tutela del trattamento dei dati personali, poi novellato dal D.lgs. n. 101/2018 e dal D.L. n. 139/2021.

A tal proposito, lo strumento giuridico per eccellenza della normativa sulla *privacy* è il dato personale, il quale consiste in tutte quelle informazioni dirette o indirette che identificano o rendono identificabile una persona fisica, attraverso la conoscenza delle sue abitudini, del suo stile di vita, del suo stato di salute, della sua situazione economica e di tutto ciò che riguarda il suo patrimonio personale.

La tutela dei dati personali ha un risvolto come vedremo non solo sul piano nazionale ma anche europeo con il Regolamento UE n. 2016/679 in inglese *General Data Protection Regulation,* GDPR.

Ed infine, verranno trattate le fattispecie che indirettamente tutelano la riservatezza dei dati personali, ossia l'art. 615 *ter* c.p. Accesso abusivo a sistemi informatici, l'articolo 615 *quater* c.p. Detenzione e diffusione

---

dottrinale e giurisprudenziale ormai cospicua, penso che a questo precedente non si possa dare gran peso».

abusiva di codici di accesso, e l'articolo 617 *quater* c.p. Intercettazione abusiva.

2. Diritto alla privacy e all'identità personale

L'esigenza dell'individuo di proteggere la propria riservatezza, o per meglio dire la "*privacy*" è strettamente sempre connessa alla natura umana.

Questa si caratterizza per il bisogno intrinseco di differenziare la sfera individuale pubblica, strettamente collegata ai rapporti sociali ed interpersonali, dalla propria sfera individuale privata, nella quale ogni azione è sottratta alle ingerenze esterne non autorizzate e riguarda prevalentemente aspetti della vita intima e familiare.

Se facciamo un passo indietro nel tempo, già nel periodo della *polis* greca esisteva la distinzione tra vita privata e pubblica, in cui quest'ultima era maggiormente esaltata e riservata alle persone istruite.

Lo stesso Aristotele definiva l'uomo come un "animale sociale-politico"[14], che necessitava di scambi sociali e culturali, poiché chi viveva maggiormente nel privato era considerato *extra societatem*.

Successivamente, dopo qualche secolo vi fu un cambio di tendenza, poiché venne riconosciuta la sacralità del focolare domestico ai cittadini romani dell'antica Roma, i quali venivano tutelati e protetti nello svolgimento della loro vita privata.

Ai giorni d'oggi il termine privacy viene definito, un concetto «*exasperatingly vague and evanescent*»[15], al quale non si può attribuire un'interpretazione unitaria, ma potremmo dire che consiste in un insieme di diritti il cui fulcro è composto da situazioni soggettive.

Pertanto oggi, il diritto alla privacy non consiste solamente nella violazione della vita privata, ma ha assunto anche mediante l'utilizzo

---

[14] Concetto di *"politikòn zôon"* di Aristotele espresso nel trattato Politica, traduzione a cura di Federico Ferri, Bompiani editore Milano, 2016

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

dell'informatica una metamorfosi, che ha cambiato definitivamente la rotta del concetto di privacy oggi tendente a controllare e a gestire la circolazione dei dati personali non solo *stricto sensu*, bensì proiettati verso la tutela di beni come la reputazione e l'onore.

Infatti, alla luce di quanto sopra argomentato il predetto potere di gestione e di controllo della circolazione dei dati personali ha come obiettivo principale la tutela della dignità umana in relazione alla sua identità.

Dunque, il concetto di *privacy* coincide con la protezione dell'identità personale che consiste nel complesso delle informazioni relative ad un soggetto e trasferite al pubblico.

Sul punto la Corte di Cassazione[16] ha ritenuto che l'identità personale, consiste nella rappresentazione fedele del proprio modo di essere agli occhi della società, invece, la riservatezza consiste nella propria sfera personale che non si desidera mostrare all'esterno.

Pertanto, la dottrina e la giurisprudenza maggioritaria ritengono che l'identità personale deve essere come il diritto alla propria immagine sociale, ossia la proiezione della propria personalità così come risulta nella realtà.

Sull'argomento è importante evidenziare le analisi condotte dal Professore Rodotà[17], il quale riteneva che al fine di scongiurare che l'identità personale venga sottoposta a profili ed algoritmi che favoriscono meccanismi di etichettamento, rischiando l'annullamento dell'autodeterminazione individuale e l'unicità dell'essere umano, nonché la sua eccezionalità è necessario intervenire con una normativa forte di protezione e controllo dei dati personali sia a livello nazionale che internazionale.

---

[16] Cass. penale 22.6.1985, n. 3769

[17] S RODOTA., *Il mondo nella rete*. Quali i diritti, quali i vincoli, Roma – Bari, 2014
S. RODOTÀ *Il problema della responsabilità civile*, Milano, Giuffrè, 1961; 1964.

Infatti, il professor Rodotà portava avanti il principio di dignità, libertà ed eguaglianza, colonne portanti della sua ideologia su cui basava il percorso evolutivo della nuova normativa sul diritto alla *privacy.*

Soltanto un'adeguata protezione dei dati personali può rivelarsi un ottimo strumento per assicurare l'integrità e combattere il fenomeno della frammentazione e polverizzazione dell'identità personale.

A tal proposito, Rodotà intuì che l'identità personale con l'utilizzo del web non era più configurabile come dimensione immobile, ma come intangibile della propria proiezione sociale.

In buona sostanza possiamo ritenere, che attraverso esperimenti effettuati nel laboratorio giurisprudenziale e anche mediante il supporto della dottrina il diritto alla privacy ha acquisito con il tempo fluidità e dinamicità.

Sul punto non possono non essere citati due giovani famosi avvocati americani, Samuel Warren e Louis Brandies,[18] che per la prima volta sulla *Harvard Law Review* nel dicembre del 1890 pubblicarono il loro saggio, "*the right to be let alone*" ovvero il diritto ad essere lasciati soli e godere della propria sfera privata.

Il saggio sopra richiamato si basa sulla tutela del diritto alla *privacy* ed è considerato la colonna portante su cui oggi poggia l'istituto giuridico della *privacy.*

I due giovani avvocati consideravano la vita anche dal punto di vista intellettuale ed emotivo spiegando che solo una parte del dolore, del piacere e del profitto della vita risiede nei beni materiali.

Pertanto, il concetto di *privacy* si basa inizialmente sulla solitudine dell'io e sulla libertà, acquisendo un risvolto giuridico che con il tempo ha invaso una parte dei nostri codici, poiché sarà ritenuto un diritto inviolabile da tutelare.

---

[18] SAMUEL WARREN E LOUIS BRANDIES,[18] autori del saggio, "the right to be let alone Pubblicato per la prima volta sulla *Harvard Law Review* nel dicembre del 1890, The Right to Privacy rappresenta la pietra angolare su cui poggia il moderno istituto giuridico della privacy, considerato al giorno d'oggi come il diritto fondamentale su cui si fonda la libertà individuale di fronte al cosiddetto "*Capitalismo della Sorveglianza" (Zuboff, 2018).*

Tale saggio fu considerato dai giuristi contemporanei una pietra miliare nella quale venne affrontato il tema della privacy come bene astratto ma concreto, poiché il piacere e il dolore sono delle sensazioni ed emozioni che vanno tutelate alla stregua del bene materiale attraverso una crescita ed un riconoscimento legale, in questa maniera i giudici possono offrire la necessaria protezione.

Infatti, le fotografie, gli articoli dei giornali, hanno ormai oltrepassato il recinto della vita privata e domestica e soprattutto i numerosi dispositivi tecnologici minacciano di rendere noto ciò che invece si vuole mantenere riservato.

La legge a tal proposito deve offrire un rimedio efficace e valido, affinché, la circolazione dei dati personali non autorizzati sia bloccato e ritenuto illecito, poiché vi è una continua invasione della *privacy* da parte dei social e dei mezzi di pubblica comunicazione.

3. Definizione del bene della riservatezza

La tutela penale della *privacy* ruota attorno al diritto della riservatezza che è un bene giuridico protetto ed autonomo a cui la società attribuisce particolare rilevanza.

Con l'introduzione dell'informatica intorno ai primi anni settanta hanno inizio le prime forme di conservazione e archiviazione dei dati, i supporti cartacei piano piano scompaiono per dare il posto a processi telematici che selezioneranno grandi quantità di informazioni e di dati personali.

A tal proposito la paura che le nuove tecnologie possano ledere i dati personali inseriti in varie banche dati, fa sorgere la necessità di proteggere e tutelare la riservatezza come bene giuridico.

Necessita, pertanto, procedere ad un'interpretazione estensiva del diritto alla riservatezza, poiché il bene da tutelare non è soltanto la sfera

privata come intimità, ma anche il rispetto della libertà di scelta di ciascuno soggetto senza essere costretto ad uniformarsi.

Fino a qualche anno fa, nonostante vi fossero norme che riguardavano la protezione del diritto alla *privacy,* come il diritto all'immagine secondo l'articolo 10[19] del codice civile, l'inviolabilità del domicilio ai sensi dell'articolo 614 [20]del codice penale, nell'ordinamento giuridico italiano, non era prevista una normativa specifica che prevedesse espressamente una tutela alla riservatezza.

Per la prima volta il vero punto di svolta per il riconoscimento del diritto della riservatezza è stata una sentenza della Corte di Cassazione del 1975[21] nella quale furono riconosciuti i principi fondamentali su cui si fondano i requisiti essenziali della riservatezza.

Attraverso il riconoscimento dei diritti fondamentali, l'individuo viene considerato come singolo ma contestualmente partecipe alla vita della collettività pur mantenendo una sfera privata che riguarda la sua reputazione e la tutela della personalità individuale come componente della sfera privata costituita dalla riservatezza.

In questa prospettiva la reputazione è ritenuta come la stima che la collettività gode nei confronti di una determinata persona che si contrappone alla riservatezza che invece, riguarda unicamente la sfera relativa all'aspetto dell'individualità, poiché si riferisce solamente all'aspirazione del soggetto a conservare nella propria intimità determinate informazioni strettamente personali.

---

[19] 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».*

[20] 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.*

[21] Cass. 27 maggio 1975, Santuosso, in VISINTINI, I fatti illeciti Padova 2004. Relazione annuale del Garante, RODOTÀ S., Roma, 2003

Infatti, la violazione della riservatezza consiste nella divulgazione di particolari informazioni relative alla vita privata di un soggetto, le quali possono incidere sulla sua vita di relazione con la collettività e quindi ledere la sua reputazione.

Sul punto il giurista Mantovani[22], ed anche il giurista Bricola[23] hanno affrontato la tematica sulla tutela penale della riservatezza.

In particolare il Bricola, considera sia la reputazione che la riservatezza due entità contrapposte, poiché la reputazione si fonda sul presupposto di ciò che la collettività conosce su una determinata persona e la relativa opinione sulla stessa.

Diversamente, la riservatezza si fonda sulla opposta volontà da parte dell'avente diritto di non mettere a conoscenza dei fatti strettamente personali a terze persone.

Dunque, il Bricola[24] sostiene che l'interesse alla riservatezza è successivo rispetto all'interesse della vita privata, ossia il diritto alla riservatezza consiste nell'interesse a mantenere nell'ambito della propria sfera privata determinati fatti che l'avente diritto desidera restino tali, impedendo l'attività di terzi che vogliono divulgarle, invece, l'interesse al rispetto della vita privata consiste nell'impedire che altri vengano a conoscenza di circostanze relative alla propria vita privata.

In buona sostanza la riservatezza difende la sfera privata dalla divulgazione di notizie legittimamente acquisite e il diritto al rispetto della vita privata difende il soggetto da interferenze esterne in questa sfera.

Altri studiosi[25] hanno messo in relazione la tutela dell'onore dell'immagine e del nome da tutelare all'interno del concetto di *privacy*.

---

[22] F. MANTOVANI, *Diritto alla riservatezza e libertà di manifestazione del pensiero con riguardo alla pubblicità dei fatti criminosi*, in AA.VV. *Il diritto alla riservatezza e la sua tutela penale, (atti del terzo simposio di studi di diritto e procedura penale, Varenna 5-7 Settembre 1967)*, Milano, 1970, pp. 405 ss.

[23] F. BRICOLA, *Prospettive e* limiti, cit., p. 1088.

[24] F. BRICOLA *PROSPETTIVE E LIMITI*, CIT., P. 1084.

[25] G. GIACOBBE, nel tentativo di ricostruire la storia dell'analisi dottrinaria sull'ammissibilità della tutela della *riservatezza*, espone il tentativo di considerarla come un *diritto soggettivo*. L'Autore non manca di sottolineare come questa teoria si fondi sulla possibilità di fruire degli strumenti preesistenti (tutela dell'onore e reputazione), il che

In particolare, il diritto all'immagine è collegato alla tutela della vita privata in quanto soggetto di diritto, ma ci sono degli elementi che vanno differenziati poiché non coincidono perfettamente.

La tutela apprestata all'onore e alla reputazione non solo risulta di più ampia portata, ma per loro è prevista una differente tutela giurisdizionale che presuppone l'individuazione del grado e dell'intensità della lesione, che in un certo qual modo la rende incompatibile con il diritto alla riservatezza che invece presuppone l'applicazione della sanzione in presenza di determinati atti e comportamenti illeciti che riguardano fatti della sfera privata.

In conclusione tra la riservatezza e la reputazione c'è una matrice comune ma hanno diversità strutturali relative alla tutela apprestata dall'ordinamento giuridico e un diverso interesse di cui consta il diritto alla riservatezza.

---

come visto nel testo non garantisce una tutela adeguata all'interesse in esame; ma mediante l'utilizzo di specifici strumenti tecnici (i quali consentano la tutela *oggettiva* del bene prima che avvenga la lesione) è possibile attuare una tutela basata sulla predisposizione di modelli comportamentali che si fondi sul controllo delle modalità e delle tecniche di acquisizione della notizia. 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.

In tale panorama il diritto alla riservatezza si esprime attraverso il controllo e la gestione sui propri dati personali intesi come "corpo elettronico", ormai inserito in svariate banche dati di diversi luoghi.

Un diritto i cui elementi fondamentali devono intendersi come il complesso di poteri e doveri che appartengono a ciascun individuo.

Il fulcro del discorso si fonda, pertanto, sulla ricerca del riferimento normativo e costituzionale del diritto alla riservatezza attraverso il quale si possono trarre le dovute valutazioni sull'opportunità di costituire una tutela penale.

Per quanto riguarda la tutela costituzionale, come si può facilmente evincere, gli articoli 14, 15 e 21 della Costituzione rispettivamente sul domicilio, sulla libertà, sulla segretezza della corrispondenza e sulla libertà di manifestazione del pensiero, tutelano indirettamente aspetti privati, ma è soprattutto l'analisi interpretativa dell'articolo 2 della Costituzione, che viene considerato come formula aperta, poiché riconosce il diritto alla riservatezza come un diritto inviolabile e prevede una tutela dei " *diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità".*

In correlazione ai predetti articoli della Costituzione Italiana si possono analizzare l'articolo 12[26] della Dichiarazione Universale dei diritti dell'uomo, nella quale viene sancito il principio secondo il quale "*nessun individuo può essere sottoposto a interferenze nella sua vita privata"* e l'articolo 8 [27] della Convenzione europea sulla salvaguardia dei diritti dell'uomo e delle libertà fondamentali il quale prevede il "*diritto di ogni persona al rispetto della sua vita privata e familiare*".

---

[26] 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».*

[27] 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».*

Analizzato e compreso il contenuto del diritto alla riservatezza è opportuno evidenziare che lo stesso per sua natura è un bene giuridico suscettibile di subire trasformazioni nel tempo, in stretta correlazione con il cambiare del contesto storico e sociale in relazione alle esigenze dei luoghi e delle circostanze richiedendo la mobilità del suo contenuto.

Per tali motivazioni come non è possibile dare una definizione rigida e predefinita del diritto alla riservatezza, allo stesso modo non è possibile stabilire *ex ante* tutte le fattispecie che possono potenzialmente essere lesive del bene giuridico oggetto di tutela.

Ribadendo il concetto superiore relativo all'impossibilità di una definizione prestabilita ed immutabile del diritto alla riservatezza, una parte autorevole della dottrina[28] analizzando le radici sottese al diritto alla riservatezza ha evidenziato un dato importante, che va oltre il diritto della tutela della propria vita privata, ossia la tutela del diritto affinché nessuno, possa se non autorizzato, utilizzare o servirsi dei dati personali di un altro soggetto.[29]

Il concetto di *privacy* si basa inizialmente sulla solitudine dell'io, sulla libertà di tenere riservate alcune informazioni strettamente personali, acquisendo piano piano un risvolto giuridico che ha invaso parte dei nostri codici poiché sarà ritenuto un diritto inviolabile da tutelare.

Ciò porta a ritenere che il bene giuridico della riservatezza è caratterizzato da una duplicità di elementi, da un lato il diritto al segreto ossia il diritto di mantenere riservati i propri dati e informazioni personali e dall'altro lato il diritto che può assumere varie sfaccettature come la salvaguardia sull'utilizzo, sulla gestione e sul controllo della propria identità personale al fine di proteggere i propri dati.

In questa maniera si passa ad una nuova definizione del diritto alla riservatezza, ossia da un concetto immobile e statico che fa riferimento esclusivamente al segreto dei dati personali e della propria vita privata al concetto più dinamico e moderno, ossia quello di avere il controllo e la

[28] [86]F. MUCCIARELLI I*nformatica e tutela penale della riservatezza, in Il diritto penale dell'informatica nell'epoca di internet*, PICOTTI L. Padova, 2004
[29] CARNELUTTI F., *Diritto alla vita privata*, in Riv. Trim. dir. Proc., 1995

gestione di tutti i dati e le informazioni che ormai nell'attuale società informatica circolano in modo incontrollabile e veloce all'interno dei sistemi informatici.

A questi cambiamenti l'ordinamento giuridico italiano ha dato un enorme impulso, soprattutto in relazione al diritto del singolo, mediante l'introduzione di nuove fattispecie incriminatrici, attraverso le quali ha acquisito strumenti capaci di reprimere condotte lesive per la tutela del bene giuridico della riservatezza**.**

Necessita, pertanto, procedere ad un'interpretazione estensiva del diritto alla riservatezza, poiché il bene da tutelare, se negli anni 70/80 era esclusivamente la vita privata come intimità, negli anni 90 il bene da proteggere è il diritto al controllo dei propri dati personali, con la inevitabile conseguenza che in quest'ultima prospettiva si è ampliato il concetto del diritto alla riservatezza.

Per tali motivi, giova ribadire, il diritto alla riservatezza subisce dei sostanziali cambiamenti in relazione al contesto storico, culturale e tecnologico, non potendo per sua natura essere rigidamente classificato a priori.

Dunque, la *privacy* si fonda principalmente su due pilastri: la riservatezza e il controllo. Alla prima si addice il silenzio, all'altra la trasparenza.

La prima normativa dedicata al tema della tutela penale relativa al diritto alla riservatezza come bene giuridico individuale e alla vita privata è stata la Legge 8 aprile 1974, n. 98 "Tutela della riservatezza e della libertà e segretezza delle comunicazioni".

Questo non vuol dire che nell'impianto iniziale del codice Rocco non vi fossero norme che in maniera indiretta, mediante figure penali aventi ad oggetto beni giuridici di diversa natura, non tutelassero la riservatezza e la *privacy.*

Basterà fare riferimento al titolo XII relativo ai delitti contro la persona, al capo III ai delitti contro la libertà individuale o alle fattispecie incriminatrici relative alla inviolabilità dei segreti, come la violazione,

sottrazione e soppressione di corrispondenza, interruzione o impedimento illeciti di comunicazioni telegrafiche o telefoniche, reati che puniscono tutte le azioni aventi ad oggetto rivelazione di segreti.

Con il sopraggiungere della tecnologia informatica si sono manifestati importanti aspetti ritenuti meritevoli di tutela e altrettanto sono sopraggiunte nuove insidie che hanno reso la precedente normativa del codice, insufficiente a tutelare, nella società attuale il diritto alla sfera della propria vita privata.

Pertanto, è sopraggiunta nella coscienza sociale la necessità di tutelare i nuovi interessi emersi, sicuramente fra questi vi è il bene giuridico della riservatezza o della sfera privata, sotto una chiave più moderna, secondo un termine inglese diritto alla *privacy.*

Il diritto alla riservatezza, alla *privacy* e alla tutela della propria vita privata, sono terminologie che si riferiscono a concetti sintetici anche se con piccole differenze di significato fanno capo ad un unico bene giuridico tutelato dalla Costituzione Italiana.

In particolare l'articolo 2[30] chiamata "clausola aperta" conferisce un'interpretazione dinamica, ossia che può essere adattata a varie fattispecie nelle quali viene manifestata la personalità del soggetto come espressione del bene giuridico della riservatezza, sia come singolo che nelle formazioni sociali.[31]

---

[30] L'articolo 2 della Costituzione in argomento espressamente afferma 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"*.

[31] 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».*

3.1 (*segue*) L'articolo 2 della Costituzione come "clausola aperta"

L'articolo 2 della Costituzione Italiana rappresenta per eccellenza la cornice entro cui vengono inserite la maggior parte delle attività con cui un soggetto svolge la propria vita privata suscettibile di tutela costituzionale.

[32]L'art. 2 Cost, prevede in particolare che lo Stato tutela 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. L'individuo è posto al centro dell'ordinamento giuridico al fine di affermare la sua personalità e garantendo la tutela dei dritti inviolabili, sia nel contesto sociale che in quello strettamente individuale.[33]

Cosicché il riconoscimento e la salvaguardia del bene giuridico del diritto della *privacy* costituisce un diritto costituzionalmente protetto, nonché la massima espressione del rispetto dell'essere umano.

Pertanto la ricerca del fondamento costituzionale del diritto alla riservatezza è un *prius* logico giuridico, senza il quale qualsiasi riconoscimento di carattere non costituzionale verrebbero in contrasto con le altre libertà aventi invece rango costituzionale senza possibilità di creare eventuali bilanciamenti.

Infatti diventa logico ritenere che il rapporto tra le altre libertà costituzionali e la riservatezza deve svilupparsi su uno stesso livello di parità.

---

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

[33] 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».*

A tal proposito, giova ribadire, che tra le varie norme costituzionali l'articolo 23 della Costituzione riconosce maggiore sostegno al diritto alla riservatezza rispetto ad altre norme successive il cui contenuto è più circoscritto a singoli aspetti della personalità umana.

In tale contesto l'articolo 2 ha il compito di garantire costituzionalmente i diritti inviolabili dell'essere umano al fine di avere una completa tutela.

Soltanto in questa maniera l'ordinamento giuridico giunge alla realizzazione di proteggere in maniera efficace la persona umana.

Pertanto, la natura di norma aperta dell'articolo 2 della Costituzione ha la funzione fondamentale di conferire al testo costituzionale quel grado di elasticità che permette di adeguarsi da parte del diritto alle modificazioni sociali e culturali cui l'essere umano va incontro all'interno di una società in continua evoluzione, quindi potremmo dire che è una costituzione vivente che tutela gli interessi nel contesto sociale.

Ecco che, in base a tali considerazioni, il riconoscimento costituzionale della riservatezza fa venir meno quel sospetto di forzatura del testo costituzionale nel momento stesso in cui soddisfa il fine superiore di apprestare effettiva tutela alla persona umana e ai suoi diritti fondamentali.

La riservatezza pur essendo di rilevanza autonoma ha anche un ruolo strumentale, poiché mira a sottrarre determinate informazioni strettamente personali alla conoscenza di terzi e quindi ad assicurare alla persona il pieno godimento dei propri diritti fondamentali sanciti dalla costituzione che sono: 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 la corrispondenza .

La Corte di Cassazione sull'articolo 2 ha espresso un'interpretazione piuttosto generica, precisando che l'obiettivo del predetto articolo è la protezione dell'essere umano in tutte le sue manifestazioni, poiché si colloca come fulcro dei bisogni materiali e spirituali della persona umana non potendo per tali motivazioni avere delle finalità riepilogative.

Pertanto, l'articolo 2 della Costituzione italiana è definito come una clausola aperta per la tutela apprestata verso la libertà di scelta dell'individuo, di conseguenza diventa idoneo a valorizzare nuovi aspetti che possono emergere in capo all'individuo purché fondamentali.[34]

Il pregio di tale articolo consiste nella sua elasticità alla stessa stregua dalla norma generale ed astratta, l'unico inconveniente riguarda il grande lasso di tempo tra la sua entrata in vigore e gli attuali cambiamenti, soprattutto con riferimento alle novità di natura tecnologica che sono sopravvenuti. [35]

A tal riguardo una parte della dottrina si sofferma maggiormente sul principio dell'inviolabilità che viene riconosciuto ai predetti diritti fondamentali posti al vertice della piramide dei valori costituzionali. L'elemento dell'inviolabilità attribuisce ai predetti diritti una caratteristica che li rende unici per la loro intangibilità e immodificabilità, anche di fronte al procedimento di revisione costituzionale. [36]

Sulla base di questa concezione l'articolo 2 ha l'obiettivo di garantire costituzionalmente tutti quegli interessi che si caratterizzano in un determinato contesto storico, sociale e politico, da ciò si apre l'interpretazione della valutazione sotto l'aspetto sostanziale e teleologico e non astratto, in questa maniera si attua lo scopo della Costituzione ossia di proteggere i diritti dell'essere umano.[37]

Pertanto, l'articolo 2 come norma aperta attraverso il grado di elasticità di cui è composto, consente di adeguarsi alle varie modificazioni culturali e sociali in cui la società naturalmente si trova a dover affrontare,

---

[34] 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.

[35] 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.

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

[37] 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».*

delineando la caratteristica peculiare di "costituzione vivente" ossia capace di adeguarsi al contesto sociale sempre mutevole e di rafforzare ove necessario una tutela adeguata al passo con i tempi.[38]

Ciò posto, il riconoscimento da parte della Costituzione italiana e precisamente nell'articolo 2 al diritto alla riservatezza, sembra soddisfare appieno la tutela della persona e dei suoi diritti inviolabili.

Si può dunque affermare che la riservatezza, pur avendo una sua autonomia, possiede un ruolo strumentale, nel senso che garantisce ad ogni soggetto la tutela di intrusione da parte di terzi nella propria sfera privata, al fine di assicurare il pieno godimento dei diritti fondamentali sanciti dalla Costituzione. [39]

Nel linguaggio tecnico giuridico il diritto alla riservatezza consiste nel diritto di proteggere i propri dati personali e di tutto ciò che riguarda la propria sfera privata dai poteri pubblici e dai soggetti terzi che a volte entrano nella nostra vita intima al fine di conoscerne le caratteristiche peculiari individuali ed utilizzarli in maniera illecita.

Il tema della riservatezza è un diritto oggi di grande attualità, poiché come non mai è messo a rischio dalle nuove e numerose tecnologie che ormai fanno parte del nostro *modus vivendi.*

La società ci espone a fornire quotidianamente per varie motivazioni i nostri dati personali che poi non si è sicuri che vengano garantiti e custoditi nella maniera corretta, mettendo a repentaglio la nostra riservatezza e anche la nostra dignità umana.

---

[38] 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.,

[39] 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».*

3.2. (*segue)* La riservatezza come riflesso degli art. 3,14,15 e 21 della Costituzione

La Costituzione italiana prevede al suo interno altri articoli che rafforzano ulteriormente la tutela della *privacy*, in quanto riguardano altri interessi particolari della vita privata di un soggetto.

L'espressione "pari dignità sociale" e "pieno sviluppo della persona umana", esaltano la capacità di autodeterminazione dei cittadini come elemento di democrazia.

L'articolo 3 [40] della Costituzione italiana, tutela interessi quali, la dignità e lo sviluppo della persona diritti di carattere prettamente sociale che non devono essere visti in un'ottica di contrapposizione alla sfera individuale, ma di compensazione nella quale si esprimono il diritto alla riservatezza e alla vita privata.[41]

Le predette affermazioni vanno contestualizzate in relazione all'avvento dell'informatica e alle necessarie modifiche apportate al concetto di *privacy,* pertanto non è più adeguato effettuare una distinzione tra individualità e collettività se non si vuole rischiare di dare una falsa rappresentazione della realtà.

Per cui il riferimento alla dignità sociale espressamente indicata nell'articolo 3 della Costituzione italiana è considerata non come qualcosa

---

[40] Art. 3 della Costitzione italiana: *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".*

[41] 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». Infine, è d'obbligo segnalare che la dottrina del BRICOLA, sulla base della distinzione da lui sostenuta tra diritto alla riservatezza e diritto al rispetto della vita privata, ritiene costituzionalizzato solo quest'ultimo, e non anche il diritto alla riservatezza; questo sulla base della formulazione dell'art. 8 della Convenzione europea e dell'art. 12 della Dichiarazione universale dei diritti dell'uomo, che prevedono rispettivamente "l'ingerenza" e l'interferenza arbitraria".

di diverso dalla riservatezza, poichè è strettamente legata al concetto di decoro e di reputazione alla persona.[42]

La dottrina[43] più favorevole riconosce l'articolo 3 Cost., come un supporto costituzionale al diritto alla riservatezza, poichè ha dato maggior impulso alla protezione della sfera privata, affinché la dignità venga realmente rispettata quale strumento del libero sviluppo della persona.

Infatti, la libertà personale deve essere intesa non solamente dal punto di vista fisico ma anche in relazione alla dignità umana, spesso considerata meno importante, invece deve essere armonizzata con il diritto alla riservatezza ed alla *privacy* [44].

In questa maniera l'inviolabilità della libertà personale protegge il soggetto da ogni indebita ingerenza altrui nella propria sfera fisica e psichica.

Anche l'articolo 14 Cost., prevede un altro diritto inviolabile ossia il domicilio, nel senso che non è possibile effettuare ispezioni o perquisizioni, se non nei casi espressamente previsti dalla legge secondo le garanzie prescritte per la tutela della libertà personale. [45]

Ancora l'articolo 15 Cost, "*La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La*

---

[42] 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.Come già accennato il Bricola ritiene che il delitto di indiscrezione sarebbe posto a tutela della vita privata, mentre la divulgazione violerebbe la riservatezza; Mantovani sostiene contra, che il bene giuridico tutelato dalle due disposizioni sia unico, in quanto esse costituiscono due modalità di aggressione al medesimo bene: la riservatezza.
RODOTÀ S., Tecnologie e diritti, Bologna, 1995, pp. 29 ss.

[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.

[44] VALENTI A. M., La dignità umana quale diritto inviolabile dell'uomo, Perugia, 1995, pp. 9 ss.

[45] MORSILLO G., La tutela penale del diritto alla riservatezza, MILANO, 1966, P. 274.

loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge".[46]

Una piccola parte della dottrina[47] nega la rilevanza costituzionale del diritto alla riservatezza, poiché in contrasto con la libertà di espressione.

La libertà di espressione in realtà non entra per forza in conflitto con il diritto alla riservatezza, poiché manifestare il proprio pensiero mediante la comunicazione e far circolare determinate notizie non si traduce necessariamente in una limitazione della libertà di pensiero.

L'articolo 21 Cost prevede espressamente che, "*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…"*

Dalla lettura del predetto articolo 21 Cost, si deduce che le attività relative alla manifestazione del pensiero e divulgazione delle informazioni, sono espresse in relazione ad altre libertà parimenti garantite costituzionalmente.

Dal predetto assunto si evince che la manifestazione del pensiero e l'informazione non hanno un valore assoluto, ma devono essere funzionali allo sviluppo del singolo e della collettività in ossequio al diritto alla riservatezza.

Pertanto, l'articolo 21 Cost. delimita i confini entro i quali basare il fondamento costituzionale del diritto alla riservatezza, ossia riconoscere il diritto di poter esprimere le proprie idee e anche la libertà di tacere e di rispettare la *privacy* altrui.[48]

---

[46] 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"».*

[47] VALENTI A. M., La dignità umana quale diritto inviolabile dell'uomo, Perugia, 1995, pp. 9 ss.

[48] 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

Per cui tutte le volte che terze persone diffondono informazioni relative a soggetti che non hanno dato il loro consenso, quest'ultimi subiscono una lesione delle loro libertà negative cioè di riservatezza espressamente tutelata dall'articolo 21 della Costituzione italiana.

Dunque, attraverso l'applicazione del criterio del bilanciamento si attribuisce un uguale riconoscimento costituzionale sia al diritto di parlare, che al diritto di tacere, attribuendo pari dignità a ciascuno, senza creare una gerarchia interna tra le due libertà che invece, riguardano situazioni di pari livello.

4. Evoluzione della normativa italiana dalla legge n. 98 del 1974 alla legge n. 547 del 1993 sulla criminalità informatica

Con l'introduzione della L.98/1974 il legislatore ha integrato le norme già esistenti relative all'inviolabilità dei segreti e al domicilio, con lo scopo di rendere più completo l'ambito di tutela, proprio in relazione ad una maggiore valorizzazione del bene giuridico della riservatezza.

Quando si parla di bene della riservatezza, giova ribadire, intendiamo riferirci al diritto esclusivo di un soggetto di controllare e gestire i fatti relativi alla propria vita privata e di tenerli custoditi senza che altri non autorizzati ne possano venire a conoscenza.

Con questo non si vuole affermare che la sfera privata coincide con quella del segreto anche se è oggetto di tutela penale, ma con il tutelare la sfera della riservatezza vengono protetti anche alcune notizie strettamente riservate alla persona, di carattere professionale o anche scientifico industriale.

Ovviamente la tutela del segreto può essere ritenuta strumentale alla tutela della riservatezza quando i segreti che sono protetti riguardano elementi della vita privata di un soggetto che solo lui essendo l'interessato può conoscere.

In particolare gli articoli introdotti dalla legge n. 98/1974 riguardano l'articolo 615 *bis c.p.* "interferenze illecite nella vita privata", l'art. 617 *bis* c.p. "Installazione di apparecchiature atte ad intercettare o impedire comunicazioni telegrafiche o telefoniche" e l'art. 617 *ter* c.p. "falsificazione, alterazione o soppressione di contenuto di comunicazioni".

L'assetto normativo relativo alla tutela della riservatezza è stato oggetto di varie evoluzioni e si è via via arricchito con vari interventi legislativi di particolare importanza, infatti dopo la legge del 1974, negli anni 90 è subentrata la Legge 23 dicembre 1993, n. 547 riguardante le "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".

La predetta normativa ha cercato di colmare le lacune che si sono venute a creare a seguito delle nuove tecnologie informatiche, con l'introduzione di nuove fattispecie incriminatrici nel corpo del codice penale in cui già era intervenuta la Legge del 74.

Le novità introdotte con la legge 547/93 riguardano gli articoli 615 *ter* del c.p. "Accesso abusivo a un sistema informatico o telematico", l'art. 615 *quater* c.p. "Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici" e l'art. 616 c.p. che ha introdotto accanto al concetto di corrispondenza anche quello informatico e telematico.

L'art. 617 *quater* c.p. "intercettazione impedimento o interruzione illecita di comunicazioni informatiche o telematiche", l'art. 617 *quinquies* c.p. "installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche".

Ai fini della presente indagine sulla *privacy*, sono maggiormente pertinenti soprattutto gli articoli 615 *ter, quater* e 617 *quater e quinquies* del codice penale introdotti dalla legge 547/93 che verranno trattate in seguito, poiché fattispecie che indirettamente tutelano la riservatezza dei dati personali.

5. La legge 31 dicembre 1996, n. 675. "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali"

In Italia la normativa sulla privacy trova ingresso non tanto con l'introduzione della Convenzione di Strasburgo che non ebbe molta influenza nel nostro sistema giuridico, ma con il Trattato di Schengen, il quale prevedeva l'attuazione alla libera circolazione delle persone con l'eliminazione dei controlli alle frontiere e la Direttiva n. 95/46.

Nel 1996 con l'introduzione della legge n. 675, che riguarda la "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali", l'obiettivo del legislatore era quello di colmare molte lacune che la nostra legislazione presentava in tema di dati personali.[49]

Pertanto, le finalità perseguite dalla superiore normativa risiedevano nell'attuazione di garantire le libertà fondamentali e la dignità dell'essere umano con particolare riferimento all'identità personale e alla riservatezza, poiché il trattamento dei dati personali era alla base delle relazioni sociali ed economiche e ciò determinava, le modalità con le quali era giusto che si svolgesse il trattamento dei dati personali.

Per effetto della legge n. 675/96, prendeva sempre più importanza l'espressione "trattamento dei dati personali" sino a quel momento ignorato, poiché non vi era ancora un'adeguata regolamentazione giuridicamente rilevante, in quanto ancora non era stata attribuita la giusta importanza a tale tema.

L'art. 1 della predetta legge prevedeva: "*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*

[49] IMPERIALI R., Codice della Privacy, Milano, 2005.

associazione", contenuto poi riportato all'interno dell'art. 2 comma 1 del Codice *privacy*.[50]

Inoltre, l'articolo 1, comma 2 della legge 675/96 indicava il significato di alcuni termini come trattamento, dato personale, responsabile, titolare e interessato utilizzati nel testo normativo, al fine di rendere più chiara la legge e porre la persona al centro della scala dei valori.

La legge 675/96 prevedeva inoltre, che qualsiasi attività relativa al trattamento di dati personali doveva svolgersi secondo i criteri di liceità, correttezza del trattamento e soprattutto pertinenza e cioè aggiornamento dei dati trattati nel rispetto del principio del c.d. "diritto all'oblio".

Il diritto cosiddetto "all'oblio" si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata.

Pertanto, qualora il titolare del trattamento dei dati non avesse ottemperato all'attuazione di tali principi, avrebbe posto in essere un trattamento illecito e avrebbe dovuto risarcire l'eventuale danno cagionato all'interessato, sia materiale che morale.

Nella predetta normativa la nozione di *privacy* si era allargata fino a ricomprendere tutte quelle regole sulla circolazione dei dati personali facendo riferimento alla rilevanza costituzionale che ne prevede la tutela.

Tale normativa, pertanto, seppur in maniera generale aveva già indicato esplicitamente quelli che erano gli scopi legittimi del trattamento dei dati personali, i quali dovevano essere acquisiti per una finalità specifica e utilizzati soltanto ed esclusivamente per tali scopi e per un determinato periodo di tempo non superiore a quello necessario al raggiungimento dell'obiettivo per cui erano stati acquisiti.[51]

---

[50] 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.

[51] RODOTÀ S., Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali, in Riv. Crit. Dir. Priv., 1997, p. 558.

Pertanto, alla luce dell'analisi dell'impianto normativo della legge numero 675/96, si può concludere che il trattamento dei dati personali non è riconducibile soltanto al soggetto al quale si vuole difendere il diritto alla *privacy*, ma consiste nell'interesse improntato sulla lealtà e la correttezza come su qualsiasi altro rapporto giuridico tra le parti.

Se consideriamo valida l'ottica del trattamento dei dati personali e l'instaurazione di un rapporto giuridico obbligatorio tra il titolare e l'interessato, ciò comporta una serie di obblighi in capo ai soggetti coinvolti.

Nonostante l'articolo inizi con chiunque, si tratta dunque di soggetti obbligati al rispetto di determinate condotte che però possono essere ricoperte soltanto da particolari soggetti e quindi il precetto penale si riferisce a coloro che ricoprono il ruolo specifico indicato dalla legge.

Per tali motivi, vengono definiti reati propri, ossia che possono essere commessi solo da chi possiede una data qualifica ed occupa una determinata posizione giuridica.

Probabilmente sarebbe stato più adeguato attribuire alla legge 675/96 il ruolo di legge speciale per quanto concerne il trattamento dei dati personali con le dovute sanzioni amministrative ed inserire anche le disposizioni penali.

In conclusione da un'analisi della normativa in argomento si rileva la mancanza di completezza ed esaustività della disciplina della legge 675/96, infatti successivamente furono introdotte altre leggi, sempre nel settore del diritto alla protezione, alla riservatezza, all'identità personale, che prese il nome di codice della *privacy.*

6. Il d.lgs. n. 196 del 30 giugno 2003 "Codice in materia di protezione dei dati personali"

Nel gennaio del 2004, con il D.L.gs n. 196/2003 entrò in vigore il codice della *privacy,* il quale aveva l'obiettivo di sistemare e fare ordine sulla ormai stratificata normativa relativa al trattamento dei dati personali.

La tutela della protezione dei dati personali assurgeva pertanto, ad una figura giuridica indipendente, slegata da influenze esterne accostandosi però, all'esigenza di tutelare un diritto più esteso, ossia il diritto alla dignità personale di ogni essere umano.

La *ratio legis* della normativa in argomento introdotta nel 2003 cercava dunque, di trovare un equilibrio tra la correttezza relativa alla raccolta e al trattamento dei dati personali e la necessaria circolazione degli stessi senza pregiudicare l'avente diritto. [52]

Il D.L.gs n. 196/2003 al momento in cui fu emanato, disciplinava i rapporti giuridici sia delle persone fisiche che delle persone giuridiche, prevedendo per entrambi una tutela per il trattamento dei dati molto contenitiva e restrittiva.[53]

Il codice della *privacy* era composto fondamentalmente da tre parti: dall'art. 1 all'art. 45 disciplinava le disposizioni generali, dall'art. 46 all'art. 140 prevedeva le disposizioni relative a specifici settori, ed infine dall'art. 141 all'art. 186 riguardava la tutela dell'interessato e le sanzioni.

Come già in precedenza anticipato l'articolo 2 del decreto in argomento, mira a garantire il trattamento dei dati personali nel totale rispetto dei diritti inalienabili e delle libertà fondamentali, della riservatezza, della dignità personale, così come espressamente disciplinato dalla Costituzione italiana,

---

[52] MANNA A., Prime osservazioni sul testo unico in materia di protezione dei dati personali: profili penalistici, par.1, su www.privacy.it/archivio/manna20031125.html.

[53] BOLOGNINI L. PELINO E., Codice privacy: tutte le novità del d.lgs. 101/2018, Milano, 2019, 950 Cfr. D.L. 201/2011, convertito nella L. 214/2011, il quale ha limitato l'applicazione della predetta normativa alle sole persone fisiche (ivi compreso l'ambito professionale), con ciò procedendo ad eliminare l'obbligo di implementazione per i dati personali dei soggetti con personalità giuridica, nell'ottica di un processo di semplificazione della macchina burocratica ed in considerazione del fatto che i dati afferenti alle persone giuridiche risultano già, per legge, essere per lo più pubblici.

ed inoltre, ribadisce che il diritto alla protezione dei dati personali assurge a diritto autonomo rispetto agli altri diritti.[54]

Inoltre, all'articolo 3 del predetto decreto[55] viene introdotto un particolare elemento innovativo, consistente nell'utilizzo di sistemi informatici capaci di gestire i dati in modo legittimo, poiché programmati con particolari meccanismi di sicurezza e finalizzati a perseguire gli obiettivi consentiti dalla legge, senza essere invasivi nei confronti dell'interessato e soprattutto senza recare pregiudizio alla sua immagine e alla sua riservatezza.

In particolar modo l'articolo 11 del D.lgs. n. 196/2003 sancisce che la predetta attività di trattamento dei dati deve avvenire secondo i principi di correttezza e liceità.

Dalla lettura dell'articolo 11 sembra che il legislatore abbia voluto descrivere l'attività di trattamento dei dati con due sinonimi, "correttezza e liceità" invece, i predetti termini, hanno due differenti significati.

Il termine liceità fa riferimento alla circostanza secondo la quale, i dati devono essere trattati in relazione ai principi espressamente stabiliti dalla normativa in argomento, invece, con il termine correttezza il legislatore ha voluto esprimere la necessità di contemperare gli interessi tra il titolare del trattamento dei dati e l'interessato.

Soffermandoci ancora sul contenuto dell'articolo 11 del codice della *privacy* si evince il principio di minimizzazione dei dati, ossia l'utilizzo degli stessi esclusivamente per il raggiungimento degli scopi e delle finalità per i quali erano stati acquisiti, con l'obbligo di effettuare secondo i principi di trasparenza la loro conservazione soltanto per il tempo necessario al

[54] G., Commento breve al D.LGS.VO N. 196/ 2003. Codice in materia di protezione dei dati personali, 5, su https://www.diritto.it/archivio/1/20807.pdf.

[55] l'art. 3 del Codice privacy, rubricato «Principio di necessità nel trattamento di dati», il quale afferma che «I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità».

trattamento, con il consenso scritto dell'avente diritto se riguardano dati sensibili.[56]

I soggetti facenti parte del rapporto giuridico che si instaura a seguito del trattamento dei dati personali indicati nel codice della *privacy* sono: il Titolare, il Responsabile, gli Incaricati, l'interessato ed il Garante.

Per quanto riguarda il titolare, questo si può identificare con una persona fisica o giuridica, la pubblica amministrazione o in qualsiasi associazione o ente, il quale insieme ad altro titolare sono competenti per le scelte da intraprendere relativamente agli strumenti da adoperare per lo svolgimento delle modalità del trattamento dei dati personali, incluso i sistemi di sicurezza.

Il Titolare, dunque, costituisce il primo soggetto nei confronti del quale nascono le prime responsabilità ed i primi obblighi di legge.

Il Responsabile può essere come nel caso del titolare, una persona fisica, giuridica, la pubblica amministrazione o un altro organismo, che viene nominato dal titolare per supportarlo nel trattamento dei dati personali.

Un'altra figura ancora, attinente all'aspetto attivo del rapporto giuridico è l'incaricato, il quale è una persona fisica che viene autorizzata dal titolare e qualche volta anche dal Responsabile a compiere le operazioni necessarie di trattamento dei dati personali.[57]

L'interessato invece, è il soggetto passivo del rapporto giuridico in questione è la persona fisica a cui si riferiscono i dati del trattamento quindi l'avente diritto.[58]

Infine, un'altra figura di particolare importanza è il Garante, che è un'autorità pubblica autonoma, introdotta con la legge numero 675 del 1996, il quale ha il compito di controllare che l'attività del responsabile e del titolare del trattamento dei dati personali, sia corretto e illecito ed eventualmente irrorare delle sanzioni penali o amministrative.

---

[56] MANNA A., Codice della privacy: nuove garanzie per i cittadini nel Testo unico in materia di protezione dei dati personali, in Diritto Penale e Processo, 2004.
MODESTI G., Commento, cit., p. 5; MANNA A., Prime osservazioni, cit., par. 1.

[57] Articolo 4, comma 1, lettera h) Codice privacy.

[58] Articolo 4, comma 1, lettera i) Codice privacy.

Dall'analisi del codice della *privacy* ante riforma emerge che la seconda parte mira a tutelare gli strumenti e i sistemi di gestione e di controllo del trattamento dei dati personali al fine di attuare la garanzia espressamente prevista dalla legge.

Nella terza parte invece, il codice della *privacy* prevede l'applicazione di sanzioni amministrative e penali nei confronti di chi si è reso responsabile di un comportamento illecito e contrario alle norme di legge, pregiudicando l'interessato.

L'obiettivo è quello di inserire un sistema sanzionatorio più valido, dissuasivo, strettamente collegato e proporzionato alle violazioni commesse.

Ad ogni modo l'originario decreto sulla privacy del 2003 rimane in vigore anche se è stato molto modificato ed integrato con nuove normative che in prosieguo verranno esaminate.

7. La nozione di dato personale

Lo strumento giuridico per eccellenza della normativa sulla *privacy* è il dato personale, il quale consiste in tutte quelle informazioni dirette o indirette che identificano o rendono identificabile una persona fisica, attraverso la conoscenza delle sue abitudini, del suo stile di vita, del suo stato di salute, della sua situazione economica, e di tutto ciò che riguarda il suo patrimonio personale.

Nella già menzionata prospettiva i legislatori nazionali e comunitari lavorano al fine di proteggere l'insieme di tutti i diritti connessi all'identità personale e alla riservatezza di ogni essere umano.

Pertanto, qualunque informazione che si riferisca anche indirettamente ad una persona fisica identificata o identificabile anche con riferimento ad altre informazioni che apparentemente possono non fornire in maniera completa ed immediata informazioni, viene definito dato personale.

A tal proposito è opportuno precisare che i dati personali si riferiscono ad una persona chiamata "interessato" e può essere soltanto una persona fisica e non giuridica.

Infatti, con la parola personale si intende la possibilità di identificare un soggetto attraverso i dati acquisiti o da acquisire.[59]

L'identificazione consente di individuare con certezza un soggetto e di distinguerlo da un altro, ad esempio i c.d. "cookie", che spesso incontriamo quando navighiamo su internet, ai quali mettiamo un click, sono considerati dati personali, poiché attraverso il browser si possono acquisire dati ed informazioni relative al soggetto che naviga in rete.

Da ciò si può dedurre che il dato personale è assolutamente un concetto dinamico, nel senso che ha una particolare importanza ed influenza il contesto nel quale viene acquisito, poiché anche se si è in possesso di un'unica informazione che di per sé non è sufficiente ad identificare un soggetto, può essere adoperata per conoscere attraverso un controllo incrociato altre informazioni utili per l'identificazione, per tali motivazioni, assurge lo stesso a dato personale anche una informazione apparentemente non completa.

I dati personali si differenziano in varie tipologie di appartenenza, in relazione alle loro caratteristiche e per tali motivi vengono trattati con regole differenti, in ragione della categoria e della forza di incidere nella vita dell'interessato.

Inoltre, i dati personali sono definiti comuni e mai anonimi, poiché i dati comuni riguardano le informazioni che identificano il soggetto come il nome, il cognome, il codice fiscale e l'indirizzo, mentre vi sono altri dati che non posseggono il requisito dell'identificabilità, in quanto vengono soltanto associati a quelli comuni e da soli non ricoprono la veste di dato personale.

La categoria dei dati giudiziari, ad esempio consiste nell'iscrizione nel casellario giudiziario, iscrizione all'anagrafe delle sanzioni amministrative

[59] LAMANUZZI M. Diritto penale e trattamento dei dati personali.

dipendenti dal reato e il loro trattamento può essere permesso soltanto dietro autorizzazione di un provvedimento del Garante o di una disposizione di legge che indichi le motivazioni e le finalità di tale trattamento.

All'interno dei dati personali si individuano i dati sensibili che si riferiscono a elementi strettamente personali come le opinioni politiche, la religione professata, l'appartenenza sindacale, i dati genetici relativi alla salute, alla vita sessuale e all'orientamento sessuale della persona, questi ultimi sono considerati dati super sensibili, poiché sono gli unici ai quali non è concesso trattarli se non dietro autorizzazione e consenso dell'interessato.[60]

Nello specifico sono considerati dati sensibili, i dati che riguardano caratteristiche genetiche ereditarie, dati biometrici e tutto ciò che è relativo alla vita sessuale e alla salute di un individuo.

Infatti, a tal proposito il GDPR disciplina una tutela differente e maggiore nei confronti dei dati sensibili, sulla base dei principi stabiliti dalla Costituzione, poiché non si tratta di dati di carattere neutrale, ma con caratteristiche strettamente riservate alla vita dell'individuo che non possono essere facilmente resi di pubblico dominio, tenuto conto che l'utilizzo improprio di tali dati potrebbe causare pregiudizi e danni alla dignità personale e alla riservatezza dell'interessato.[61]

---

[60]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»

[61] MARTORANA M., BARBERISI A., PIZZETTI F., *GDPR*, cit., 4. Ebbene, stante il radicamento dei social-network nella società attuale, è questo uno dei casi più comuni, di dati strettamente sensibili che vengono ad essere resi pubblici dallo stesso interessato. È proprio attraverso i social che il soggetto si trova ad esprimere proprie idee ed appartenenze politiche, a dare informazioni sul proprio stato di salute o sul proprio orientamento e vita sessuale, andando, in tal modo, a rendere pubblici quei dati che, poiché strettamente inerenti alla propria persona, alle proprie idee ed orientamenti, la normativa dell'Unione e dello stato membro vieterebbe a chiunque di trattare e dunque far circolare.

Un'altra tipologia di dati è quella c.d. "dati semi- sensibili", che riguardano ad esempio i nominativi inseriti nelle *black list*, e tutti quei dati attinenti alla situazione patrimoniale dell'interessato definita come *tertium genus* il cui trattamento in modo scorretto e non autorizzato potrebbe arrecare parecchi danni all'avente diritto.

8. Il ruolo del Garante nel trattamento del dato personale.

L'autorità Garante, la cui costituzione fu per la prima volta prevista dalla Direttiva 46/94/CE, aveva il ruolo di proteggere i dati personali delle persone fisiche.

A tal proposito è di preminente importanza evidenziare l'introduzione nel 2007 dell'art. 16 TFUE e nel 2000 l'art. 8 della Carta di Nizza, le quali normative prevedevano la costituzione di Autorità indipendenti per ciò che riguardava il diritto alla tutela dei dati personali.

Con il Regolamento UE si è potuto costituire un sistema di Controllo e Vigilanza unitario, strutturato in maniera omogenea ed avente un'uniformità normativa che era prescritta dal Regolamento stesso.

In particolare, ogni Stato membro, ha la facoltà di attuare un vigile controllo che non si limita soltanto all'interno dei confini nazionali, ma un controllo dinamico, non rilegato esclusivamente alla mera sorveglianza passiva, ma posto in essere da soggetti attivi che ricoprono delle specifiche funzioni all'interno del trattamento.[62]

All'Autorità, sono attribuiti poteri preventivi al fine di evitare comportamenti che possono ledere i diritti dell'interessato sia durante l'istruttoria che a posteriori, poteri che si esprimono attraverso l'emissione di

[62] RICCIO G. M., SCORZA G.., op. cit., 429. Gli Autori mettono in luce come già l'art. 286 del TCE, introdotto con il Trattato di Amsterdam del 1997, facesse riferimento all'Autorità di controllo nell'ottica di impostazione di un sistema di vigilanza che rendesse effettiva e reale la tutela dei dati personali così come riconosciuta dal diritto dell'Unione**.**

autorizzazioni e prescrizioni con la competenza di svolgere la funzione di arbitro.

Una particolare peculiarità dell'Autorità di Controllo è l'indipendenza, che consiste nella facoltà di poter svolgere con un margine di discrezionalità e senza essere sottoposto ad altri organi sovraordinati, la propria funzione di tutela nei confronti delle persone fisiche.

Inoltre, la predetta indipendenza può essere di tipo funzionale e finanziario.

L'indipendenza funzionale, si caratterizza per l'attribuzione in capo al Garante di un potere autonomo, in questo modo il Garante può adottare una condotta più incisiva nei confronti delle altre parti, non essendoci nessun organo superiore che possa controllarlo o gestirlo, tale autonomia funzionale, come poc'anzi accennato, necessita anche di un'autonomia finanziaria che permette al Garante di poter svolgere appieno il suo operato in piena autonomia e indipendenza finanziaria.

Pertanto, dalla lettura del Regolamento[63] si evince che l'Autorità è un organismo pubblico e che deve avere una propria indipendenza finanziaria, per cui ogni Stato ha le proprie entrate che servono per finanziare l'autorità di controllo, oltre ad attingere ad eventuali finanziamenti pubblici europei.

A tal proposito l'articolo 54 del Regolamento prevede in particolare che ogni Stato membro ha il compito di introdurre una legge nel proprio ordinamento giuridico che disciplini l'Autorità di Controllo, stabilendo le risorse necessarie per l'assolvimento delle sue funzioni, che devono fondamentalmente coincidere con le disposizioni espressamente previste dal Regolamento.

Per tali motivi, il legislatore europeo ha conferito dei poteri molto ampi di autonomia al legislatore nazionale soprattutto in tema di Autorità di controllo, in maniera tale che ogni Stato membro possegga la propria normativa di

[63] Art. 52 GDPR "indipendenza": Ogni Stato membro provvede affinché ogni autorità di controllo sia soggetta a un controllo finanziario che non ne pregiudichi l'indipendenza e disponga di bilanci annuali, separati e pubblici, che possono far parte del bilancio generale statale o nazionale.

riferimento che si inserisca in maniera armonica nel proprio contesto socio giuridico inserendosi nel tessuto sociale e rispettando le caratteristiche e le peculiarità di ogni singolo Stato.

In Italia il legislatore nazionale, sulla scorta dell'autonomia concessagli dal legislatore comunitario in materia del trattamento dei dati personali, ha introdotto il decreto legislativo n. 101/2018 che ha novellato il decreto legislativo n. 196/2003 e ha delineato così il ruolo del Garante secondo le disposizioni espressamente stabilite nel Regolamento ritenendolo un punto di riferimento.

Pertanto, in Italia il Garante e l'Autorità di Controllo sono indipendenti e hanno la funzione di regolamentare e gestire la corretta applicazione delle disposizioni interne in correlazione con quelle comunitarie, in tema di protezione dei dati personali.

Il Garante nella sua composizione è formato da un organo di vertice che è il collegio che è costituito da quattro componenti che sono eletti per metà dalla camera di deputati e per metà dal Senato, dopo la formazione del predetto collegio viene nominato il presidente ed il vicepresidente, tutti i componenti del collegio durano in carica sette anni e devono essere persone di comprovata esperienza sul settore, affinché l'organo possa funzionare in maniera corretta e competente.

Compito precipuo del Garante è quello di assicurare che il trattamento dei dati sia effettuato con liceità e correttezza e quindi in maniera conforme alle regole dell'ordinamento giuridico sia interno che comunitario.

In particolare il decreto legislativo n.101/2018 a tal proposito ha modificato l'articolo 2 *septies* conferendo al Garante la competenza di poter gestire misure di garanzia molto delicate come il trattamento di dati genetici, biometrici e sanitari.

Invece, per quanto riguarda la funzione del Garante relativamente al controllo preventivo della tutela dei dati personali, così come sancito dal Regolamento, risulta essere stato compromesso dal decreto Capienze, poiché è stato abrogato l'articolo *2 quinquiesdecies* del decreto legislativo 196 del 2003.

Prima dell'abrogazione di tale articolo, la norma prevedeva che il Garante avesse il potere di emanare provvedimenti di carattere generale, ma anche di carattere preventivo, ossia la pubblica amministrazione poteva consultare il Garante prima di effettuare l'emissione di un provvedimento che riguardava il trattamento di dati personali ad alto rischio, affinché il Garante potesse intervenire a tutela del soggetto interessato.

Con l'abrogazione dell'articolo *2 quinquiesdecies* del D.lgs. 196/2003 in argomento, il Garante non ha più alcun potere di intervento in maniera preventiva al fine di correggere eventuali errori o situazioni ad alto rischio ed eventualmente a riequilibrare le posizioni del soggetto interessato e della pubblica amministrazione in cui quest'ultima nel rapporto con il cittadino ha sempre per sua natura una posizione di vantaggio.

Pertanto, al fine di Garantire effettivamente la tutela dei dati personali all'avente diritto, in ordine alla libertà e alla correttezza dei dati sensibili, si è di recente avvertita in Italia la necessità che il Garante intervenga per bloccare provvisoriamente alcuni provvedimenti attuati dalla pubblica amministrazione, in maniera tale da colmare la lacuna legislativa formatasi a seguito dell'abrogazione dell'articolo *2 quinquiesdecies* del D.lgs. 196/2003 di cui sopra.

Continuando con la disamina della figura del Garante è importante fare riferimento al decreto legislativo n. 101/2018, il quale attraverso le modifiche apportate al codice della *privacy* ha ampliato le competenze del Garante, mediante le quali è possibile che quest'ultimo possa trovare un equilibrio tra la protezione e la circolazione dei dati personali, attraverso poteri autorizzativi che gli consentono il riutilizzo dei dati già trattati, qualora diventi impossibile o difficile informare gli interessati sarà il Garante a prestare l'autorizzazione al riutilizzo degli stessi per le medesime finalità.

Pertanto il Garante qualora abbia accertato la presenza di difficoltà o pregiudizi nella gestione dei dati personali, nel caso in cui sia necessario riutilizzare i dati dell'avente diritto già posseduti, il Garante è abilitato ad esercitare come gli altri soggetti attivi del rapporto un'attività a carattere

preventivo consistente nel riutilizzo dei predetti dati sulla base dei principi di liceità e correttezza. [64]

Si evince pertanto che l'Autorità Garante svolge un ruolo fondamentale nella protezione e tutela dei dati personali, attraverso anche la continua collaborazione con i soggetti interessati, con il titolare e con il responsabile, mediante i quali, nel rispetto della normativa svolge un'attività di interazione e collaborazione ove richiesto dalla fattispecie.

Il Garante nella sua funzione di guida al fine di garantire la tutela dei dati personali ha un ruolo trasversale, nel senso che le sue funzioni non si limitano soltanto dentro i confini nazionali ma anche nel rispetto del Regolamento partecipando alle attività dell'Unione Europea ed internazionale.

Inoltre, dopo le ultime modifiche apportate al codice della *privacy* da parte del decreto Capienze c'è stato un ulteriore ridimensionamento dei poteri del Garante, soprattutto come abbiamo già accennato, in ordine alla sua funzione preventiva nei riguardi della pubblica amministrazione.

A tal proposito il Consiglio dei Ministri ha statuito che nei casi di necessità e d'urgenza anche se non è prevista un'attività preventiva del Garante è possibile che quest'ultimo possa intervenire in una fase successiva al fine di esprimere il proprio parere riequilibrando la fattispecie del caso concreto.[65]

Dunque, nonostante i poteri preventivi del Garante siano stati ridimensionati, in alcune fattispecie particolari, possono trovare attuazione mediante il parere espresso del Presidente dal Consiglio dei Ministri dal quale ormai dipendono.

Un'altra importante funzione conferita al Garante consiste nel predisporre una relazione annuale sull'attività svolta, relativamente al trattamento dei dati personali sul territorio nazionale e anche per quanto avvenuto in territorio

---

[64] BOLOGNINI L., BISTOLFI C., PELINO E., Il regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali, Milano, 2016

[65] MARTORANA M., BARBERISI A., PIZZIMENTI F., OP. CIT., P. 117. 271
BOLOGNINI L., BISTOLFI C., L. PELINO E., OP. CIT., PP. 622 E SS. 272

europeo e internazionale, la predetta relazione verrà trasmessa al Parlamento ed al Governo italiano, in modo tale da tracciare una linea di condotta che il Governo può eventualmente analizzare ed intervenire.

Il Garante, invece continua a mantenere una funzione preventiva nei confronti del titolare e del responsabile del procedimento relativo al trattamento dei dati personali.

A tal proposito, il Garante ha la facoltà di emettere dei pareri vincolanti, qualora abbia accertato la presenza di violazioni poste in essere da parte del titolare e del responsabile con la conseguenza di irrogare a questi ultimi, se necessario, delle sanzioni.

Inoltre, il Garante ha anche il potere di accedere ai dati che sono stati elaborati e trattati dal titolare e dal responsabile e nel caso in cui dovessero emergere delle difformità rispetto alla normativa, il Garante ha facoltà di sollecitare il titolare ed il responsabile a correggere eventuali difformità rispetto alle disposizioni vigenti ed eventualmente a fissare un termine entro il quale i predetti soggetti attivi devono definire in maniera corretta il trattamento dei dati su cui il Garante ha rilevato la difformità.[66]

Nel caso in cui l'interessato venga a conoscenza delle difformità relative ai propri dati personali, come nella fattispecie di cui sopra, può proporre reclamo al Garante, facendo presente le violazioni che ha rilevato a norma dell'articolo 77 del Regolamento UE 2016/679 e degli articoli 140 *bis* e 143 del codice della *privacy,* così come modificato dal decreto legislativo n. 101/2018.

Successivamente alla proposizione del reclamo si instaurerà un procedimento amministrativo caratterizzato da una fase istruttoria in cui il Garante emetterà un provvedimento tenendo conto anche dell'articolo 58 del Regolamento.[67]

Il provvedimento emesso dal Garante potrà essere oggetto di impugnazione mediante la proposizione di un ricorso giurisdizionale ai sensi

---

[66] I provvedimenti del Garante possono essere impugnati davanti all'Autorità Giudiziaria. 268 MARTORANA., OP. CIT., P. 117.

[67]

degli articoli 143 e 152 del codice della *privacy* e dell'articolo 78 del Regolamento.

Per quanto riguarda gli articoli 140 e 142 del codice della *privacy,* si ritiene che il reclamo sia il mezzo di tutela più efficace in caso di violazione dei diritti dell'interessato e può essere presentato da parte dell'avente diritto direttamente al Garante dimostrando i propri diritti violati.

Diversamente rispetto a ciò che avveniva in precedenza l'interessato poteva presentare eventuali lamentele solo al titolare e al responsabile e in caso di diniego decorso 15 giorni, potevano proporre reclamo nei confronti del Garante.[68]

Invece, adesso è possibile proporre ricorso direttamente al Garante, il quale accerterà i requisiti del caso concreto e procederà all'archiviazione o all'instaurazione di un procedimento amministrativo con la relativa istruttoria, volta ad accertare la fondatezza e la legittimità della richiesta avanzata dall'interessato.

A tal proposito l'articolo 83 del GDPR che ha novellato l'articolo 186 del codice della *privacy* indica le sanzioni con cui l'autorità Garante[69] dovrà

---

[68] BOLOGNINI L., BISTOLFI C., L. PELINO E., op. cit., 814 e ss.

[69] 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

attenersi nell'adozione dei provvedimenti che emetterà, poiché i provvedimenti sanzionatori dovranno basarsi sull'effettività, sulla dissuasività e sulla proporzionalità relativa al momento della commissione od omissione del reato, con la conseguente applicazione di una sanzione che seguirà i criteri indicati dalla normativa.

Tali criteri riguardano la gravità, la durata, la tipologia della violazione, la natura e la tempestività con cui i soggetti attivi si sono attivati per porre rimedio i predetti criteri sopra elencati, saranno presi in considerazione dal Garante e valutati, tenendo conto anche del numero degli interessati e degli eventuali danni subiti.

Le modalità di applicazione del sistema sanzionatorio sono espressamente previste dal GDPR, le quali sono volte anche ad appurare l'eventuale presenza di dolo o colpa in capo all'autore del reato, ossia dell'elemento psicologico del reato.[70]

Dall'azione o dall'omissione posta in essere dall'autore della violazione, il Garante potrà effettuare una valutazione al fine di stabilire la sanzione più opportuna al caso concreto.

Infatti, a tal proposito il Garante essendo titolare di una funzione sanzionatoria potrà valutare la tipologia del dato personale violato e qualora questo si configuri come dato ad alto rischio o particolarmente sensibile, potrà applicare le sanzioni specifiche in ordine alla circostanza.

---

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.

[70] MARTORANA M., BARBERISI A., PIZZIMENTI F., OP. CIT., P. 117. 271 BOLOGNINI L., BISTOLFI C., L. PELINO E., OP. CIT., PP. 624.

Infine, il Garante nell'esercizio dei suoi poteri investigativi e di controllo, può avvalersi dell'attività collaborativa della Guardia di Finanza, soprattutto per svolgere determinati indagini qualora il Garante sia a conoscenza di una *notitia criminis*.

La figura del Garante, è altresì impegnata nella tutela del dato personale non soltanto sul piano amministrativo, ma anche sotto l'aspetto penale nel senso che collabora alle indagini e alle attività investigative che di volta in volta si rendono necessarie.

Sul punto il codice *privacy* prevede che il Pubblico Ministero possa informare l'Autorità di controllo in ordine ad un fatto previsto come violazione al codice della *privacy* o del GDPR.

Da ciò si evince l'importanza delle funzioni del Garante all'interno del sistema penale e della tutela dei dati personali, con un meccanismo di collegamento per evitare che ci siano sovrapposizioni nel processo amministrativo e in quello penale rispettando il principio del *ne bis in idem*.[71]

Inoltre, la figura del Garante ha spinto il legislatore delegato ad introdurre delle figure delittuose disciplinate ai sensi dell'articolo 168 e 170 del codice della *privacy* che riguardano le false dichiarazioni rese al Garante o interruzione all'esecuzione dei compiti ed intralcio all'esercizio di poteri del Garante.

Ciò posto, alla luce delle argomentazioni sopra rappresentate l'obiettivo della normativa italiana e di quella comunitaria è di tutelare il trattamento dei dati personali, per tali motivi il Garante in Italia assume un ruolo principale, poiché possiede dei poteri che gli consentono di assumere una posizione attiva e di controllo.

[71] È necessario che il reclamo contenga: una descrizione quanto più dettagliata possibile dei fatti e delle circostanze su cui si fonda; l'indicazione delle disposizioni che si presumono essere state violate e delle misure richieste; gli estremi identificativi del titolare e del responsabile (ove quest'ultimo sia conosciuto); la documentazione utile e necessaria ai fini della valutazione del reclamo da parte dell'Autorità Garante; l'eventuale mandato ed un recapito per l'invio delle comunicazioni (di fondamentale importanza quest'ultimo proprio in considerazione del fatto che uno dei motivi per impugnare i provvedimenti del Garante, emessi a seguito di reclamo, è proprio la mancata comunicazione del provvedimento all'interessato).

In conclusione, possiamo affermare che l'attuazione del decreto legislativo n. 101/2018 ed il Regolamento 2016/679, hanno contribuito ad estendere il novero dei poteri del Garante con l'obiettivo di apprestare una tutela sempre più incisiva per i diritti dell'interessato.

9. La tutela dei dati personali nell'Unione europea e il Regolamento UE n. 2016/679

La tutela dei dati personali nel diritto comunitario è disciplinata dal Regolamento UE n. 2016/679 (di seguito, il "Regolamento" o "GDPR"), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Adottato dal Consiglio e dal Parlamento europeo in data 27 aprile 2016 e definitivamente reso operativo dagli Stati membri il 25 aprile 2018.

A tal proposito l'articolo 8 della Convenzione Europea dei diritti dell'uomo in seguito chiamata CEDU[72] è uno degli strumenti di carattere sovranazionale, mediante il quale, si stabilisce che ogni individuo ha diritto a vedere rispettata la propria sfera di azione privata, attraverso il bilanciamento dei vari diritti che sono tutelati dall'ordinamento giuridico.[73]

Lo stesso enunciato è contenuto nella Carta dei diritti fondamentali dell'Unione Europea emanata a Nizza nel 2000, chiamata in seguito Carta.

A tal proposito l'art. 7 prevede che ogni soggetto ha diritto al rispetto della propria sfera privata del proprio domicilio e delle proprie comunicazioni. [74]

---

[72] Art. 8 CEDU par.2: «*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 alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui*».

[73] LAMANUZZI M., Diritto penale e trattamento dei dati personali. I reati previsti dal Codice della privacy e la responsabilità amministrativa degli enti alla luce del regolamento 2016/679/UE, in IusOnline, 1/2017

[74] RODOTÀ S., Tecnologie, cit., 101 ss. RODOTÀ S., Intervista su privacy e libertà, Bari, 2005. 28 RODOTÀ S., *Discorso di presentazione della Relazione annuale del Garante al Parlamento*, anno 2001. In tale occasione, l'allora Presidente del Garante asseriva che: «*[...] 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*

Sia nella CEDU che nella Carta è enunciato il principio del rispetto della vita privata che si basa sulla protezione dei dati personali.

Il diritto alla protezione dei dati personali è espressamente disciplinato dall'articolo 8 della Carta[75], relativamente all'ordinamento europeo, e costituisce una fonte dalla quale si può identificare una distinzione tra due elementi quello dei dati personali da proteggere e quello della *privacy.*

Il predetto articolo 8 prevede la presenza di una particolare figura che è il Garante per il controllo del rispetto delle norme ivi indicate, e la concisa definizione del fulcro essenziale dei diritti fondamentali dell'uomo alla protezione dei dati personali.

La tutela del diritto in argomento trova il suo fondamento nell'ambito dell'ordinamento giuridico italiano nell'alveo dell'articolo 2 della Costituzione, nel quale la protezione dell'essere umano e della sua identità personale, trovano stretta connessione col principio di dignità umana espressamente sancito dall'articolo 2 e 3 della Costituzione.

Oggi a causa della globalizzazione e dell'evoluzione sociale ormai tutta informatizzata si è verificato un ampliamento dei confini del concetto di dignità personale e conseguente tutela dei dati personali.

I predetti dati possono essere trattati soltanto per le finalità concordate e con il consenso della persona titolare che ne può disporre.

Ogni soggetto ha il diritto di accedervi ed utilizzarli ed eventualmente di intervenire apportando modifiche.

A ciò va aggiunta la possibilità di riconnettere i principi sulla libertà personale, ossia la libertà di manifestare le proprie idee, come libertà e tutela dei dati personali, poiché la tutela dei dati personali comporta la protezione di tutti i diritti fondamentali dell'essere umano.

---

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». LAMANUZZI M., Diritto penale e trattamento dei dati personali, cit.

[75] Art. 8 Carta dei Diritti Fondamentali dell'Unione Europea: «1. *Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.*

Appare pertanto evidente che in una società basata ormai sulla tecnologia informatica, l'individuo è identificato attraverso i suoi dati personali, per tali motivi il rispetto della persona umana risiede principalmente nella protezione di tali dati che lo caratterizzano.[76]

In Italia la Legge n. 675 del 31 dicembre 1996, ha consentito nel nostro paese, l'ingresso della Direttiva europea 95/46/CE, del 24 ottobre 1995 (definita anche "Direttiva madre"), emessa dal Parlamento e dal Consiglio dell'Unione Europea, con lo scopo di proteggere e di consentire una corretta circolazione dei dati personali delle persone fisiche. [77]

L'uscita di scena della legge 675/96, è avvenuta ad opera del decreto legislativo 196/2003 riguardante il "Codice della privacy" che mira a dare un ordine alla materia in argomento, cercando di dare un segnale forte alla definizione e tutela dei dati personali.[78]

Ma ciò che più di ogni altra norma garantirà l'effettività dei diritti sanciti, sarà la consapevolezza della diffusione della "cultura della *privacy"* necessaria per promuovere, ad un tempo, lo sviluppo economico, la libertà, l'efficienza amministrativa e la dignità dell'essere umano.

La predetta Direttiva ha permesso che le normative dei paesi aderenti all'Unione, si uniformassero rispettando le libertà e i diritti fondamentali in essa sottesi.[79]

La predetta legge 675/96, aveva l'obiettivo di riconoscere al concetto di *privacy* e al diritto alla riservatezza la veste di diritto assoluto ed inviolabile, la cui violazione comportava l'applicazione di pesanti sanzioni di natura civile, penale ed amministrativa.

---

[76] BONFANTI M. E., *Il diritto alla protezione dei dati personali nel Patto internazionale sui diritti civili e politici e nella Convenzione europea dei diritti umani: similitudini e difformità di contenuti*, 2011, p. 44537 MORTATI C., *Istituzioni di diritto pubblico*, Padova, 1975, 1038 ss.

[77] BONFANTI M. E., *Il diritto alla protezione dei dati personali*, CIT., 447.
LAMANUZZI M., Diritto penale, CIT., 226.

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

[79] FINOCCHIARO G., La protezione dei dati personali in Italia: regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101, Bologna, 2019, 12. paese, alla difesa dell'ordine e alla prevenzione dei reati, alla 31

Il Codice (D. lgs. 196/2003), ha abrogato la legge precedente rivisitando l'intera disciplina sul trattamento dei dati personali, al fine di aggiornare la normativa sulla tutela dei dati personali.

Ciò per fare fronte agli innumerevoli interventi tecnologici e per creare un'armonia a livello normativo nei vari Stati membri dell'Unione, poiché si era creata una certa disomogeneità, probabilmente a causa del margine di libertà che ogni Stato aveva nelle modalità di applicazione della normativa, per cui soltanto con l'introduzione del Regolamento nel 2016 si è risolto il problema, uniformando la legislazione dei diversi Stati membri e si ebbe una situazione di maggiore armonia all'interno della normativa sulla *privacy* a livello europeo e nazionale.

Nel 2016 venne emanato il Regolamento UE 2016/679, più conosciuto come Regolamento generale sulla protezione dei dati (GDPR).

Tale Regolamento ha le caratteristiche di legge generale rispetto alla Direttiva UE 2016/680 ed alla Direttiva UE 2016/681.

La successiva Direttiva UE 2016/680 regola la raccolta e la gestione effettuata da autorità competenti per la tutela del trattamento dei dati personali, con lo scopo di effettuare indagini e accertamenti su eventuali reati e l'applicazione di sanzioni penali, nonché in ordine alla libera e regolare circolazione di tali dati.

La Direttiva UE 2016/681 riguarda, invece, l'utilizzo del codice di prenotazione (PNR) con l'obiettivo di prevenire e perseguire la commissione di reati gravi o di terrorismo.

L'Italia in relazione alla superiore normativa ha adeguato le leggi nazionali alle disposizioni del Regolamento 2016/679 con il D.lgs. n. 101/2018 ed ha recepito le predette due Direttive con il D.lgs. n. 51/2018 e con il D.lgs. n. 139/2021**.**

Il Regolamento UE n. 2016/679 chiamato, il "Regolamento" o "GDPR", adottato dal Consiglio e dal Parlamento europeo in data 27 aprile 2016, riguarda il trattamento alla protezione e alla libertà di circolazione dei dati, i quali vengono disciplinati in maniera assolutamente paritetica riconoscendo ad entrambi pari dignità ed importanza.

Il Regolamento, è suddiviso in 11 capitoli, 99 articoli e 173 *considerandum* e come abbiamo poc'anzi enunciato, il Regolamento viene denominato con l'acronimo, GDPR (General Data Protection Regulation), finalizzato alla protezione della persona umana e alla circolazione legittima dei dati personali nell'ottica dei diritti inalienabili e delle libertà fondamentali dell'essere umano.[80]

Dalla lettura dei primi *considerandum,* si evince che l'obiettivo è quello di creare un concetto comune che sia ispirato a principi di sicurezza, di giustizia e di libertà, al fine di realizzare un'economia unica tra i vari paesi membri che possa dare benessere alle popolazioni. [81]

Infatti, il Regolamento UE 2016/679 ha l'obiettivo di ottenere il più possibile l'applicazione di varie normative giuridiche in materia di protezione di dati personali, all'interno degli ordinamenti dei paesi membri dell'Unione.

A tal proposito il Regolamento ha stabilito che gli Stati membri devono emanare disposizioni di attuazione e creare autorità di controllo vista la possibilità da parte degli Stati membri di introdurre delle modifiche, al fine di tutelare concretamente la *privacy* e la libertà di espressione.

A seguito di ciò, ogni Stato membro ha disciplinato a modo proprio la normativa sopra rappresentata, comportando una inevitabile diversità in ordine ad alcuni punti, come ad esempio in Italia, la figura del Garante viene considerata di particolare rilievo poiché gli è stata attribuita una "capacità interventista e non di mero controllo", a differenza di altri paesi come l'Irlanda, in cui la figura del Garante ha avuto maggiori difficoltà ad attecchire, e di conseguenza ha una funzione poco definita, con la conseguenza di un potere minore nello svolgimento della sua attività di gestione e di controllo dei dati.[82]

---

[80] REGOLAMENTO UE 2016/679, ART. 1.
RICCIO G. M., SCORZA G., BELISARIO E., GDPR e normativa privacy, Milano, 2018.
COSTANTINI F., Il Regolamento (UE) 679/2016 sulla protezione dei dati personali, Il Quotidiano Giuridico, 6, 2018.

[81] RICCIO G. M., SCORZA G., BELISARIO E., GDPR, CIT., 7.
EX MULTIS CFR. RICCIO G. M., SCORZA G., BELISARIO E., GDPR, CIT., 7-8.

[82] MALGIERI G., Inquadramento normativo, cit., 4 ss.
BOLOGNINI L., BISTOLFI C., PELINO E., Il regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali, Milano, 2016, 14 ss.

Tale flessibilità e diversità all'interno dei sistemi normativi dei singoli paesi membri ha dato maggiore opportunità al GDPR di attecchire nel tessuto legislativo relativo al tema del trattamento dei dati personali dei singoli Stati membri e di armonizzarsi con la normativa nazionale già esistente.

D'altronde non sarebbe stato possibile tagliare definitivamente le radici normative già radicate da decenni sulla tutela dei dati personali in ogni singolo ordinamento giuridico applicando *ex novo* una legislazione che non si amalgamasse con quella già esistente sia in materia amministrativa che penale, per cui la predetta flessibilità è stata senz'altro positiva.

Altre finalità possono essere dedotte dagli artt. 1 e 2 del Regolamento il quale mira alla tutela della circolazione dei dati personali soltanto nei confronti delle persone fisiche e quindi nei riguardi di tutti i diritti che sono attinenti alla sfera dei diritti inviolabili che sono strettamente legati alla natura dell'essere umano.

All'interno del Regolamento è venuto meno il concetto e il termine di vita privata, poiché l'argomento affrontato è soltanto sulla protezione dei dati ciò per rimarcare che a seguito dell'evoluzione informatica la tutela al trattamento dei dati personali ha trovato attecchimento in ogni ambito della vita sociale.

Pertanto, oggetto principale del Regolamento deve essere *la privacy* vista nella sua totalità, sia sotto l'aspetto della riservatezza, della circolazione dei dati, dell'identità personale in abrogazione della direttiva numero 95/46/CE. [83]

Inoltre, il Regolamento ha lo scopo di applicare la tutela a tutte quelle attività svolte sul web che utilizzano i dati degli utenti digitali, in relazione alle quali i titolari, ad esempio e-commerce, social network, o altre piattaforme dovranno applicare il diritto dell'Unione.

Può pertanto accadere che lo stabilimento non coincide sempre con la sede legale, ma può essere qualsiasi organizzazione stabile che svolga anche una minima attività.

---

[83] MARTORANA M., BARBERISI A., PIZZETTI F., GDPR e Decreto Legislativo 101/2018: vademecum del professionista: obblighi, adempimenti, strumenti di tutela, Milano, pp. 121 e ss.;

Lo stabilimento si può trovare all'interno di uno dei paesi dell'unione ed il trattamento dei dati può svolgersi all'interno dell'attività di tale stabilimento, ovvero lo stabilimento si può anche trovare in un paese terzo rispetto all'Unione ma il trattamento dei dati e il monitoraggio degli stessi avviene all'interno dei paesi dell'Unione.

Inoltre, il Regolamento prevede che i soggetti attivi che interagiscono nel trattamento e nella circolazione dei dati personali sono: l'interessato, il titolare ed il responsabile.

A) L'articolo 4, paragrafo 2, punto 3), del Regolamento UE 2016/679 si riferisce all'interessato come persona fisica a cui fanno riferimento i dati personali.

L'Interessato può essere soltanto una persona fisica e non anche una persona giuridica, un ente o un'associazione.

Nello specifico il concetto di interessato è cambiato con l'evoluzione della società in cui viviamo, nel senso che oggi tutti possiamo essere potenziali interessati ad un trattamento, poiché tutti siamo potenzialmente soggetti ad esempio a riprese con telecamere installate per le strade cittadine, per cui il concetto di interessato è un concetto dinamico.

Per tali motivi la normativa conferisce all'interessato dei diritti:

1) La possibilità di revocare il consenso in qualsiasi momento;

2) Ottenere informazioni su quali dati siano trattati dal titolare del trattamento;

3) Cambiare il contenuto dei dati;

4) Accedervi per conoscerne le modalità di utilizzo;

5) La possibilità di esercitare un diritto di opposizione al trattamento in tutto o solo in parte;

6) Proporre opposizione ai trattamenti automatizzati quando il trattamento non è compatibile con le finalità del consenso;

7) chiedere il blocco quando i dati sono stati utilizzati in violazione delle norme di legge.

Per l'esercizio di tali diritti, l'interessato può rivolgersi direttamente al titolare del trattamento il quale deve collaborare con l'interessato per lo

svolgimento dell'esercizio dei suoi diritti. Infine, i dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato. Le finalità devono essere determinate, esplicite e legittime.

B) L'articolo 4, paragrafo 1, punto 7), del Regolamento UE 2016/679, si riferisce al titolare la cui funzione può essere rivestita da una persona fisica o giuridica o dall'autorità pubblica che individualmente o assieme ad altri, stabilisce gli strumenti e le finalità del trattamento dei dati personali;

C) l'articolo 28 paragrafo 2 del Regolamento UE 2016/679, si riferisce al responsabile, in qualità di persona fisica o giuridica o l'autorità pubblica, tratta i dati personali per conto del titolare.

Inoltre, è previsto che il responsabile in presenza di particolari circostanze possa nominare un altro soggetto denominato sub responsabile al fine di tutelare e non interrompere in caso di proprio impedimento il trattamento dei dati personali.

L'interessato, nel rapporto giuridico con il responsabile ed il titolare, si trova in una posizione di sfavore ed il Regolamento cerca di riequilibrare le predette posizioni.[84]

Al fine di risolvere le superiori problematiche il Regolamento ha introdotto la possibilità di gestire il predetto rapporto giuridico sulla scorta del principio di *accountability* che consiste nell'attività da parte del titolare di porre in essere una condotta capace di adottare delle misure tecniche e organizzative che garantiscano e dimostrino che la procedura del trattamento dei dati personali adottata è stata effettuata in conformità e secondo i criteri espressamente stabiliti dal Regolamento, tenendo in debita considerazione i pericoli, l'ambito di applicazione, nonché i rischi in cui sono sottoposti i diritti inviolabili e le libertà fondamentali in relazione al trattamento dei dati personali.

È di palmare evidenza che il compito del titolare non è soltanto finalizzato a mettere in atto tutte le misure idonee attraverso un continuo controllo che accerti la presenza o meno di criticità, ma consiste anche nel relazionare e

[84] BOLOGNINI L., BISTOLFI C., PELINO E., Il regolamento, cit., 2-3.

dimostrare l'attuazione della procedura di trattamento dei dati personali realmente svolta.

Al fine di attuare il principio di *accountability* sopra menzionato, il Regolamento prevede agli artt. 37-39 la figura del c.d. DPO, acronimo di *Data Protection Officer*, soggetto estraneo rispetto all'interessato, al titolare e al responsabile.

Il DPO ha la funzione di fornire consulenza sulle normative e sugli obblighi di legge relativi al trattamento e protezione dei dati personali su larga scala sia al titolare che al responsabile, nonché ha un ruolo di unione tra l'Autorità Garante ed il titolare/responsabile del trattamento.

10. Altre fattispecie a tutela della riservatezza: art. 615 *ter* c.p. Accesso abusivo a sistemi informatici, 615 *quater* c.p. Detenzione e diffusione abusiva di codici di accesso, 617 *quater* c.p. Intercettazione abusiva

A tal proposito è opportuno concludere il presente capitolo con l'analisi di alcune fattispecie di reato che indirettamente tutelano la riservatezza dei dati personali.

In particolare, l'articolo 615[85] *ter* del codice penale, prevede la reclusione fino a tre anni per coloro che accedono abusivamente all'interno dei sistemi informatici protetti o continuano a rimanervi contro la volontà dell'interessato.

Nella predetta fattispecie di reato che consiste nell'accesso abusivo a sistemi informatici, il legislatore mira a tutelare due differenti fattispecie di reato, una riguarda l'intrusione abusiva da parte un soggetto che non è autorizzato all'interno di un sistema informatico violando le misure di

[85] L'art 615-*ter* c.p. prevede che "*chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni".*

sicurezza e l'altra fattispecie, invece, riguarda colui che inizialmente viene autorizzato ad entrare in un sistema informatico altrui, ma vi permane oltre il tempo consentito per scopi diversi da quelli per cui era stato autorizzato. Dall'analisi[86]della predetta norma si è potuto constatare che il soggetto attivo ai fini della configurazione del reato, non deve essere necessariamente un esperto, ossia un hacker, ma è sufficiente che sia realizzato anche da collaboratori di un'azienda che hanno avuto l'accesso per motivi lavorativi e poi sono rimasti per acquisire informazioni non autorizzate.

Infatti, il secondo comma dell'articolo 615 *ter* c.p. prevede che i soggetti che inizialmente sono autorizzati ad accedere a sistemi informatici personali, approfittino della circostanza e permangono oltre il tempo stabilito per acquisire informazioni di dati e utilizzarli in maniera illecita.

In tale circostanza è prevista un'aggravante per l'intrusione da parte di un operatore di sistema al quale si conferisce una fiducia essendo un collaboratore dell'azienda e che conosce in maniera approfondita e dettagliata i sistemi di sicurezza.

Infatti è proprio il rapporto fiduciario che viene intaccato tra il lavoratore e l'azienda, poiché entrando abusivamente utilizza codici conosciuti per motivi lavorativi e sfrutta a proprio vantaggio e a danno altrui tale circostanza.

Ad ogni modo l'articolo 615 *ter* del codice penale, prevede che tale accesso sia abusivo e quindi senza alcuna autorizzazione da parte del titolare, soltanto nel secondo comma, prevede che qualora il soggetto sia stato autorizzato e vi permanere oltre il tempo stabilito per scopi differenti da quelli per cui era stato autorizzato, commette un illecito.

Alla luce di quanto sopra argomentato si evince che il *focus* del reato è determinato dall'accesso a sistemi informatici senza l'autorizzazione da

---

86 LORUSSO P., L'insicurezza dell'era digitale. *Tra cybercrimes e nuove frontiere dell'investigazione: Tra cybercrimes e nuove frontiere dell'investigazione.* Milano, FrancoAngeli, 2011
LUPARIA L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa* (l.18 Marzo 2008, n. 48). Profili processuali, in "Diritto penale processuale", 2008.

parte dell'interessato.

Pertanto, al fine di stabilire se il reato di accesso abusivo ai sistemi informatici si è consumato è indispensabile tenere in considerazione il tempo in cui questo si è realizzato e l'elemento psicologico soggettivo del dolo e della colpa.[87]

Il luogo e il tempo *locus commissi delicti,* in cui si considera iniziato il reato non è necessariamente il luogo in cui si trova il *server* ma il luogo in cui avviene l'accesso abusivo.

Pertanto, il reato si perfeziona nel momento in cui si sono superate tutte le misure di sicurezza ai sistemi di protezione e il soggetto attivo riesce ad entrare all'interno del sistema informatico che conserva i dati personali, soltanto in quel preciso momento viene considerato il tempo ed il luogo in cui viene commesso il reato.

Invece, l'elemento psicologico è dato dalla volontà dell'autore del reato ossia dalla coscienza e volontà di voler entrare abusivamente all'interno di un sistema informatico senza alcuna autorizzazione da parte dell'interessato e trarne vantaggio.

Poi vi è la fattispecie denominata, "Contro la volontà tacita" che si verifica quando il sistema prevede una *password* per l'accesso e l'autore del reato non ne è in possesso, in questo caso si parla manomissione o intrusione illecita, poiché la predetta condotta avviene senza alcuna autorizzazione da parte dell'interessato.

Si è anche parlato della "misure di sicurezza", le quali si riferiscono ad una *password*, un'identificazione del volto o dell'impronta digitale, tutte tecnologia che soltanto l'interessato o chi viene autorizzato può mettere in atto per entrare all'interno dei sistemi informatici, in mancanza delle quali si tratta di intrusione illecita.[88]

---

[87] FLOR R., Art. 615-ter c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto, in "Diritto penale processuale", 2008
FONDAROLI D., SOLA L., La nuova normativa in materia di criminalità informatica: alcune riflessioni. Bologna, Clueb, 1995

[88] MANTOVANI M., Diritto penale. Parte speciale. Delitti contro il patrimonio. Padova, CEDAM, 2009

[89]In conclusione dall'analisi dell'articolo 615 *ter* del codice penale emerge che il concetto di abusività dell'accesso si configura mediante l'intrusione ad un sistema di sicurezza informatico senza alcuna autorizzazione espressa o tacita da parte dell'interessato agendo appunto in maniera abusiva.

Dall'analisi dei due articoli, 615 *ter* e 615 *quater*[90] *c. p.* si evince che sono tra di loro interdipendenti.

Nel reato di cui all'articolo 615 *quater* la detenzione e la diffusione abusiva di codici di accesso può costituire un reato di pericolo diretto, quando il bene giuridico tutelato è considerato come il domicilio di natura informatica, se invece la tutela si sposta alla riservatezza informatica, può essere inquadrato come reato di pericolo indiretto.

Nel caso di reato di pericolo indiretto, la tutela del bene avviene in un momento precedente, ossia quando ancora non si è prodotto l'evento lesivo, ma è sufficiente la situazione di solo pericolo, ancora non dannosa per iniziare a tutelare il bene giuridico.

Pertanto, tra i reati della riservatezza informatica come l'articolo 615 *quater* del codice penale, la soglia di punibilità è molto anticipata, poiché il pericolo si considera presente in maniera eventuale, ossia quando nel caso di specie si posseggono i codici abusivi anche se ancora non divulgati.

A tale circostanza viene considerata un'aggravante se il reato è commesso in danno ad "*... un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità*", ovvero *"da un pubblico ufficiale o da un*

MENGONI E., Accesso autorizzato al sistema informatico o telematico e finalità illecite: nuovo round alla configurabilità del reato [Nota a sentenza] Sez. V, 16/2/2010 (dep. 21/5/2010), in "Cassazione penale", 2011

[89] PADOVANI T. (a cura di), Codice Penale. Milano, Giuffré, 2007

PAIS S. – PERROTTA G., L'indagine investigativa. Manuale teorico pratico, Padova, Primiceri, 2015

[90] L'articolo 615-*quater* del codice penale, testualmente recita: "*chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo è punito con la reclusione fino ad un anno e con la multa sino ad euro 5164…..".*

incaricato di un pubblico servizio…, ovvero con abuso della qualità di operatore di sistema".

Sul punto è doverosa una importante precisazione, il semplice possesso dei dati personali senza alcuna autorizzazione anche se non divulgati, determina sempre un illecito, ai sensi dell'art. 615 *ter* c.p., poiché si è commesso il reato di accesso abusivo.[91]

Dunque gli elementi che definiscono il reato in questione sono il dolo specifico, il profitto e l'aver cagionato danno altrui[92].

Se un soggetto terzo intercetta abusivamente le comunicazioni digitali intercorrenti tra due o più soggetti "destinatario e mittente" al fine di trarne vantaggio, si configura, il reato di intercettazione abusiva di cui all'art. 617*quater*[93] del codice penale.

L'intercettazione abusiva di comunicazioni telematiche è annoverata tra le tipologie di reati di carattere informatico, poiché si configurano rispetto i reati tradizionali, attraverso sistemi elettronici.

Il reato di intercettazione abusiva si differenzia rispetto al reato disciplinato dall'art. 616 del c.p., relativo alla violazione di corrispondenza, poiché il contenuto dell'informazione o dei dati intercettati senza autorizzazione non rimangano all'interno dei sistemi informatici del trasgressore, ma vengano trasmessi in tutto o in parte, in rete, mediante qualsiasi mezzo di informazione al pubblico.

---

91 PICOTTI L., La nozione di criminalità informatica e la sua rilevanza per le competenze penali europee, in "Rivista trimestrale di diritto penale dell'economia", 2011
PICCINI M.L., VACIAGO G., Computer crime: casi pratici e metodologie investigative dei eati informatici, Bergamo, Moretti&Vitali, 2008
RICHARDS J., Transnational criminal organizations, Cybercrime and money laundering, CRC Press, Boca Raton, FL, 1999

92 RINALDI P.G., Commento all'art. 6 della l. 547/1993, in "Legislazione penale", 1996
ROSSI VANNINI A., La criminalità informatica: le tipologie di computer crimes di cui alla l. 547/1993 dirette alla tutela della riservatezza e del segreto, in "Rivista trimestrale di diritto penale dell'economia".

93 Il primo comma dell'art. 617-*quater,* codice penale, prevede che "*chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni".*

Naturalmente i dati e le informazioni carpite abusivamente devono essere strettamente personali e i destinatari devono essere soggetti determinati o determinabili.

Il contenuto dei dati acquisiti abusivamente può avere qualsiasi forma, come una foto o un video e poi inviato ad un destinatario individuato o individuabile.

Le azioni oggetto di incriminazione sono pertanto relative alla intercettazione, interruzione e impedimento delle comunicazioni digitali.

L'intercettazione consiste nell'appropriarsi da parte di un terzo estraneo al rapporto, di contenuti comunicativi senza alcuna autorizzazione e all'insaputa delle parti, il quale riesce ad intromettersi ed a carpire nel momento della trasmissione tutti i dati personali della comunicazione.

Però affinché il predetto reato si configuri, è necessario che l'autore del reato eluda i sistemi di sicurezza, ed acquisisca abusivamente la comunicazione in corso[94].

Qualora il reo non riesca ad acquisire nella loro integrità tutti i dati trasmessi tra le parti non si potrà configurare il reato di intercettazione, ma soltanto il reato di interruzione ed impedimento di comunicazioni digitali.

Inoltre, il reato di intercettazione prevede anche la circostanza che tranne se il fatto costituisca più grave reato, verrà irrogata la medesima pena, a chiunque attraverso qualsiasi mezzo di informazione al pubblico rivela il contenuto di informazioni riservate.

11. Conclusioni

Dallo studio del presente capitolo è emerso che in materia di tutela sul trattamento e sulla circolazione dei dati personali è necessario adeguarsi il più possibile alle disposizioni espresse nel Regolamento 2016/679, poiché

[94] FIANDACA MUSCO E., Diritto penale. Parte speciale. 2.1: I delitti contro la persona. Bologna, Zanichelli, 2013

i principi ispiratori del GDPR aiutano a rendere più omogenea la normativa sia a livello nazionale che europeo.

La società attuale è fondata ormai su l'utilizzo della rete per qualsiasi attività quotidiana, sia sociale che economica, per cui la tutela del dato personale assume un'importanza fondamentale, sia nella fase dell'acquisizione che nella fase della circolazione ed infine nel momento della conservazione, al fine di tutelare la riservatezza e la dignità umana.

I concetti introdotti dal nuovo Regolamento sono svariati, in particolare il diritto all'oblio (articolo 17), il diritto alla portabilità dei dati (articolo 20), il diritto di accesso (articolo 15), la disciplina sui social e minori (articolo 8), ed in particolar modo il 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, liceità e correttezza relativamente al trattamento dei dati personali ed il principio *di accountability.*

Il principio della trasparenza espressamente previsto dal GDPR impone che le informazioni destinate al pubblico o all'interessato siano di facile accesso e comprensione senza trabocchetti, poiché talvolta la complessità tecnologica rende difficile per l'interessato comprendere le conseguenze delle proprie attività poste in essere sulla rete, relativamente alle informazioni personali che involontariamente vengono fornite dall'avente diritto.

Determinante è l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento assicurandosi cosi di un trattamento equo e trasparente.

Il principio *di accountability* costituisce le fondamenta su cui si basa il GDPR ed è recepito dall'articolo 24 in forza del quale tenuto conto del contesto e delle finalità, il titolare del trattamento ha la facoltà di mettere in atto tutte le misure tecniche e organizzative adeguate al fine di garantire

e poter dimostrare che la sua condotta in relazione al trattamento è stata posta in essere in conformità al presente Regolamento.

Pertanto, alla luce dell'analisi dell'impianto normativo sulla *privacy* si può concludere che il trattamento dei dati personali non è riconducibile soltanto al soggetto al quale si vuole difendere il diritto alla *privacy*, ma consiste nell'interesse improntato sulla lealtà e la correttezza come su qualsiasi altro rapporto giuridico tra le parti.

Alla luce dell'ambito normativo sopra descritto, nel prossimo capitolo verranno esaminati il sistema sanzionatorio penale ed amministrativo sotto l'aspetto del decreto legislativo 101/2018 e del Decreto Capienze.

CAPITOLO II

LA TUTELA PENALE DEL DATO PERSONALE: DAL D.LGS. N. 101/2018 AL D. LGS N. 139/2021

SOMMARIO: 1. I reati in materia di privacy. Introduzione – 2. I soggetti del trattamento del dato personale e i loro compiti – 3. integrazione del codice della privacy D.lgs. n. 101/2018 al Regolamento Europeo– 4. D. lgs 18 maggio 2018 n. 51- 5. Il D.L. n. 139/202 Decreto Capienze - 6. Le integrazioni effettuate dal D.lgs. n. 101/2018 e dal D.L. n. 139/2021 al sistema sanzionatorio - 6.1. (*segue)* Illeciti amministrativi e Violazioni penali – 7. art. 167 codice privacy: trattamento illecito di dati personali – 8. art. 168 codice privacy: notificazioni e dichiarazioni false al Garante - 9. art. 170, codice privacy: L'inosservanza di provvedimenti del Garante - 10. "Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori" art. 171 C.d.P. e pene accessorie art. 172 C.d.P.- 11. Considerazioni finali

1. I reati in materia di privacy. Introduzione

In seguito all'articolo 13 della "legge di delegazione europea" del 25 ottobre 2017 n. 163 in tema di tutela dei dati personali, il legislatore italiano ha avvertito la necessità di adeguare il nostro ordinamento giuridico italiano alle disposizioni del GDPR Regolamento 2016/679/UE.

Dopo un lungo iter legislativo nel quale hanno preso parte attiva in funzione consultiva sia le Commissioni parlamentari sia il Garante alla privacy, il D. Lgs 101/2018 ha realizzato un vero e proprio intervento di novellazione codicistica con lo scopo di effettuare una coordinazione tra il sistema interno italiano e le disposizioni del Regolamento Generale cercando il più possibile di non effettuare particolari cambiamenti.[95]

Il D.lgs 101/2018, giova ribadire ha novellato alcune disposizioni del vecchio Codice *Privacy,* come si evince dall'abrogazione dell'art. 2 del D.lgs. del 2003, sostituendolo con un nuovo articolo 2 nel quale si prevede che «*Il presente Codice reca disposizioni per l'adeguamento dell'ordinamento*

[95] D'AGOSTINO., *La tutela penale dei dati personali nel riformato quadro normativo*: un primo commento al D.Lgs. 10 agosto 2018, n. 101, in Archivio Penale, n. 1, 2019,

nazionale alle disposizioni del Regolamento», con l'obiettivo di indicare che le disposizioni del Codice novellato sono limitate a contenere le norme nazionali di adeguamento al GDPR.[96]

Tra le modifiche apportate viene abrogato l'art. 23 riguardante l'eliminazione del trattamento effettuato senza il consenso dell'interessato, presupposto dell'illecito trattamento di dati, in tale fattispecie si è operata una vera *abolitio criminis* parziale con la conseguenza che verranno applicate le sanzioni amministrative previste dal Regolamento.

Dunque, attraverso il predetto decreto sono state modificate ed introdotte nuove finalità del codice sulla *privacy*, come si evince dall'abrogazione dell'articolo 2 del D.lgs. 196 del 2003 introducendo un nuovo articolo.

Infatti, il predetto articolo 2 specifica che le finalità del codice novellato riguardano l'adeguamento dell'ordinamento nazionale e le disposizioni del Regolamento GDPR.

Il predetto Regolamento UE 2016/679 attribuisce i poteri e la competenza ad un organo chiamato Autorità di controllo, per la tutela dei diritti e le libertà fondamentali delle persone fisiche che riguardano il trattamento dei dati personali.

In Italia, le stesse competenze sono attribuite all'Autorità Garante della *Privacy* istituito dalla legge 31 dicembre 1996 numero 675 ed espressamente disciplinato dal codice della *privacy* (D.lgs. n. 196/2003), il quale assume il compito di autorità amministrativa indipendente.

Le modifiche apportate dal D.lgs. n. 101/2018 concernente i poteri e le competenze del Garante per la protezione dei dati personali non si discostano eccessivamente da quanto il Codice della privacy prevedeva già prima della riforma, poiché riguardano per lo più le funzioni del Garante in relazione alle disposizioni del Regolamento.

In particolare al Garante viene assegnato il potere di monitorare la corretta applicazione delle disposizioni sia comunitarie che interne nell'autonomia che il Regolamento ha voluto concedere al legislatore nazionale.

---

[96] PIZZIMENTI F., Codice privacy italiano dopo il Gdpr: come leggerlo e applicarlo ex decreto 101/2018, in agendadigitale.it, 2018

L'Autorità Garante diventa una figura *super partes* relativamente al trattamento dei dati personali con poteri e competenze finalizzati a garantire la tutela dei diritti della persona umana, in relazione al rispetto delle disposizioni introdotte dal Regolamento.

Il legislatore nazionale attraverso il decreto di adeguamento attribuisce all'Autorità Garante in materia di protezione dei dati personali un ruolo non soltanto di mero indirizzo attribuendogli specifici poteri, attraverso i quali non è soltanto un arbitro o organo di mera vigilanza, ma un organo di tutela attivo nel rispetto delle norme sancite dal Regolamento.[97]

Pertanto, le modifiche introdotte sui combinati disposti dal legislatore europeo e dal legislatore nazionale in ordine alla circolazione e protezione dei dati personali che hanno novellato il Codice della Privacy sono finalizzati a connettersi con il Regolamento UE n. 679/2016 per una migliore armonizzazione ed attuazione della normativa in argomento.

Le innovazioni di particolare rilievo sono, inoltre, le modifiche apportate sul campo amministrativo e penale sia a livello comunitario che nazionale.[98]

2. I soggetti del trattamento del dato personale e i loro compiti

Il concetto della protezione dei dati personali si sviluppa intorno alla tutela della vita privata la quale nel corso del tempo si è evoluta adattandosi alle mutate esigenze della nuova realtà tecnologica attribuendo oggi al concetto di "sfera privata" non solo l'aspetto familiare ed intimo, ma anche l'aspetto professionale.

---

[97] R. PANETTA, Decreto di adeguamento GDPR: come cambiano le sanzioni e gli illeciti penali del Codice Privacy, Assago, 21.11.2018

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

Per tali motivi l'art. 1 del Regolamento UE 2016/679 ha come obiettivo il trattamento dei dati personali, nell'ottica di attuare la protezione al servizio dell'essere umano contemperando la tutela secondo il principio di proporzionalità con gli altri diritti inviolabili ed inalienabili.

La definizione del termine "trattamento dei dati" è espressamente disciplinata anche dall'art. 4 n. 2 del Regolamento, il quale lo definisce come qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi tecnologici ed applicate ai dati personali.[99]

Per quanto riguarda il trattamento dei dati personali è possibile fare un elenco meramente esemplificativo delle attività più comuni che normalmente vengono svolte come la registrazione dei dati, ossia inserire i dati su un supporto elettronico e conservarli, la raccolta, che consiste nell'acquisizione dei dati, l'organizzazione ritenuta come catalogazione dei dati mediante un particolare procedimento ed infine la comunicazione, consistente nella trasmissione dei predetti dati a terze persone o la cancellazione o distruzione dei predetti dati personali.

Dal Regolamento UE n.679 del 2016 è possibile trarre alcuni riferimenti utili, in particolare l'art. 4, il quale definisce il dato personale come qualsiasi informazione riguardante una persona fisica, chiamata interessato identificata o identificabile.

È identificabile la persona fisica che può essere individuata direttamente o indirettamente con particolare riferimento ad un identificativo come il nome i dati relativi all'ubicazione un identificativo online o a uno o più elementi caratteristici della sua identità fisica, genetica, psichica, economica, culturale o sociale.

Una specifica disciplina è prevista per particolari categorie di dati indicati dagli artt. 9 e 10 del Regolamento che costituiscono i dati sensibili e i dati giudiziari.

---

[99] MACALUSO F., PURIFICATI J., Dizionario della privacy, cit., 276.
BOLOGNINI L., BISTOLFI C.., Il regolamento, cit., 86-87. 168 Cfr. WP29, op. 1/2015, p. 7, nota 13. 173 WP29, opinione 4/2007, p. 22.
BOLOGNINI L BISTOLFI C., PELINO E., Il regolamento, cit., 169.

Il trattamento dei dati personali crea al suo interno un rapporto giuridico tra i vari soggetti quali il Titolare, il Responsabile, l'incaricato, il DPO (Data Protection Officer), l'Autorità e il Garante ciascuno per le loro competenze raccolgono, gestiscono, comunicano e conservano i dati dell'interessato che è colui a cui i dati personali si riferiscono.

Il titolare del trattamento dei dati possiamo definirlo come il fulcro attorno al quale orbitano le scelte in relazione alle finalità da perseguire nel trattamento.

La figura del titolare può essere rivestita da una persona fisica, una persona giuridica o un'autorità pubblica, la quale ha l'obbligo giuridico di porre in essere un'attività che garantisca con una dimostrazione che il trattamento dei dati sia stato eseguito in totale conformità alle disposizioni del Regolamento e alle disposizioni nazionali.

Il titolare è pertanto definito anche il soggetto primario, poiché gli viene attribuito il potere di nominare eventualmente dei collaboratori per la realizzazione di attività relative al trattamento dei dati personali che sono chiamati responsabili, ai quali il titolare impartirà specifici compiti. [100]

Il titolare svolge prevalentemente obblighi relativi alla sicurezza, obblighi relativi alla garanzia nei confronti dell'interessato e obblighi di collaborazione e di controllo con i responsabili.

I compiti del titolare sono quelli di predisporre l'analisi dei rischi e in alcuni casi realizzare una valutazione d'impatto sulla protezione dei dati (PIA), nell'ambito di un più generale Risk Assessment seguita da una possibile "Consultazione preventiva" dall'Autorità Garante se le misure di sicurezza adottate non consentano di escludere o limitare i rischi per i diritti e le libertà degli interessati al trattamento.

Inoltre, il titolare deve essere in grado di dimostrare di aver adottato tutte le misure giuridiche, tecniche e organizzative per la protezione dei dati personali con la possibilità di verificare in un secondo momento che le

---

[100] BOLOGNINI L., BISTOLFI C., PELINO E., IL REGOLAMENTO, CIT., 120. 170 BOLOGNINI L., BISTOLFI C., PELINO E., IL REGOLAMENTO, CIT., 121. 171 PANETTA R., CIRCOLAZIONE, CIT., 17 SS.
172 PANETTA R., Circolazione, cit., 17 ss

misure adottate siano state efficaci, al fine di prevenire trattamenti illeciti sui dati o eventuali danni in capo agli interessati al trattamento.

A tal proposito è necessario stabilire precisi limiti temporali nella conservazione delle varie tipologie e categorie di dati, attraverso l'adozione di una specifica "*Data retention policy*" ed inoltre, garantire preventivamente che non siano stati resi noti dati personali ad un numero indefinito di persone e nell'eventualità creare particolari procedure di autorizzazione e autenticazione.

Altra funzione svolta dal titolare consiste nelle modifiche e nell'aggiornamento delle nomine dei "Responsabili del trattamento" relative alle sub-deleghe a terzi nel caso di attività che riguardano un trattamento di dati personali in un contesto di sub-appalto o sub-fornitura di servizi.

Il titolare svolge anche il compito di provvedere alla realizzazione di nuovi adempimenti nel caso di trasferimenti di dati personali verso un Paese terzo.

Attraverso consulenti esterni o mediante un Responsabile della protezione dei dati, il titolare predispone piani di formazione periodica del personale e della revisione del Regolamento aziendale interno sul corretto utilizzo degli strumenti elettronici, posta elettronica e internet e al rafforzamento degli obblighi di informativa nei confronti dei dipendenti.

Una funzione di un certo rilievo è la tenuta da parte del titolare di un Registro delle attività di trattamento con il quale può dimostrare la conformità di tutti i trattamenti in conformità a ciò che prevede la regolamentazione europea e garantire un corretto trattamento e gestione dei dati personali.

Nel caso in cui si verifichino violazioni di dati personali c.d. "data breach", il titolare deve adottare una specifica procedura mediante comunicazioni all'Autorità Garante o agli interessati al trattamento.

Il titolare, inoltre, può decidere di nominare un Responsabile che consiste in un'altra figura del trattamento dei dati, mediante il quale per suo conto si occupi degli adempimenti in materia di privacy.

Il Responsabile del trattamento deve fornire garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

Secondo l'art. 4 n. 8 del Regolamento UE n.679 del 2016 per Responsabile si intende "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".

I trattamenti da parte di un Responsabile, eventualmente nominato dal titolare sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri. L'art. 28 del Regolamento UE n.679 del 2016 definisce nel dettaglio il contenuto del contratto o dell'atto giuridico di nomina del responsabile.

In base all'art. 2-*quaterdecies* del d.lgs. n.101 del 2018 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.

In tal caso 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 loro autorità diretta in genere chiamati incaricati.[101]

Altro soggetto del rapporto in argomento è l'interessato persona fisica identificata o identificabile cui si riferiscono i dati personali.

Per quanto riguarda la figura dell'interessato, come abbiamo già rappresentato in precedenza, riguarda il soggetto i cui dati personali si riferiscono.

---

[101] 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».*

Sul punto il regolamento prevede che con la morte dell'interessato viene meno la persona fisica e quindi si estinguono i diritti soggettivi, ma non si estinguono i diritti degli eredi nei confronti del *de cuius* mantenendo il diritto di accedere alle informazioni del proprio parente defunto.

A tal proposito il d.lgs. n.101 del 2018 in attuazione del Regolamento UE, prevede all'art. 2-*terdecies* una disciplina specifica per il trattamento dei dati personali concernenti persone decedute. I relativi diritti possono essere esercitati da chi ha un interesse proprio o agisce a tutela dell'interessato, in qualità di suo mandatario o per ragioni familiari meritevoli di protezione.

Altra figura di rilievo è il responsabile della protezione dei dati (Data Protection Officer" DPO)

Secondo l'art.37 del Regolamento UE n.679 del 2016 il titolare del trattamento e il responsabile del trattamento designano un responsabile della protezione dei dati nel caso in cui il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali.

Le principali attività svolte dal responsabile della protezione dei dati (Data Protection Officer" DPO) consistono in trattamenti che, per loro natura, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala.

Nel quadro normativo del trattamento dei dati personali all'art. 37 del Regolamento è subentrato un nuovo termine, "larga scala" che consiste nell'obbligo di nominare la figura del D.P.O., nonostante il Regolamento più volte faccia riferimento al termine su larga scala, non enuncia mai una definizione concreta e chiara, lo stesso dicasi per il decreto attuativo del 2018 n. 101 in ambito nazionale nel quale non viene mai espressa una definizione ben precisa di tale locuzione.

Soltanto nel *considerandum* 91 del GDPR[102], si stabilisce che si possono considerare trattamenti su larga scala, quei trattamenti che hanno

[102] Considerandum 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*

per oggetto sia a livello regionale, nazionale che sovranazionale la gestione ed il controllo di una grande quantità di dati che per loro natura necessitano di una particolare protezione, poiché presentano dei rischi e delle criticità dovute alla quantità di interessati.

Altra fonte a cui possiamo fare riferimento per un supporto è il gruppo di lavoro articolo 29 nel quale vengono indicate le linee guida al fine di poter constatare se il trattamento dei dati personali può essere stato posto in essere o meno su larga scala.[103]

Il Gruppo di lavoro sopra menzionato anche mediante l'utilizzo dell'art. 37 GDPR enuncia alcune fattispecie mediante le quali si arriva ad una specifica definizione della nozione di larga scala: per esempio il trattamento dei dati personali raccolti durante il ricovero dei malati in strutture sanitarie, ovvero il trattamento di dati rilevati in ordine ad un luogo c.d. "geolocalizzazione", o mediante il trattamento dei dati riguardanti il servizio di trasporto pubblico, ed ancora il trattamento dei dati personali svolto da banche e assicurazioni ed infine il trattamento dei dati personali in ordine al settore della telefonia mobile e non.

Le fattispecie sopra riportate sono uno dei tanti esempi in cui si può considerare il trattamento dei dati, "su larga scala".

---

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 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".

[103] ANTONINI E., Il Trattamento illecito di dati personali nel Codice della Privacy – i nuovi confini della tutela penale, in Diritto e procedura penale 2005, 44

Alla luce delle superiori argomentazioni diventa sempre più necessario individuare la definizione della nozione di larga scala, al fine di nominare i *data protection officer* (DPO).

Il predetto Gruppo di lavoro ha individuato una serie di requisiti che devono essere presenti, affinché, si possa parlare di trattamento dei dati su larga scala, innanzitutto il numero degli interessati, ossia la quantità di persone coinvolte nel trattamento dei dati, che può essere espresso o in percentuale o a numero, la quantità di dati e le varie categorie che sono utilizzate nel trattamento, la delimitazione del territorio oggetto del trattamento e la durata delle operazioni relative al trattamento dei dati in oggetto.

La figura del DPO ha la funzione di aiutare il titolare soprattutto nelle fattispecie di particolare complessità, come quella del trattamento dei dati su larga scala in cui le tecniche di trattazione sono molto complesse e possono provocare lesioni ai diritti fondamentali degli interessati.

Il soggetto DPO è nominato in maniera obbligatoria nell'ambito della pubblica amministrazione, mentre nel campo privato potrà essere nominato soltanto nella fattispecie in cui siano presenti i requisiti previsti dall'art. 37 GDPR.

Pertanto, la figura del DPO viene nominata quando il titolare o il responsabile svolga delle attività inerenti al trattamento dei dati personali su larga scala.

Dall'analisi del gruppo di lavoro articolo 29 si evince come sia importante stabilire se il titolare del trattamento dei dati sia un ente pubblico o un privato, nel caso in cui sia un ente pubblico vi è sempre l'obbligo di nominare un DPO, invece nella fattispecie in cui il soggetto sia un privato non vi è nessun obbligo alla nomina della figura del DPO tranne nel caso in cui i dati abbiano dei volumi di particolari dimensioni.

In questi casi è possibile avvalersi di sistemi automatizzati come nel caso di dati particolarmente sensibili come quelli di natura sanitaria, relativi alla salute o alle confessioni religiose o all'orientamento sessuale dell'interessato.

Da ciò si desume che non tutti gli individui privati che svolgono trattamento di dati personali sono sottoposti alla disciplina della nomina del DPO.

Infatti, sono esclusi i professionisti sanitari singoli o liberi professionisti che svolgono la loro attività individualmente tranne coloro che svolgono la professione in maniera associata.

Il trattamento di dati personali su larga scala è affrontato dal legislatore comunitario nell'interesse della protezione dei diritti dell'interessato, la cui responsabilità è in capo al titolare per la gestione e il controllo con l'obiettivo di riequilibrare la necessaria tutela del trattamento dei dati personali in oggetto.

L'aspetto da analizzare sull'unità o pluralità dei dati personali potrebbe non essere utile, invece quello che bisogna esaltare è la possibilità di far evolvere i tradizionali diritti fondamentali della riservatezza e dell'identità personale.

Il fulcro del discorso è la possibilità di autodeterminarsi grazie alla propria consapevolezza di sé stessi nei confronti degli altri e quindi la possibilità di accedere ai propri dati e di rettificarli, tale controllo ha l'obiettivo di inibire l'invadenza degli altri nel proprio ambito privato.

A livello giuridico internazionale si usa la terminologia "*data protection*" con la quale si vuole evidenziare che è sufficiente stare chiusi nel proprio guscio per tutelare i propri dati personali.

Nello stesso tempo è giusto vivere liberamente confrontarsi con la società e le nuove tecnologie e proiettarsi attraverso l'esterno mantenendo il controllo sulla circolazione dei propri dati e sulla limitazione imposta agli altri affinché senza le dovute autorizzazioni non possano venirne a conoscenza.[104]

Oggi più che in passato si sente la necessità di tutelare la propria identità digitale attraverso l'autodeterminazione, pertanto il denominatore

---

[104] CIRILLO G. P., La tutela della Privacy nel sistema del nuovo codice dei dati personali, Padova, 2004.2 RODOTÀ S., in Intervista su Privacy e Libertà
RODOTÀ S., IN INTERVISTA SU PRIVACY E LIBERTÀ
RODOTÀ S., Il mondo nella rete. Quali i diritti, quali i vincoli, Roma – Bari, 2014

comune è il controllo sui propri dati, poiché noi siamo le nostre informazioni ossia "*habes corpus* in chiave digitale".

In una società come la nostra in cui le informazioni circolano velocemente e continuamente tutelare i propri dati diventa ormai essenziale al fine di evitare illegittime intrusioni che possano permettere agli altri di insinuarsi nella nostra sfera privata.

Ciò vuol dire che la riservatezza e il trattamento di dati personali non devono diventare un limite all'esercizio della libertà, ma devono poter convivere e contemperarsi fra di loro.

Solitamente nei discorsi comuni le due terminologie si sovrappongono la nozione di riservatezza con quella di diritto alla *privacy,* in cui la riservatezza è un elemento specifico del diritto alla protezione dei dati personali in quanto si tratta di due istituti giuridici diversi ma riguardanti lo stesso argomento, spesso invece utilizzati per sbaglio come sinonimi.[105]

Pertanto, il diritto alla protezione dei dati personali è un concetto maggiore poiché non consiste soltanto nel controllo delle informazioni private, ma anche nel diritto di scegliere cosa vogliamo rendere noto ai terzi e ciò che non vogliamo rendere noto a terzi.

Con la conseguenza che la protezione dei dati personali può in senso lato comprendere anche *la privacy*, ma anche la mera autodeterminazione informativa, ossia la protezione di ogni informazione riferita o riferibile a una persona identificata o identificabile qualsiasi sia il contenuto.

A tal proposito la Corte Giustizia dell'Unione Europea[106] è intervenuta stabilendo in maniera netta la distinzione fra le due terminologie, il diritto alla *privacy* come diritto a limitare le ingerenze altrui nella propria sfera,

---

[105] RODOTÀ nel discorso di presentazione della relazione annuale del Garante al Parlamento dell'anno 2001.
MESSINETTI. in Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali in Enc. Dir., Milano, 1983.

[106] Corte Giustizia UE (Grande Sezione), 6 ottobre 2015, C-362/14, nel celebre caso Maximilian Schrems c. Data Protection Commissioner.
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.
RODOTÀ S. Tecnologie e diritti, Bologna, 1995.

ed il diritto alla protezione dei dati personali, ossia il corretto trattamento dei dati nel rispetto della libertà e dei diritti fondamentali dell'essere umano.

La differenza pertanto è di palmare evidenza se andiamo ad analizzare il bene giuridico oggetto di tutela nell'uno e nell'altro diritto.

Nel diritto alla *privacy* la tutela è rivolta verso la sfera privata e quindi di natura esclusivamente soggettiva.

Invece, nel diritto alla protezione dei dati personali il bene giuridico tutelato è la correttezza e liceità della protezione dei dati personali avendo una natura sia soggettiva che collettiva.

In questo modo possiamo affermare che la nozione di *privacy* mira a tutelare la vita privata, indipendentemente dal trattamento dei dati, invece, il trattamento dei dati personali, mira alla correttezza del trattamento indipendentemente dalla sfera privata del soggetto.

In conclusione il diritto alla protezione dei dati personali può essere visto sotto l'ottica di un incredibile risorsa che può conferire alla persona la sua libertà, pur mantenendola al centro della società digitale.

3. L'integrazione del codice della privacy D.lgs. n. 101/2018 al Regolamento europeo

Il recepimento e il conseguente adeguamento dell'ordinamento giuridico italiano alla direttiva dell'Unione europea si è potuto realizzare grazie all'attività del Governo con l'introduzione del D.lgs. n. 101/2018 che ha integrato il D.lgs. n. 196/2003 intervenendo sul trattamento di determinati dati sensibili e giudiziari e sui codici deontologici e di buona condotta.

In questa maniera il Governo italiano mediante delega del Parlamento ha introdotto nel D.lgs. n. 101/2018[107] alcune norme specifiche relative alla

[107] PIZZETTI F., I consigli per leggere e applicare bene il decreto 101/2018, www.agendadigitale.i

definizione di affari pregressi, ossia reclami effettuati al Garante prima del 2018 e non ancora risolti, inoltre ha novellato parte del codice della privacy.

In tale stravolgimento sono stati riconosciuti nuovi compiti al Garante come i codici di deontologia e di buona condotta e sono stati anche modificati alcuni criteri su cui si basano le autorizzazioni in generale.

Per quanto riguarda le norme relative al codice di deontologia e di buona condotta è rimasto invariato l'art. 12 del D.lgs. n. 196/2003, il quale è stato ritenuto perfettamente valido, poiché si fonda sulla liceità e sulla correttezza del trattamento dei dati personali.

I predetti codici di deontologia e di buona condotta sono stati rinominati "regole deontologiche". [108]

Al fine di fare chiarezza il D.lgs. n. 101/2018 ha novellato buona parte del D.lgs. n. 196/2003, che comunque rimane in vigore perfettamente adeguato al Regolamento UE 2016/679.[109]

Le novità introdotte dal D.lgs. n. 101/2018 riguardano principalmente misure di garanzia che consistono in particolari sistemi di sicurezza innovativi per la tutela e la circolazione del trattamento dei dati personali, relativamente ai dati genetici, biometrici e sanitari in cui per la prima volta il Regolamento prevede una tutela specifica.

Il Regolamento prevede che il trattamento dei dati e la relativa responsabilità del titolare si debba basare sul principio *dell'accountability* a differenza del D.lgs. n. 196/2003 pre-novella che prevedeva delle piccole ed insufficienti misure in cui il titolare era obbligato a rispettare.

In ordine all'incessante evoluzione informatica e per la particolarità della materia, al fine di attuare una protezione reale del trattamento dei dati il decreto legislativo n. 101/2018 all'art. 2-*septies,* comma 5 ha integrato e modificato il codice della privacy italiano, prevedendo che il Garante ogni due

[108] MALGIERI G., Inquadramento normativo, cit., 5 ss

[109] PANETTA R., Circolazione e protezione dei dati personali, tra libertà e regole del mercato, Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018, Milano, 2019, 635 ss. Art. 2-quater d.lgs. 196/2003, così come modificato dal D.lgs. n. 101/2018.

anni, possa valutare ed individuare nuovi sistemi di sicurezza per meglio garantire i diritti di riservatezza e di tutela della *privacy* degli aventi diritto.

Il Regolamento UE 2016/679 prevede dagli artt. 15 a 22 che alcuni diritti riconosciuti all'interessato in materia di trattamento dei dati personali possano essere in particolari circostanze limitati o addirittura esclusi, qualora dovessero essere in contrasto con l'interesse pubblico dell'ordinamento intero di uno Stato membro.

Un ulteriore novità introdotta e novellata dal codice della *privacy* italiano riguarda la validità del consenso prestato da colui che ha compiuto 14 anni, al quale viene riconosciuta la capacità e la consapevolezza di comprendere il consenso fornito per il trattamento e la circolazione dei propri dati personali.

Diversamente, per il minore di 14 anni è necessario che il consenso venga emesso soltanto da chi esercita la responsabilità genitoriale.[110]

A tal proposito viene istituito un ente unico nazionale di accreditamento cui il Garante può intervenire in caso di gravi inadempimenti effettuati dal titolare, al fine di attuare una tutela maggiore per l'interessato.

Inoltre, continuando con la nostra disamina, il codice della *privacy* modificato e novellato dal D.lgs. 101/2018 prevede che l'interessato possa presentare un reclamo al Garante e un ricorso anche all'autorità giudiziaria.

A tal riguardo gli articoli 142 e 144 del predetto codice prevedono che il reclamo sia definito in un tempo massimo di nove mesi, se ciò non dovesse accadere l'interessato può sempre proporre altri reclami.

Invece, in merito all'inserimento e all'utilizzo di elenchi telefonici questi possono essere gestiti dal Garante insieme all'Autorità per le garanzie delle comunicazioni.

Un'altra caratteristica del nuovo codice della *privacy* in relazione all'aspetto sanzionatorio penale riguarda la riformulazione e l'introduzione di nuove fattispecie di reato, in particolare gli articoli 167 *bis* e 167 *ter* codice della *privacy* che riguardano illecite comunicazioni di fusioni ed acquisizioni fraudolente di dati, soprattutto su larga scala.

---

[110] CASSANO G., COLAROCCO V, GALLUS G.B., M., Il processo di adeguamento al GDPR: aggiornato al d.lgs. 10 agosto 2018, n. 101, Milano 2018, 9 e ss.

La necessità di rimodulare l'assetto sanzionatorio penale è stata determinata dai numerosi attacchi *Cyber,* agli *hacker* e ai *malware* che con il progresso della tecnologia sono sempre più presenti e capaci di violare anche sistemi di sicurezza più moderni e sofisticati.

In buona sostanza i reati introdotti con il D.lgs. 101/2018 sono in particolare: trattamento illecito dei dati (art. 167); comunicazione e diffusione illecita dei dati personali oggetto di trattamento su larga scala (art.167-*bis*); acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala (art.167-*ter)*; falsità nelle dichiarazioni al Garante e interruzioni dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante (art.168); inosservanza di provvedimenti del Garante (art.170); violazione delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori (art. 171) che verranno trattati in maniera dettagliata nei paragrafi successivi.

4.D. lgs 18 maggio 2018 n. 51

In data 24/05/2018 è stato pubblicato sulla G.U. serie generale n. 119 il Decreto legislativo 18 maggio 2018, n. 51 emanato in attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

Il provvedimento, che si compone di cinquanta articoli è suddiviso in otto Capi, dedicati a specifici aspetti della materia, che rinviano al regolamento (UE) 2016/679 nelle parti il cui contenuto risulta coincidente con la direttiva.

Con riguardo al Capo primo, nel rispetto dei criteri direttivi generali previsti dall'articolo 32 della legge 234 del 2012, si è inteso anzitutto fornire una disciplina organica del trattamento di dati personali per fini, appunto, di

prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.

Tale disciplina supera e pertanto sostituisce gran parte di quella di cui ai titoli I e II della Parte seconda del Codice privacy, che per il settore giudiziario si applicava ai trattamenti svolti nell'esercizio di funzioni giudiziarie in sede tanto civile quanto penale.

Il primo Capo tratta gli aspetti generali, i principi applicabili, le condizioni e i presupposti per il trattamento legittimo dei dati. Viene menzionata la possibilità di utilizzare il regolamento come fonte normativa supplementare oltre a quella legislativa per il trattamento dei dati (compresi quelli sensibili) a patto che siano previste adeguate garanzie per i diritti e le libertà dell'interessato.

Al contrario, la decisione automatizzata, inclusa la profilazione, è lasciata alla sola fonte legislativa e garantita da specifiche protezioni a causa dei rischi che potrebbero comportare per i diritti e le libertà dell'interessato.

Il secondo Capo riguarda i diritti dell'interessato e recepisce le norme del Capo III della direttiva, viene stabilito che l'esercizio di questi diritti (ricezione di informazioni, accesso, rettifica, cancellazione, limitazione del trattamento) possa essere limitato, ritardato o escluso se necessario per proteggere la sicurezza pubblica o altri interessi specificamente identificati.

Per quanto riguarda i dati personali contenuti negli atti giudiziari o nel casellario giudiziale, questi diritti possono essere esercitati in conformità alla disciplina del settore per preservarne le specificità.

Si è poi previsto che gli stessi diritti siano esercitabili, relativamente ai dati personali contenuti in atti giudiziari o nel casellario giudiziale, trattati in sede procedimentale ovvero esecutiva, conformemente alla disciplina di settore, al fine di salvaguardarne le specificità, avvalendosi della possibilità riconosciuta al legislatore nazionale dall'art. 18 della direttiva (art. 14, comma 1).

Il terzo Capo del regolamento riguarda il titolare e il responsabile del trattamento dei dati personali, descrive i principali obblighi per queste figure,

inclusa la nomina obbligatoria di un responsabile della protezione dei dati per garantire la sicurezza dei dati stessi.

Inoltre, prevede il parere obbligatorio del Garante per gli atti normativi che potrebbero avere un impatto sulla protezione dei dati personali.

Il Capo disciplina inoltre gli obblighi di sicurezza del trattamento, compreso l'obbligo di notificare eventuali violazioni relative ai dati personali.

La nomina del responsabile della protezione dei dati è stata prevista anche per l'autorità giudiziaria, per garantire la corretta gestione dei trattamenti di dati sensibili, in ragione dell'ausilio che tale figura può fornire nella gestione di trattamenti complessi e spesso inerenti dati sensibili, quali appunto quelli svolti in sede giurisdizionale (art. 28).

Il quarto Capo disciplina il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali.

Il quinto Capo contiene norme importanti, come l'esclusione del potere di controllo del Garante sulla legittimità del trattamento svolto dall'autorità giudiziaria e dal pubblico ministero, che hanno un particolare status nel nostro ordinamento.

Inoltre, prevede anche sanzioni amministrative per la violazione delle norme di recepimento della direttiva, con limiti più elevati se la violazione riguarda i diritti degli interessati o le norme sul trasferimento dei dati all'estero.

Sono state anche previste sanzioni amministrative, per la violazione delle norme di recepimento della direttiva, secondo lo schema generale previsto dal Regolamento, con i criteri e le garanzie ivi previsti, nonché con cornici edittali più elevate qualora la violazione concerna i diritti degli interessati o le norme sul trasferimento dei dati all'estero (art. 42).

Il Capo sesto del regolamento riguarda le sanzioni penali per la violazione delle norme sulla protezione dei dati personali, infatti prevede la riproduzione di alcuni reati già previsti dal Codice, come la falsa dichiarazione al Garante e l'inosservanza di provvedimenti dell'Autorità.

Inoltre, introduce una nuova fattispecie delittuosa per il trattamento illecito di dati personali, che sanziona i trattamenti effettuati in violazione di

determinate disposizioni rilevanti, con dolo specifico di danno o profitto e con la condizione di punibilità di un nocumento nei confronti dell'interessato.

Il Capo sesto reca le norme sanzionatorie penali, nel rispetto dello specifico criterio direttivo di cui all'articolo 11 della legge di delegazione. Oltre alla sostanziale riproduzione, in termini invariati, dei peculiari delitti di false dichiarazioni al Garante e inosservanza di provvedimenti dell'Autorità già previsti dal Codice, l'articolo 43 introduce una specifica fattispecie delittuosa (nella struttura in parte analoga a quella dell'attuale articolo 167 del Codice) di trattamento illecito di dati personali.

Tale norma sanziona, in particolare, i trattamenti realizzati in violazione di talune specifiche disposizioni ritenute maggiormente rilevanti, con dolo (specifico) di danno o di profitto e in presenza della condizione di punibilità (intrinseca) della determinazione di un nocumento nei confronti dell'interessato.

Il Capo settimo del codice in questione riguarda la riproduzione essenziale delle norme già esistenti per garantire la libera circolazione dei dati personali e la prevenzione dei reati.

Il Capo ottavo, invece, contiene le norme di coordinamento e le abrogazioni, nonché una clausola per garantire l'aspetto finanziario, la quale soddisfa la necessità di avere un quadro giuridico solido e coerente in materia di protezione dei dati personali nell'Unione Europea, con efficaci misure di attuazione.

Dall'analisi sopra effettuata è di palmare evidenza che sia il decreto legislativo n.101/2018 che ha novellato il codice della *privacy* italiano che il GDPR hanno apportato notevoli modifiche e cambiamenti strutturali al concetto del trattamento della circolazione dei dati personali sia in campo europeo che nazionale attuando una maggiore protezione.[111]

Diversamente la Direttiva UE 2016/680 che riguarda il completamento del trattamento dei dati personali a livello Eurounitario è stata di minor impatto rispetto alla precedente.

[111] MARTORANA M., BARBERISI A., PIZZETTI F., *op. cit.,* p. 141.

Tale normativa persegue l'obiettivo di proteggere i dati personali delle persone fisiche che vengono trattati dalle autorità competenti al fine di prevenire, accertare e reprimere i reati che violano la libera e lecita circolazione dei dati.[112]

Pertanto, al fine di prevenire eventuali minacce alla pubblica sicurezza in ambito comunitario, poiché vi è uno scambio di informazioni e di dati tra le autorità nazionali ed europee, è stato ritenuto più opportuno utilizzare il Regolamento UE 2016/679 essendo una norma generale in tema di protezione dei dati personali delle persone fisiche, piuttosto che la Direttiva UE 2016/680 norma di carattere prettamente speciale.

La natura speciale della Direttiva UE 2016/680 al fine di raggiungere gli obiettivi prefissati si occupa in particolare modo del settore giudiziario poiché la prevenzione, l'accertamento e la repressione non possono prescindere dalla tutela della riservatezza e dei diritti fondamentali di ogni essere umano.[113]

La predetta Direttiva inoltre si distingue per la sua conformità ai principi dettati dal GDPR prevedendo ove necessario delle eccezioni per il raggiungimento di determinati obiettivi, poiché tali eccezioni possono essere attuate soltanto se lo Stato membro emani delle norme all'interno del proprio ordinamento giuridico specifiche per la tutela dei dati della persona fisica considerata come singolo.

Il legislatore nazionale mediante il Decreto legislativo n. 51/2018 ha dato attuazione alla Direttiva UE 2016/680 che ha come scopo specifico la prevenzione, l'indagine, l'accertamento ed il perseguimento di reati e l'esecuzione di sanzioni penali nell'ambito del trattamento dei dati personali da parte delle autorità competenti.[114]

---

[112] *Considerandum* n. 7 Direttiva UE n. 16/680.

[113] MARTORANA M., BARBERISI A., PIZZETTI F., op. cit., pp. 143 e 144.

[114] l Decreto in linea con le disposizioni della direttiva recepita ha inteso porre in essere una regolamentazione organica del trattamento dei dati personali effettuato per fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, la quale sostituisce in gran parte quella contemplata nei titoli I e II della seconda parte del Codice.

[561] «*Il trattamento è lecito se è necessario per l'esecuzione di un compito di un'autorità competente per le finalità di cui all'art. 1 comma 2, e si basa sul diritto dell'Unione europea o su disposizioni di legge o, nei casi previsti dalla legge di regolamento che individuano i dati personali e le finalità del trattamento*».

Il D.lgs. n. 51/2018 che ha delineato le condotte punibili in caso di offesa dei diritti dell'interessato nell'ambito del trattamento dei dati personali, in particolare è stato oggetto di critiche dall'articolo 43 all'articolo 46, poiché ha comportato una duplicazione di alcune fattispecie già previste nel vecchio codice della *privacy.*

Invece, le riforme apportate dal D.lgs. 101/ 2018 al D.lgs. n. 196/2003 sono considerate valide anche perché novellate nella maniera adeguata, ma lo stesso non può dirsi per gli articoli dal 43 al 46 del D.lgs. n. 51/2018, che prevedono reati ricalcati in modo pressoché identico alla formulazione del vecchio Codice *Privacy* e tale circostanza ha comportato degli scompensi di trattamento su fattispecie uguali o simili.

Se analizziamo il D.lgs. n. 51/2018 emergono cinque figure di reato per ciascuna delle quali in caso di condanna di un soggetto la relativa sentenza viene pubblicata ai sensi dell'articolo 36 commi 2 e 3 c.p.

Se analizziamo attentamente l'articolo 43 del D.lgs. n. 51/2018 emerge che il legislatore abbia voluto individuare due fattispecie di reato che sono strutturate intorno all'articolo 167 codice della *privacy.*

La prima fattispecie di reato ai fini della sua configurabilità prevede la reclusione da sei mesi ad un anno e sei mesi, nel caso in cui un soggetto violi l'articolo 5 comma 1 del decreto in argomento rubricato "liceità del trattamento" traendone un profitto per sé o per altri o al fine di arrecare un danno altrui.

Per completezza l'articolo 5 comma 1 del D.lgs. n. 51/2018 deve essere ricollegato ad un'altra norma che è l'articolo 1 comma 2 a cui lo stesso rinvia.[115]

Purtroppo, il predetto collegamento tra i due articoli sopra menzionati comporta un duplice passaggio ermeneutico interpretativo che inevitabilmente fa sorgere delle difficoltà interpretative.

Come per gli altri articoli anche in quest'occasione il legislatore ha utilizzato il pronome "chiunque" quando sappiamo benissimo che la fattispecie in oggetto riguardante il trattamento dei dati personali può essere

[115] BRIZZI F., op. cit., p. 178

consumata soltanto da colui che ricopre la carica di funzionario dello Stato che opera nel settore giudiziario.[116]

Il legislatore nonostante la predetta considerazione non ha voluto definirlo come reato proprio per il semplice motivo che nell'ambito del trattamento dei dati personali, spesso si fa ricorso a soggetti esterni piuttosto che a strutture statali, pertanto ha ritenuto opportuno non attribuire relativamente alla predetta fattispecie delittuosa la struttura di reato proprio e pertanto attribuire al soggetto agente una qualifica specifica.

Ai fini dell'imputazione soggettiva del reato rimane invariata come per le altre fattispecie relative a tale ambito l'elemento del profitto e l'aver cagionato un danno altrui che riveste l'ulteriore finalità per la configurazione del dolo specifico.

In questa maniera, lo spazio di operatività della predetta fattispecie rimane molto limitata e circoscritta alla presenza dei due predetti elementi, il profitto per sé o per altri ed il danno incidendo sulla sua effettiva attuazione.[117]

In realtà l'elemento più importante a cui bisogna fare attenzione, affinché la fattispecie incriminatrice in argomento si configuri dovrebbe essere la sola condotta illecita perpetrata attraverso la comunicazione o la diffusione dei dati personali senza il consenso dell'interessato e senza che sia necessaria la contestuale presenza del profitto e del danno.

La fattispecie delittuosa espressamente prevista dal comma 2 dell'articolo 43 D.lgs. n. 51/2018, prevede l'applicazione della reclusione da uno a tre anni, qualora il soggetto agente abbia utilizzato i dati personali in violazione degli articoli 7 e 8 comma 4 per arrecare danno altrui o trarne profitto per sé stesso o per altri, formulazione identica alla normativa *ante* riforma.[118]

---

[116] PIZZETTI F., *op. cit.,* p. 152

[117] TRONCONE P., *op. cit.,* p. 222.

[118] L'attività di trattamento è devoluta con questo provvedimento unicamente all'Autorità pubblica, volendo in questo modo il diritto dell'Unione designare con la lett. g) dell'art. 2 «Autorità competente»: «1) qualsiasi autorità pubblica dello Stato, di uno Stato membro dell'Unione europea o di uno Stato terzo competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; 2) *qualsiasi altro organismo o entità incaricato dagli ordinamenti interni di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica».*

Il legislatore delegato con la predetta figura criminosa, richiama il comma 4 dell'art. 8 che si riferisce a quel trattamento di dati che pone in essere una condotta discriminatoria in relazione alla razza, all'origine etnica, al colore della pelle, alla lingua, alla religione, alle opinioni politiche, alla disabilità e all'orientamento sessuale.

Pertanto, sono stabiliti dalla normativa in argomento la capacità di ingerenza nella sfera privata delle persone che è giustificata dalla salvaguardia di un interesse superiore che è la sicurezza che ha sostituito l'ordine pubblico e la pubblica tranquillità, poiché il bene giuridico tutelato dalla norma è la riservatezza e i diritti fondamentali che devono essere trattati attraverso un corretto utilizzo dei sistemi informatici nel trattamento dei dati giudiziari.[119]

Continuando con la disamina del D.lgs. n. 51/2018 emerge che gli articoli 44 e 45 possono essere annoverati come articoli speculari agli articoli 168 e 170 del Codice *Privacy.*

In particolare l'articolo 44 persegue le falsità di atti, dichiarazioni, documenti o notizie rese al Garante la cui pena comporta la reclusione da sei mesi a tre anni del reo.

L'articolo 44 nel caso del reato di falso nei procedimenti davanti il Garante sia nella fase istruttoria che in quelle successive individua una clausola di sussidiarietà che comporta la punibilità del soggetto attivo tranne se il fatto non costituisca un reato più grave.

Nel predetto reato il bene giuridico tutelato è la fede pubblica e si configura come reato di pericolo e di dolo generico.[120] La condotta di tale reato è considerata a forma libera ed il pronome "chiunque" utilizzato dal legislatore al fine di individuare l'autore del reato configura lo stesso come reato comune[121].

Anche l'articolo 45 che riguarda la condotta illecita relativa al mancato adempimento dei provvedimenti dell'autorità Garante si pone come norma di

---

[119] DE MINICO G., *Costituzione. Emergenza e terrorismo,* Jovene, Napoli, 2016, in particolare da p. 195.
[120] PIZZETTI F., *op. cit.,* p. 152.
[121] CADOPPI A., CANESTRARI S., MANNA A., PAPA M., *op. cit.,* p. 937 e ss.

chiusura ed è considerato un reato a forma libera con dolo generico e rientra tra i reati comuni.

Vi è poi, l'articolo 46 del D.lgs. n. 51/2018 che riguarda le pene accessorie per i reati di cui ai predetti articoli da 43 e 45 che si basano prevalentemente nella pubblicazione della sentenza di condanna penale ai sensi dell'articolo 36 del codice penale.

Alla luce di quanto esposto in precedenza sul D.lgs. n. 51/2018 sono evidenti i difetti di coordinamento con il D.lgs. n. 101/2018, in particolare l'articolo 43 D.lgs. n. 51/2018 è strutturato in maniera speculare sul precedente articolo 167 codice della *privacy,* creando non pochi contrasti e asimmetrie interpretative.

Si verifica, pertanto una discrepanza di trattamento di fattispecie fra i due decreti che hanno da una parte il danno configurato come elemento costitutivo della fattispecie delittuosa, dall'altra invece come condizione obiettiva di punibilità.[122]

Dall'analisi del decreto in argomento si evince che gli articoli 43 e 45 fanno riferimento alla violazione di reati differenti rispetto agli articoli 167 e 170 del codice della *privacy* e che l'articolo 44 viene considerato una norma speciale rispetto all'articolo 168 del codice della *privacy,* tutto ciò crea una duplice qualificazione penale con la conseguenza che possono essere attratte contestualmente in più fattispecie.

Pertanto, sembra opportuno negare qualsiasi concorso formale di reati soprattutto per la necessità di non voler incappare in nessuna violazione del principio del *ne bis in idem,* infatti la presenza dell'una piuttosto che dell'altra fattispecie verrà valutata di volta in volta non essendoci una clausola di sussidiarietà prevista dalle varie fattispecie, poiché sono molto identiche nelle loro previsioni normative.

Dalla predetta analisi si evince che il sistema sanzionatorio che riguarda la protezione dei dati personali presenta delle problematiche che a volte

---

[122] BRIZZI F., *op. cit.,* pp. 180 e 181.

possiedono dei difetti di coordinamento a livello comunitario e nazionale tra le varie discipline, creando un doppio binario amministrativo e penale ai limiti del rispetto del principio del *ne bis in idem*. [123]

In particolare per quanto riguarda la questione del doppio binario sanzionatorio amministrativo e penale relativamente alla materia dei dati personali, molto dipende da una corretta interpretazione ed applicazione dell'articolo 50 della Carta dei diritti fondamentali dell'Unione Europea, la quale non prevede una clausola che opera automaticamente quindi la questione va risolta nella fattispecie concreta al momento in cui si presenta.

Come più volte citato nel rispetto sia della Corte Europea dei diritti umani sia della Corte di Giustizia Europea, qualora nella medesima fattispecie si verificano l'applicazione di sanzioni sia di natura penalistica formale che sostanziale o ci siano sanzioni amministrative sia di natura formale ma sostanzialmente penale è necessario che l'interpretazione sia effettuata dal giudice nazionale volta a dirimere la questione e ad applicare un provvedimento che tenga conto della sanzione amministrativa eventualmente già comminata e irroghi una sanzione penale proporzionata che tenga conto dell'entità di quella amministrativa già applicata.[124]

Nella realtà purtroppo l'interprete ossia il giudice nella fattispecie concreta non ha sempre la lucidità di intervenire adeguatamente e combinare una sanzione che sia proporzionata e che tenga conto del bilanciamento tra il procedimento amministrativo e il processo penale in un doppio binario parallelo, quindi una clausola che operi in maniera automatica sarebbe auspicabile poiché potrebbe salvaguardare in maniera più sicura le sorti del soggetto destinatario della sanzione.[125]

Ulteriore elemento auspicabile sarebbe quello di creare maggiore coordinamento tra le norme del D.lgs. n.51/2018 e le disposizioni del D.lgs. n.101/2018, affinché si possano realmente risolvere le questioni in argomento.

---

[123] BOLOGNINI L., BISTOLFI C., PELINO E., *op. cit.,* pp. 705 e ss.
[124] CADOPPI A., CANESTRARI S., MANNA A., PAPA M., *op. cit.,* p. 1008 e ss.
[125] CADOPPI A., CANESTRARI S., MANNA A., PAPA M., *op. cit.,* p. 1008 e ss.

Infatti, anche se le sopra citate norme disciplinano diverse fattispecie e diversi campi riguardanti il trattamento dei dati personali si sono verificati fra di loro degli accavallamenti a causa del fatto che il D.lgs n. 51/2018 ricopia delle norme ormai del tutto abrogate del D.lgs. n. 196/2003**.**

Infatti, a conferma di quanto sopra argomentato l'articolo 43 del decreto legislativo n. 51/2018 è perfettamente identico all'articolo 167 del vecchio codice della *privacy* tale circostanza ha creato molte difficoltà interpretative, poiché la formulazione della norma precedente a cui si riferisce l'art. 43 è stata abrogata.

A conferma di ciò nella nuova formulazione il danno è l'elemento costitutivo della fattispecie criminosa, invece, nelle norme ante riforma il danno è la condizione obiettiva di punibilità su cui è costituita l'intera fattispecie criminosa.[126]

Il D.lgs. n. 51/2018 si pone in una posizione di specialità rispetto alle norme del codice della *privacy,* questo non è sufficiente ad eliminare eventuali circostanze che sono al limite della violazione del principio del *ne bis in idem*, non servendo quasi a nulla la presenza di clausole di sussidiarietà che sono contenute nella norma, poiché le une sono uguali alle altre e per tale motivo non è possibile distinguere l'applicazione dell'una o dell'altra norma al caso concreto.

Basterebbe che ci fosse un intervento decisivo da parte del legislatore delegato volto a coordinare le predette norme del sistema sanzionatorio allo scopo di dirimere eventuali difficoltà interpretative.[127]

In realtà la soluzione più auspicabile sarebbe realizzare un intervento legislativo di riforma del sistema sanzionatorio anche se in effetti ciò è accaduto con il decreto legislativo n. 139/2021, anche se tale riforma ha riguardato un intervento ampliativo dei poteri afferenti al Garante in relazione ai reati riguardanti la figura del r*evenge porn*, e inoltre, anche in relazione all'aumento delle risorse per il finanziamento della figura del Garante.

---

[126] PIZZETTI F., *op. cit.,* p. 151.

[127] BRIZZI F., *op. cit.,* p. 177: l'autore ritiene in tal caso che la Giurisprudenza dovrà necessariamente confrontarsi con il principio secondo il quale *ubi lex voluit dixit,* rinvenendo non poche difficoltà interpretative ed applicative delle norme in esame.

Ad ogni modo il decreto legislativo 139/2021 ha in un certo qual modo ridimensionato il ruolo del Garante in ordine alla sua funzione di controllo preventiva sulla tutela dei dati personali e anche in relazione ai provvedimenti adottati dalle autorità competenti.[128]

Il recente intervento di novellazione del codice della privacy ha completamente abrogato l'articolo 2 *quinquiesdecies* del D.lgs. n. 196/2003 che obbligava la Pubblica Amministrazione prima di porre in essere trattamenti ad alto rischio come ad esempio i dati sanitari o dati di interesse pubblico, di consultare il Garante il quale era investito di poteri che gli consentivano eventualmente di intervenire preventivamente a tutela del soggetto interessato.

Una volta abrogato tale articolo, il Garante non avrà più alcun potere di intervento preventivo per correggere eventualmente gli errori o le falsità che si possono verificare all'interno di dati personali ad alto rischio.[129]

Altre modifiche sono state apportate all'articolo 2 *ter* del codice della *privacy,* relativamente al trattamento dei dati effettuati da parte della Pubblica Amministrazione con l'introduzione del comma 1 *bis* sempre al predetto articolo, che sancisce che il trattamento effettuato da parte della pubblica autorità è sempre consentito quando è necessario per lo svolgimento di un

---

[128] MARATONA M., *Decreto Capienze: come è intervenuto sul codice della Privacy. Il rapporto tra il trattamento dei dati personali dei cittadini e le finalità di interesse pubblico, le modifiche ai poteri del Garante, le misure in tema di revenge porn,* Altalex, 13.10.2021. L'autore ha avuto modo in tale sede di riportare le considerazioni di Franco Pizzetti, costituzionalista ed ex Presidente dell'Autorità garante, con riguardo alla modifica normativa intervenuta in tema di *privacy* e tutela dei dati personali, che ha definito come "un intervento pesante".

[129] MARATONA M., Op.cit..
Il Decreto agirebbe, dunque, come una sorta di nulla osta preventivo sull'attività della Pubblica Amministrazione, che potrà trattare e comunicare dati anche senza specifica norma di legge. Tale depauperazione della funzione legislativa in favore della Pubblica Amministrazione si pone come alquanto preoccupante, si affida, infatti, al soggetto agente il compito di limitare la propria azione, aprendo la strada ad una sorta di libero arbitrio della P.A.
Inoltre, tale norma si pone come pericolosa per la sua indeterminatezza e la modifica apportata al Codice della *privacy*, così come posta, presta il fianco a profili di incostituzionalità, in ordine ad una presunta violazione del GDPR (gerarchicamente superiore alle norme nazionali) il quale, invece, prevede che l'interesse pubblico venga definito con norma di legge.

compito di interesse pubblico e nell'esercizio di poteri pubblici, aprendo però delle maglie di preoccupazione sulla riservatezza dei cittadini.

Inoltre, altrettante perplessità ha destato l'abrogazione del comma 5 dell'articolo 132 del codice della *privacy* che stabiliva che il trattamento dei dati personali effettuato per la prevenzione dei reati doveva essere svolto soltanto per i dati conservati rispettando tutti i dettami di qualità e sicurezza per la tutela dei dati personali trattati in rete, cosi come espressamente stabilito nella riforma del 2018 sulla base delle disposizioni del nuovo GDPR.

Pertanto, il decreto diventerebbe come un preventivo nullaosta sull'attività della pubblica amministrazione che potrà trattare i dati anche senza una specifica norma di legge.

Tale norma per la sua indeterminatezza, così per come è stata creata può avere profili di incostituzionalità in ordine alla violazione delle disposizioni del GDPR, la quale invece prevede che l'interesse pubblico venga definito con una norma di legge.

La Legge n. 205/2021, che ha convertito il Decreto Capienze ha apportato delle modifiche all'apparato sanzionatorio amministrativo del Codice della *Privacy* ed in particolare con la modifica dell'art. 166 del Codice della *Privacy* e con l'ampliamento del potere sanzionatorio riconosciuto al Garante.

L'articolo 166 codice della *privacy* comma 5 nella sua nuova struttura e formulazione prevede l'omissione della previa notifica nel caso in cui si verifichi una violazione che viene contestata all'autorità pubblica che tratta i dati e che abbia già arrecato pregiudizio agli interessati, in questo modo conferendo ampi poteri alla Pubblica Amministrazione.

Il legislatore delegato mediante il decreto Capienze ha modificato anche l'articolo 170 del codice della privacy stabilendo la procedibilità a querela di parte e quindi riducendo il campo di azione punitiva della predetta norma.

Di contro sono state viste con favore dagli addetti lavori, le modifiche che sono state realizzate nei confronti dell'articolo 166 codice *privacy* comma 7 che riguardano l'autorità Garante nei confronti del quale è stato previsto accanto al potere sanzionatorio negativo un potere positivo di promozione.

A tal proposito il Garante avrà il potere di imporre ad alcune imprese di effettuare investimenti sulla formazione e sulla tutela dei dati personali in materia di *privacy.*

L'intervento del legislatore nazionale è stato di particolare importanza soprattutto sotto alcune fattispecie come il *revenge porn* e l'ampliamento dei poteri all'autorità Garante, passaggio fondamentale per fronteggiare il fenomeno è stata l'approvazione della legge 29 luglio 2019, n. 69, meglio conosciuta come "Codice Rosso", con la quale il Revenge porn è diventato in Italia reato punibile con la reclusione da uno a sei anni e con la multa da euro 5mila a euro 15mila.

5. Il D.L. n. 139/2021: c.d. Decreto Capienze

Di recente con l'emanazione del Decreto-legge 8 ottobre 2021, n. 139[130], cd. Decreto Capienze, convertito dalla Legge 3 dicembre 2021, n. 205, entrato in vigore l'8 dicembre 2021, sono state introdotte ulteriori modifiche al codice della *privacy.*

Tra le più importanti modifiche, vi è l'articolo 2 *ter* del codice della *privacy* che prevede un ampliamento giuridico del trattamento dei dati personali, infatti la sua nuova formulazione al comma 1 prevede che sia l'art. 2 *sexies* del codice della *privacy* e sia l'articolo 6, paragrafo 3, lettera b) del Regolamento europeo, siano composti oltre che da leggi e regolamenti anche da atti amministrativi generali.[131]

Con il decreto Capienze si è anche modificato l'articolo 2 *quinquiesdeces* del Codice della *Privacy* relativamente ad alcune funzioni del Garante al quale gli è stata attribuita la competenza di emanare provvedimenti di natura generale e di disporre di misure nei confronti del titolare dei trattamenti ai

---

[130] Decreto-legge 8 ottobre 2021, n. 139, recante disposizioni urgenti per l'accesso alle attività culturali, sportive, ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali.

[131] Art. 2 ter, comma 1 Codice privacy: «*La base giuridica prevista dall'articolo 6, paragrafo 3, lettera b), del regolamento è costituita da una norma di legge o. di regolamento o da atti amministrativi generali».*

sensi dell'art. 35 del GDPR esposti a particolari rischi per l'esecuzione di un pubblico interesse.

Da un altro punto di vista, mediante l'introduzione dell'articolo 144 *bis* codice della *privacy* è stato conferito al Garante un potere in materia di *revenge porn* che si riferisce a chiunque, compresi i minori con più di 14 anni di rivolgersi attraverso segnalazioni al Garante, qualora vi sia fondato motivo di ritenere che vi siano immagini, video, registrazioni o documenti informatici privati che possono essere ceduti, pubblicati o consegnati senza il consenso dell'interessato e che hanno per oggetto immagini di atti sessuali.[132]

Il revenge porn e, più in generale, il fenomeno della pornografia non consensuale, consiste nella diffusione di immagini pornografiche o sessualmente esplicite a scopo vendicativo per denigrare pubblicamente, bullizzare e molestare la persona cui si riferiscono.

Si tratta quindi di una pratica che può avere effetti drammatici a livello psicologico, sociale e anche materiale sulla vita delle persone che ne sono vittime.

Il Garante, quando riceve la segnalazione ha quarantott'ore di tempo dal ricevimento per provvedere ai sensi degli artt. 143 e 144 del Codice *Privacy.*

In particolare l'art. 143 codice *privacy,* prevede che una volta terminata la fase istruttoria se vi sono i presupposti per l'emanazione di un provvedimento ed il reclamo non è manifestamente infondato, il Garante, prima del termine del procedimento può adottare i provvedimenti di cui all'articolo 58 del Regolamento che riguardano nello specifico, il trattamento di dati per fini di sicurezza nazionale e difesa.

Se i relativi destinatari non sono facilmente identificabili per il numero o per la complessità degli accertamenti, i predetti provvedimenti sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana.

---

[132] Art. 144 bis, comma 1 del Codice privacy: «*Chiunque, compresi i minori ultraquattordicenni, abbia fondato motivo di ritenere che registrazioni audio, immagini o video o altri documenti informatici a contenuto sessualmente esplicito che lo riguardano, destinati a rimanere privati, possano essere oggetto di invio, consegna, cessione, pubblicazione o diffusione attraverso piattaforme digitali senza il suo consenso ha facoltà di segnalare il pericolo al Garante, il quale, nelle quarantotto ore dal ricevimento della segnalazione, decide ai sensi degli articoli 143 e 144 del presente codice».*

Entro tre mesi dalla data del deposito del reclamo, il Garante fornirà notizie sullo stato del procedimento, comunicando che entro 9 mesi dalla data di presentazione, il procedimento volgerà a conclusione con il provvedimento con cui deciderà il reclamo.

L'art. 144 codice *privacy,* invece, prevede la possibilità per chiunque, di effettuare segnalazioni al Garante, il quale valuterà la fattispecie sottoposta al suo esame, anche ai fini dell'emanazione dei provvedimenti di cui all'articolo 58 del Regolamento.

Inoltre, il D.L. n. 139/2021, introduce una modifica all'art. 166 Codice *Privacy,* che stabilisce che il Garante ha il potere nel caso in cui applichi sanzioni amministrative, di proporre attività di comunicazione istituzionale, intendendo l'insieme di tutte quelle strategie di comunicazione, utilizzate da una istituzione per informare in modo diretto e univoco una comunità su un argomento sociale che accomuna tutti i diretti destinatari.

Con l'obiettivo di promuovere la consapevolezza del diritto alla protezione dei dati personali, sulla scorta di programmi preventivamente approvati dal Garante che tengano conto della proporzionalità e della gravità della violazione [133].

6. Le integrazioni effettuate dal D.lgs. n. 101/2018 e dal D.L. n. 39/2021 al sistema sanzionatorio

La combinazione tra il Regolamento numero 679/2016 che ha abrogato la Direttiva n. 95/46 ed il D.lgs. n.101/2018 che ha novellato lasciandolo in vita il D.lgs. n. 196/2003 Codice Privacy è stata possibile mediante l'intervento del legislatore nazionale, il quale al fine di omogenizzare e rendere più

[133] Art. 166, comma 7 del Codice privacy: "*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 o dell'ingiunzione a realizzare campagne di comunicazione istituzionale volte alla promozione della consapevolezza del diritto alla protezione dei dati personali, sulla base di progetti previamente approvati dal Garante".*

uniforme il diritto interno con il diritto comunitario ha dovuto effettuare un intervento mediante la tecnica della novellazione che consiste in un opera interpretativa finalizzata ad abrogare le norme completamente incompatibili e ad adeguare le norme già esistenti ai nuovi dettami di connessione con il Regolamento realizzando una normativa omogenea sulla protezione dei dati personali e sulla libera circolazione degli stessi.

La predetta normativa è sempre in continua evoluzione, poiché la società e le tecnologie continuano sempre a modificarsi per tale motivo il legislatore è intervenuto ad effettuare un'altra modifica del D.lgs. 196/2003 attraverso il cosiddetto Decreto Capienze Decreto Legge 8 ottobre 2021 n. 139 convertito in Legge il 3 dicembre 2021, n. 205.

Le novità più rilevanti del D.lgs. n. 101/2018 riguardano le modifiche introdotte al sistema sanzionatorio e soprattutto relativamente al ruolo delle sanzioni nella normativa europea con riguardo alla protezione dei dati personali.

A tal proposito l'articolo 83 del Regolamento nello specifico attribuisce all'autorità competente per il controllo la possibilità di applicare due tipologie di sanzioni amministrative, una prevede una sanzione pecuniaria fino a € 10.000.000 per le persone fisiche o per le imprese fino al 2 % del fatturato mondiale totale annuo, invece, ci sono altre sanzioni più rigorose che vengono applicate in caso di violazioni di più grave entità fino a € 20.000.000 applicate alle persone fisiche o alle imprese fino a 4% del fatturato mondiale totale annuo.

La predetta tipologia di sanzioni ha sicuramente aspetti positivi sulla tutela dei dati personali soprattutto per due motivazioni.

In primis essa fa riferimento ai poteri dell'autorità di controllo (i.e. il Garante), al quale vengono conferiti degli strumenti, capaci di tutelare l'interessato dagli attori principali del sistema di gestione, chiamati *big player tecnologici*, i quali nella precedente normativa del codice privacy avevano una posizione dominante a discapito dell'interessato.

In secondo luogo, si evidenzia l'eliminazione del minimo edittale che conferisce al soggetto competente che applicherà la sanzione una valutazione da effettuare volta per volta, specifica per ogni singola fattispecie.

In questa maniera l'entità della sanzione sarà frutto della valutazione non solo della entità della violazione commessa, ma terrà conto anche delle dimensioni e della tipologia del soggetto sanzionato. [134]

Le sanzioni da applicare devono essere ai sensi dell'art. 83 del Regolamento "effettive, proporzionate e dissuasive", stabilendo che l'Autorità di controllo nazionale deve seguire dei criteri espressamente stabiliti dal predetto articolo che consistono: nella natura della violazione, nella gravità della stessa, nella durata della violazione, nell'elemento psicologico soggettivo, ossia nel dolo o nella colpa da parte del reo e l'eventuale beneficio tratto da tale attività illecita.

Il Regolamento sembra prevedere illeciti che secondo parte della dottrina,[135] non rispettano il principio di tipicità nella individuazione del precetto.

A tal proposito, il legislatore europeo nel riassettare la normativa ha lasciato le sanzioni in modo generico sia nell'individuazione del reato che nell'applicazione del trattamento sanzionatorio introducendo però la previsione del danno come elemento caratterizzante in alternativa allo scopo di profitto.

---

[134] La *ratio* di tale abrogazione si individua 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.
Si pensi ad un soggetto titolare quale può essere un libero professionista come ad esempio un piccolo studio commerciale, o ancora un soggetto quale un artigiano che potrebbe vedersi irrogare una sanzione che, seppure nel suo minimo edittale, potrebbe porsi come del tutto sproporzionata alle dimensioni del soggetto stesso e quindi potrebbe avere un impatto devastante sullo stesso.

[135] D'AGOSTINO L., *op. cit.*, pp. 21 e ss. «*La genericità della formula utilizzata non rende affatto chiaro quale sia il margine di manovra lasciato agli Stati membri. L'elasticità della cornice edittale descritta con la locuzione "fino a" – sembrerebbe prima facie consentire ai legislatori nazionali la possibilità di differenziare la risposta sanzionatoria in base alla gravità delle violazioni; ma non è escluso che essi prediligano una lettura "minimalista", richiamando sic et simpliciter le disposizioni del Regolamento per non incorrere in procedure di infrazione».*

Dunque non si terrà contro del solo profitto economico dell'autore dell'illecito ma anche del danno arrecato agli interessati, compreso il danno d'immagine e reputazionale della vittima.[136]

Una parte della dottrina, ritiene che tale impostazione non sia accettabile considerandola non una lacuna del Regolamento, bensì come una consapevole scelta del legislatore comunitario adottata per rendere più effettiva la tutela della persona [137].

In questo modo l'articolo 83 sarebbe omnicomprensivo, poiché tutte le volte che vi sia una violazione del Regolamento sarà legittimo l'intervento dell'autorità Garante, la quale potrà applicare una sanzione amministrativa pecuniaria al caso concreto.

Il successivo articolo 84 del Regolamento disciplina due diversi aspetti. Da una parte attribuisce agli Stati membri il potere di prevedere e di inserire altre sanzioni in relazione ad eventuali violazioni non previste dall'articolo 83 del regolamento, dall'altra delinea la procedura relativa all'adozione di provvedimenti sanzionatori che il Garante è competente ad irrogare.

Il sistema sanzionatorio strutturato dal legislatore nazionale prevede nello specifico le modalità procedurali mediante le quali il Garante può emettere dei provvedimenti sanzionatori con la relativa abrogazione di tutte quelle sanzioni amministrative previste dal codice *privacy* prima della riforma.[138]

Al fine di attuare il principio penalistico del *favor rei* vi è un'alternanza delle sanzioni amministrative espressamente previste dal GDPR con le sanzioni penali previste dal vecchio codice della *privacy*, ciò è possibile purché non sia stata emessa nel procedimento penale una condanna definitiva passata in giudicato.

---

136 D'AGOSTINO L., op. cit., pp. 21 e ss. "*La genericità della formula utilizzata non rende affatto chiaro quale sia il margine di manovra lasciato agli Stati membri. L'elasticità della cornice edittale."*

137 SCAGLIARINI S., *Il nuovo codice in materia di protezione dei dati personali: la normativa italiana dopo il d.lgs. n. 101/2018,* 2019, 299 e ss.

138 PANETTA R., *Decreto di adeguamento GDPR, cit.*

A tal proposito il legislatore nazionale prevede la depenalizzazione al fine di evitare il rischio di violazione del principio del *ne bis in idem* tra sanzioni penali ed amministrative.

E' di palmare evidenza che il D.lgs. n. 101/2018 ha introdotto nuove fattispecie criminose come gli articoli 167 terzo comma, 167 *bis* e 167 *ter,* codice *privacy,* riformando sostanzialmente il sistema sanzionatorio *ex ante,* facendo sì che le sanzioni penali potessero essere applicate in quelle fattispecie in cui fosse accertato l'elemento costitutivo del dolo in capo all'autore del reato e con l'obiettivo da parte dello stesso di ottenere un vantaggio per sé o per gli altri e anche con lo scopo di arrecare danno e pregiudizio agli altri.

In questa maniera il legislatore nazionale ha voluto inserire il danno come elemento caratterizzante le fattispecie di reato in argomento.

Alla luce delle norme incriminatrici introdotte con il decreto legislativo 101/2018 in connessione con le disposizioni del GDPR si evince chiaramente che l'intervento relativo alle fattispecie penali è residuale rispetto alle sanzioni amministrative così come espressamente indicato dal legislatore europeo con il Regolamento.

6.1 (*segue)* Illeciti amministrativi e violazioni penali

Come abbiamo già constatato nelle pagine precedenti, l'articolo 83 del Regolamento prevede un primo gruppo di illeciti a cui sono previste l'applicazione di sanzioni amministrative, in tale gruppo sono annoverati gli articoli 8, 11 e dagli articoli 25 al 39, 42 e 43 del regolamento, nei quali vi rientrano tutte le violazioni degli obblighi imposti dal Regolamento nei confronti dei soggetti attivi del trattamento dei dati personali, ossia in particolare il titolare ed il responsabile.

Il Regolamento europeo al fine di proteggere i dati personali impone al titolare del trattamento di adottare tutte le misure tecniche ed organizzative capaci di tutelare in maniera ottimale e sicura i dati personali dai trattamenti illeciti.

L'articolo 8 si occupa della fattispecie relativa al trattamento dei dati personali offerti direttamente ai minori da parte di una società di informazione, l'offerta è lecita se il consenso del minore proviene da colui che ha compiuto almeno 16 anni di età, nel caso in cui abbia meno di 16 anni è necessario, affinché il trattamento sia lecito, che il consenso sia prestato dal titolare della responsabilità genitoriale.[139]

Invece, non è sempre di immediata interpretazione l'articolo 11 relativo all'applicazione della sanzione amministrativa, poiché, al primo comma, non emerge in maniera chiara l'obbligo nei confronti del titolare del trattamento, il quale nel caso in cui non sia in possesso di dati sufficienti all'identificazione dell'interessato, il titolare non dovrebbe avere alcun obbligo di trattazione, invece il secondo comma dell'articolo 11 prevede che in caso di dati insufficienti all'identificazione dell'interessato, il titolare ha il dovere di informarlo, da qui l'incomprensione a conciliare le due situazioni, ossia se il titolare non possiede sufficienti dati per identificare l'interessato di contro come potrà informarlo di tale circostanza.[140]

L'articolo 25, in particolare, prevede l'introduzione del principio *di privacy by design e privacy by default*, ossia un progetto innovativo che obbliga le aziende a predisporre fin da subito gli strumenti e le corrette impostazioni a tutela dei dati personali.

In particolare nel 2010 era già presente negli Usa e in Canada il concetto *di privacy by design*, la cui definizione fu coniata da *Ann Cavoukian, Privacy Commissioner* dell'Ontario Canada e si sviluppa attraverso vari concetti, quali la prevenzione, ossia la valutazione di eventuali rischi, già nella fase di progettazione.

---

[139] Regolamento UE 2016/679, *considerandum* n. 38, ai sensi del quale al minore viene ad essere dedicato, dal regolamento, una attenzione particolare, con una specifica protezione dei loro dati personali, poiché il legislatore dell'Unione ritiene che la percezione «*dei rischi delle conseguenze e delle misure di salvaguardia interessate, nonché dei diritti in relazione al trattamento dei dati personali*», sia, nel minore, del tutto inferiore rispetto ad un soggetto maggiorenne.

[140] CASSANO G., COLAROCCO V., GALLUS G.B., MICOZZI F.P., SORO A., BARBAROSSA M., *op.*

L'utilizzo di tecniche di pseudonimizzazione o minimizzazione dei dati, consente la libertà di compilare o meno un campo di un form assicurando la sicurezza e trasparenza durante tutto il ciclo del servizio.

E soprattutto le tempestive e chiare risposte alle richieste dell'utente di accedere nel rispetto dei suoi diritti fondamentali.

Inoltre, l'articolo 28 del Regolamento prevede l'applicazione della sanzione amministrativa nei confronti del titolare del trattamento qualora abbia nominato un responsabile che non aveva competenze tecnico organizzative pertinenti con il lavoro assegnato o quando le violazioni poste in essere dal responsabile si riferiscono al mancato adempimento di fornire informazioni al titolare relative alla nomina di eventuali sub responsabili.

Invece, l'articolo 32 prevede l'applicazione di sanzioni amministrative nel caso in cui il titolare e il responsabile pongano in essere delle violazioni amministrative in ordine all'applicazione di misure tecniche organizzative che non erano adeguate a garantire un elevato grado di sicurezza in proporzione al rischio accertato.

Infine, gli artt. 42 e 43 del Regolamento, si riferiscono all'impegno di attuare idonee garanzie che rispettano i diritti fondamentali dell'interessato[141].

L'altro gruppo di violazioni sono invece più severe, e sono individuabili al comma 5 dell'art. 83, a cui fa riferimento la sanzione amministrativa il cui ammontare può arrivare sino a fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente[142], in particolare si tratta di violazioni dei principi base del trattamento comprese le norme sul consenso e sui diritti degli interessati.

Pertanto, al fine di evitare un'applicazione delle sanzioni automatizzata il comma 2 dell'art. 83 stabilisce che nell'irrogazione della sanzione i principi che devono essere valutati per la sua applicazione riguardano: la gravità, la durata della violazione, l'elemento doloso o colposo, le misure tecniche organizzative adottate per diminuire i rischi, il modo con cui l'Autorità è

---

[141] CASSANO G., COLAROCCO V., GALLUS G.B., MICOZZI F.P., SORO A., BARBAROSSA M., *op. cit.,* 393 e ss.

[142] Art. 83, comma 5 del GDPR.

venuta a conoscenza dell'illecito, l'eventuale adesione a codici di condotta, e l'eventuale presenza di condizioni attenuanti o aggravanti applicabili alla fattispecie del caso concreto.

In ogni caso l'art. 83 è costituito da una variegata lista di violazioni per le quali vengono comminate pesanti sanzioni pecuniarie.

L'obiettivo del Regolamento è quello di adottare un sistema sanzionatorio efficace che possa dissuadere la commissione da atti illeciti con sanzioni che siano comunque proporzionate alla gravità delle violazioni commesse.[143]

Il legislatore europeo sembra che abbia voluto affidare all'introduzione dell'art. 83 l'intero impianto sanzionatorio creando una forbice amplissima nella quale vi sono svariate violazioni che a sua volta si distinguono in due categorie quella più grave e quella meno grave senza previsione di un minimo edittale.

Il metodo redazionale adoperato si basa sul concetto secondo il quale è indispensabile delineare un sistema sanzionatorio che sia efficace, dissuasivo e con sanzioni strettamente proporzionate alla gravità della violazione posta in essere.

Dunque, il legislatore europeo, attraverso la creazione di sanzioni molto gravi, le quali, giova ribadire, non prevedono neanche un minimo edittale non ha raggiunto lo scopo prefissato, poiché ha lasciato all'operatore del diritto il compito di interpretare volta per volta la sanzione più adeguata da applicare.

Inoltre, è possibile che si verifichi l'applicazione della medesima sanzione con riguardo a violazioni tra loro molto differenti, come ad esempio nel caso delle violazioni in materia di certificazioni, ossia nella fattispecie della protezione del trattamento dei dati personali e nell'omissione della tenuta del registro dei trattamenti, le predette pur essendo condotte differenti soggiacciono alla stessa sanzione, nonostante la protezione dei dati personali consista nella violazione di misure obbligatorie e l'altro illecito invece, consiste in una violazione solo eventuale.

Nella stessa direzione si muove la violazione relativa all'inosservanza dell'obbligo di notifica del *data breach,* il quale viene ad essere sanzionato

[143] MALGIERI G., Inquadramento normativo, cit., 5.

con gli stessi limiti edittali della semplice omissione di consultazione preventiva del Garante.

In particolare, l'obbligo di segnalare il *Data Breach* risiede in capo al titolare del trattamento o al responsabile, i quali hanno l'obbligo entro 72 ore di notificare la violazione al Garante per la protezione dei dati personali, in alcuni casi di comunicare la violazione alle singole persone fisiche i cui dati personali siano stati violati, a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle predette persone fisiche.

Pertanto, la genericità della formula sulla gradualità del trattamento sanzionatorio insinua delle perplessità sul margine di manovra degli Stati membri, i quali vorrebbero diversificare le sanzioni combinandole in ordine alla gravità della violazione, in Italia, invece, pare più semplice richiamare il Regolamento per evitare di incorrere in procedure di infrazione.

Alla luce delle argomentazioni sopra esposte e dall'analisi della ricostruzione precettiva, il legislatore europeo spesso pone in essere richiami *de relato* ad altre normative che però a loro volta si riferiscono ad altri destinatari, come nel caso dell'articolo 38 che prevede la funzione del responsabile della protezione dei dati e contestualmente disciplina anche gli obblighi a carico del titolare e del responsabile del trattamento, la predetta circostanza crea indubbiamente non pochi problemi interpretativi.

Alle predette violazioni sul piano giuridico nazionale sono state accostate le disposizioni del codice della *privacy* modificato e novellato dal D.lgs. n. 101/2018 e dal D.L.n.139/2021 finalizzato ad armonizzare la materia del trattamento dei dati personali con la normativa europea e modificando parte del codice *privacy* anche con l'introduzione dell'art. 166 che riguarda le violazioni di natura amministrativa, il quale prevede una lunga nomenclatura di violazioni prevedendo a seconda della fattispecie l'applicazione delle sanzioni di cui ai paragrafi 4 e 5 del GDPR, essendo un migliore collettore rispetto l'art. 83 del Regolamento.[144]

[144] PANETTA R., Decreto di adeguamento GDPR, cit.

Per quanto riguarda l'art. 166 Codice della *Privacy* il legislatore italiano rinvia alla sanzione prevista dall'art. 83, paragrafo 4, del Regolamento, nella fattispecie in cui si sia verificata una violazione delle disposizioni di cui all'articolo 2 *quinquies,* co. 2 del codice *privacy* riguardante l'informativa da sottoporre ad un minore di 14 anni a cui è stata effettuata una offerta diretta di servizi da una società di informazione, la predetta offerta deve risultare semplice e facile da comprendere qualora non dovesse rispecchiare tali canoni, comporta l'irrogazione delle sanzioni previste dall'art. 83 del Regolamento, fino a dieci milioni di euro o applicabile in parametrazione al fatturato dell'impresa, fino al 2%.

Invece, in ordine all'abrogazione dell'articolo 2 *quinquesdecies* codice della privacy, riguardante i trattamenti svolti per compiti di interesse pubblico o dati particolarmente sensibili essendo stato abrogato non vi è più la predetta violazione con delle conseguenze non molto incoraggianti per la tutela dei dati personali dei privati cittadini, poiché il diritto alla protezione dei dati personali riguarda anche «*l'interesse generale alla liceità e correttezza al trattamento, caratterizzandosi per la sua duplice natura di interesse individuale e interesse collettivo».*

Il nuovo articolo 166, codice *privacy* inoltre, prevede che possono essere sanzionate le violazioni realizzate dai fornitori di reti pubbliche di comunicazione elettronica accessibili al pubblico, quando pongono in essere le seguenti attività illecite: mancata adozione di tutte le misure e di tutte le procedure idonee per consentire all'utente in maniera semplice e gratuita di poter bloccare il trasferimento delle chiamate da parte di terzi verso il proprio terminale e comunque nella violazione di tutte quelle disposizioni che prevedono l'inserimento dei dati negli elenchi cartacei ed elettronici pubblici[145].

Invece, il secondo comma dell'articolo 166 sancisce sanzioni notevolmente più severe, poiché riguardano violazioni più gravi che hanno ad oggetto l'art. 2 *ter* del codice privacy, (fino a venti milioni di euro, o, ancora

[145] CASSANO G., COLAROCCO V., GALLUS G.B., MICOZZI F.P., SORO A., BARBAROSSA M., *op. cit.,* 402 e 403

una volta, parametrata al fatturato dell'impresa, in questo caso al 4%) riguardanti i trattamenti di cui è competente il titolare posti in essere nell'interesse pubblico o connesso all'esercizio di pubblici poteri per i casi in cui non vi sia una specifica norma di legge.

Nella normativa precedente i predetti compiti venivano svolti dal titolare soltanto in casi specifici stabiliti da legge o da regolamento, invece, nell'attuale formulazione la norma giuridica prevede una estensione anche agli atti amministrativi generali.

Pertanto, alla luce di quanto attiene all'articolo 2 *ter* codice *privacy*, si è davanti ad un ampliamento della norma giuridica per ragioni di pubblico interesse, grazie alle modifiche è sempre consentito il trattamento dei dati personali quando è strumentale allo svolgimento di un obiettivo di pubblico interesse o all'esercizio di pubblici poteri.[146]

Inoltre, si applicherà in caso di violazione dell'articolo 2 *quinquies* comma 1 che riguarda la violazione del trattamento dei dati di un soggetto infra quattordicenne posta in essere senza il suo consenso o se minore di 14 anni senza il consenso di chi esercita la responsabilità genitoriale, la sanzione espressamente stabilita dal comma 2 dell'articolo 166 codice *privacy*.

Ancora più aspre saranno le sanzioni in caso di violazione dell'art. 2 *sexies* che riguardano il trattamento di particolari tipologie di dati per motivi di pubblico interesse, nel quale il diritto interno indica i dati specifici che possono essere trattati, le modalità attraverso cui tale trattamento deve avvenire, le attività svolte sui predetti dati, il motivo dell'interesse pubblico rilevante che giustifica tale trattamento e le operazioni adottate per tutelare i diritti fondamentali dell'individuo con conseguente applicazione della sanzione amministrativa di cui sopra in caso di violazione.

Infatti, le sanzioni indicate dal comma 2 dell'art. 166 codice privacy, possono essere applicate anche per la violazione dell'art. 2 *septies*, comma 8

[146] Con tale modifica, dunque, il trattamento dei dati comuni per finalità di interesse pubblico da parte delle amministrazioni diventa sempre lecito, e se la finalità non è prevista dalla legge, la PA può indicarla con un suo atto e procedere senza intralcio al trattamento che ritiene necessario per adempiere ai propri compiti ed esercitare i poteri attribuiti.

del Codice Privacy, sul divieto di diffusione dei dati genetici, biometrici e relativi alla salute delle persone e per la violazione dell'art. 2 *octies* che riguarda il trattamento dei dati relativi a condanne penali a misure di sicurezza e a reati.

Inoltre, il predetto comma 2 dell'art. 166 codice *privacy* può trovare applicazione anche nel caso di violazione dell'esercizio dei diritti sanciti dagli artt. 15 a 22 GDPR, in ordine ai dati personali di soggetti defunti o da colui che non ha il consenso dell'avente diritto e non possiede un proprio interesse, e anche nel caso in cui l'interessato riceva un'offerta diretta di servizi delle società di informazione e abbia dichiarato per iscritto al titolare il divieto di utilizzare i propri dati personali.

A tal proposito, il legislatore nazionale ha individuato dei particolari illeciti amministrativi sui trattamenti dei dati personali che colpiscono l'ambito lavorativo riguardanti violazione di regole deontologiche da parte del datore di lavoro, il quale non ha posto in essere tutte le misure idonee a garantire un trattamento tutelato e quindi esponendo il lavoratore a dei rischi attinenti alla propria riservatezza.

Altrettanto severa è la sanzione di cui all'articolo 166 secondo comma, qualora siano stati violati gli articoli 96, 99 e 100 ai commi 1, 2 e 4 del codice, il quale configura come illecito amministrativo la condotta di colui che consente la circolazione dei dati personali senza il consenso degli studenti per obiettivi e scopi differenti rispetto a quelli per cui sono stati acquisiti, quindi al di fuori della formazione e dell'inserimento professionale, nonché la violazione delle norme sull'archiviazione e sulla diffusione di tali dati in difformità alle norme espressamente previste in materia.

In particolare il D.lgs. n. 101/2018 novellando il codice della *privacy* ha previsto che il presunto trasgressore abbia 30 giorni di tempo per presentare scritti difensivi ed essere ascoltato dall'autorità Garante.

Il Garante attraverso un'istruttoria, dopo aver sentito gli interessati ed esaminato la documentazione in atti potrà o emanare un'ordinanza di ingiunzione, oppure potrà emettere un'ordinanza di archiviazione motivata.

In ordine all'ordinanza di ingiunzione chi ha interesse tra le parti del procedimento potrà fare ricorso, ovvero potrà accettare il provvedimento emesso dal Garante nei suoi confronti e pagare la relativa sanzione amministrativa.[147]

Ancora con il Decreto Capienze il legislatore italiano è intervenuto ulteriormente a modificare l'articolo 166 codice privacy perciò che riguarda il trattamento dei dati personali da parte delle pubbliche amministrazioni.

A tal proposito, il legislatore sul predetto articolo in particolare al comma 5 nella nuova rielaborazione ha voluto conferire ampi poteri alla pubblica amministrazione nel caso di contestazioni per violazioni effettuate da parte di soggetti pubblici che hanno posto in essere nel trattamento dei dati una condotta pregiudizievole e lesiva nei confronti degli interessati, come l'omissione della previa notifica da parte dell'ufficio del Garante.

Sul punto la dottrina[148] esprime i propri dubbi, poiché reputa non completo l'intervento normativo sull'art. 166 comma 5, in particolare sul fatto che il legislatore non ha precisato quali interessi pubblici possono giustificare un'ampiezza di poteri alla pubblica amministrazione rispetto al trattamento dei dati personali degli interessati, non essendo sufficienti le motivazioni affermate nell'unico comunicato stampa rilasciato dal governo, secondo il quale, tali modifiche sono state apportate per mere esigenze di semplificazione per le quali, però si rischia di creare una lacuna di significato e di operatività nei confronti della pubblica amministrazione stessa.

Alla luce delle argomentazioni sopra esposte è di palmare evidenza che il decreto legislativo n.101/2018 è stato introdotto al fine di armonizzare le norme in tema di *privacy* e tutela dei dati personali alle nuove norme del Regolamento UE 2016/679.

Al fine di rendere possibile tale armonizzazione con le norme interne e le norme europee espressamente indicate nel Regolamento, quest'ultimo ha previsto delle specifiche clausole di apertura, affinché gli Stati membri

---

147 art. 166 D.lgs. 101/2018. MARTORANA OP. CIT.
148 MARTORANA M., *OP. CIT.*

potessero introdurre o mantenere le norme capaci di attuare in maniera reale una connessione tra le predette discipline.[149]

Ed è proprio in tale prospettiva che nell'impianto penale il legislatore italiano ha deciso di utilizzare queste clausole di apertura per introdurre delle norme specifiche di carattere penale riguardanti la tutela dei dati personali.[150]

La predetta decisione da parte del legislatore italiano è stata posta in essere nell'iniziale normativa del decreto legislativo n.196/2003 finalizzato a tutelare il trattamento dei dati personali sulla base del rispetto dei diritti e delle libertà fondamentali, della riservatezza e della dignità umana.[151]

A tal proposito è fondamentale richiamare l'attenzione sull'articolo 84 del Regolamento, il quale prevede che siano gli Stati membri a stabilire le norme attinenti alle sanzioni per le violazioni delle norme del Regolamento, che abbiano un risvolto penalistico e che non saranno sottoposte alle sanzioni amministrative pecuniarie espressamente disciplinate dall'articolo 83.

Il Regolamento, infatti ha previsto che le sanzioni da applicare devono essere proporzionate, dissuasive ed effettive.

Ciascun Paese membro, effettua una notificazione alla Commissione tutte le volte che introduce una nuova disposizione di legge, o una eventuale modifica successiva, per cui si consente agli Stati membri di creare norme in materia penale che prevedono l'introduzione di sanzioni per le violazioni non soggette a sanzioni amministrative pecuniarie di cui all'articolo 83.

In considerazione del *considerandum* 149 del GDPR, che prevede " … *l'imposizione di sanzioni penali per violazioni di tali norme nazionali e di sanzioni amministrative le quali non dovrebbe essere in contrasto con il principio del ne bis in idem quale interpretato dalla Corte di Giustizia*", il D.lgs. n. 101/2018 ha posto in essere un'attività di depenalizzazione delle norme contenute nel D.lgs. n. 196/2003, al fine di scongiurare il rischio di violazioni del principio del *ne bis in idem* tra sanzioni penali ed amministrative

[149] Bolognini L., DL Capienze, ecco le sanzioni privacy per la responsabilità sociale d'impresa, agendadigitale.eu, 2 dicembre 2021

[150] MARTORANA M., BARBERISI A., PIZZETTI F., OP. CIT., 123.

[151] PLANTAMURA V., *La tutela dei dati personali*, in Diritto, informazione e informatica, 2007, n. 3, 651 e ss.

ricollegabili a fattispecie rispettivamente penali e amministrative introducendo anche nuove fattispecie di reato. [152]

In questa maniera il legislatore nazionale ha in parte abrogato parte del vecchio codice della privacy, poiché incompatibile con le norme del regolamento, dall'altro ha inserito nuove figure di reato, mantenendo inalterate altre norme, per dar vita ad un sistema normativo più adeguato ai tempi ma soprattutto maggiormente aderente alla normativa comunitaria.

Inoltre, per quanto riguarda l'attività di depenalizzazione avvenuta con l'introduzione del D.lgs. n. 101/2018 si ricorda la totale abrogazione dell'articolo 169,[153] che riguardava le misure di sicurezza, la cui abrogazione è stata determinata dall'entrata in vigore del GDPR.

L'articolo 24 del decreto 2018/101, a seguito dell'attività di depenalizzazione di cui sopra, prevede delle nuove sanzioni amministrative "*…anche alle violazioni commesse anteriormente dal decreto stesso sempre che il procedimento penale irrevocabile non sia stato definito con sentenza o con decreto divenuto irrevocabile".*[154]

---

[152] SCAGLIARISI S., Il "nuovo" codice in materia di protezione dei dati personali. La normativa italiana dopo il d. lgs. 101/2018, Giappichelli editore, 2019, pp. 1 e ss., 299 e ss.

[153] Art. 169 Codice *privacy* «Misure di sicurezza» (abrogato), affermava: «*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 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».*

[154] Art. 24 D.lgs. 101/2018 («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*

Nonostante l'assunto contenuto nell'articolo 24[155] della norma precedente, se in una fattispecie relativa ad un procedimento penale riguardanti i reati depenalizzati di cui al decreto n. 101/2018 di cui sopra, sia stata emessa una condanna o decreto definitivo e siano divenuti irrevocabili, il giudice dell'esecuzione ha i poteri di revocare la sentenza o il decreto definitivo, motivando che il fatto non è più previsto dalla legge come reato e pertanto può disporre dei provvedimenti più adeguati.

Rimanendo nell'ottica del legislatore italiano di voler armonizzare gli illeciti penali già presenti nel codice della privacy, con la nuova normativa introdotta con il D.lgs. n. 101/2018 nella tutela dei dati personali, si evince in particolar modo l'articolo 3 che ha modificato l'articolo 50 del codice della *privacy.*

Alla violazione dell'art. 50 Codice *Privacy,* il legislatore prevede l'applicazione di una sanzione da individuarsi per *relationem,* poiché fa

---

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».

[155] 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 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 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*. 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).

riferimento alle sanzioni disciplinate dall'art. 684 del codice penale, inoltre anche la figura del minorenne viene individuata per *relationem* alla normativa prevista dall'art. 13 del D.P.R. n. 448/1988 è da intendersi come il minore infra diciottenne.

L'articolo 50 codice *privacy* prevede un illecito penale che si consuma attraverso la divulgazione di dati personali, informazioni, immagini e video che riguardano un minore, dai quali si può facilmente identificare la sua identità.

Il coinvolgimento del minore all'interno di un processo a qualsiasi titolo prevede una tutela particolare indipendentemente da qualsivoglia ruolo diretto o indiretto ne faccia parte.[156]

Il minore è inquadrato dal legislatore come soggetto meritevole di tutela poiché fragile e anche se la sua minore età di infra diciottenne è stata soltanto temporanea all'interno del procedimento, poiché ha in breve tempo raggiunto la maggiore età, sino al termine del processo verrà garantito come se fosse ancora un minorenne.

Pertanto, possiamo affermare che con il decreto legislativo 101/2018 alcune norme del codice *privacy* sono rimaste inalterate, ed altre sono state modificate e novellate con l'introduzione di nuove fattispecie di reato penale.

Per tali motivazioni l'art. 84 del Regolamento UE 2016/679, delega agli Stati membri la competenza di introdurre sanzioni in materia penale, in ordine alle violazioni del Regolamento stesso da accostare a quelle amministrative.

Ciò è stato possibile mediante l'articolo 15 del D.lgs. n. 101/2018, il quale ha svolto una duplice attività, da un lato ha modificato alcune fattispecie di reato già esistenti nell'ordinamento giuridico italiano e dall'altro ne ha aggiunte di nuove, in particolare con riferimento agli articoli 167, 167 *bis,* 167 *ter,* 168, 170, 171 del D.lgs. n. 196/2003.

---

[156] CASSANO G., COLAROCCO V., GALLUS G.B., MICOZZI F.P., SORO A., BARBAROSSA M., *op. cit.,* 412 e ss.

Nel presente capitolo si affronterà in particolare l'analisi degli articoli 167, 168, 170 e 171 del Codice Privacy, come novellati dal decreto di adeguamento.

7. art. 167 D.lgs. 196/2003: trattamento illecito di dati

L'art 167 che riguarda il «Trattamento illecito di dati» era già presente nel codice privacy ed è stato oggetto di un profondo cambiamento[157]da parte dell'art. 15 del decreto di adeguamento.

Prima della riforma, l'articolo 167 disciplinava due diversi delitti in ciascuno dei quali era prevista una clausola di riserva[158] la quale serviva eventualmente a risolvere il concorso fra norme incriminatrici attraverso la clausola sussidiaria.

In particolare l'articolo 167 stabiliva al primo comma, che **"***chiunque al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati…" [159]*

Nell'attuale formulazione del 1°comma dell'articolo 167 si prevede invece, *«Salvo che il fatto costituisca più grave reato, chiunque al fine di*

---

157 CASSANO G., V. MICOZZI F. P., SORO A., OP. CIT., 413 PANETTA R. Decreto di adeguamento GDPR, cit.

158 MANNA A., *Prime osservazioni sul Testo Unico in materia di protezione dei dati personali: profili penalistici, cit.*
Secondo l'autore la formulazione della fattispecie di trattamento illecito di dati personali, ante riforma, appariva conforme al canone delle condizioni intrinseche, strutturate secondo una vera e propria progressione criminosa sul terreno dell'offesa; ipotesi nelle quali il legislatore aveva costruito la maggiore gravità della lesione agli interessi interni al reato sotto forma di condizione obiettiva di punibilità, sì da non essere costretto, da un lato, a fare intervenire la sanzione penale ogni qualvolta si realizzasse una lesione di scarsa rilevanza dell'interesse tutelato, dall'altro a costruire l'elemento più grave come elemento costitutivo del reato, oggetto di imputazione psicologica.

159 Art. 167cdp: «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, 130, ovvero in applicazione dell'articolo 129, è punito se dal fatto deriva nocumento».
Il secondo comma, invece, 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»*.

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».[160]

L'illecito penale introdotto dal legislatore riguarda la violazione di norme poste a tutela della sfera privata dell'interessato in ordine ai servizi di comunicazione elettronica, con lo scopo di sanzionare l'autore di una condotta illecita nell'uso di dati relativi al traffico comunicativo disciplinati dall'articolo 123 del codice della *privacy,* ovvero l'utilizzo di dati per conoscere l'ubicazione dell'interessato espressamente tutelato dall' articolo 126 [161]del codice della *privacy*, o colui che pone in essere un'attività di

---

[160] Art. 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».*

[161] Art. 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*

disturbo tramite comunicazioni indesiderate come gli spam di cui all'art. 130 codice privacy[162], o che realizzi una condotta in violazione del provvedimento del Garante in ordine all'operazione di inserimento e utilizzo dei dati personali riguardanti gli interessati inseriti negli elenchi cartacei o elettronici.[163]

L'articolo 167 del codice della *privacy* novellato in parte ha fatto venir meno il riferimento all'articolo 23 che è stato abrogato, il quale attribuiva importanza all'illecito trattamento di dati realizzati senza il consenso degli interessati, pertanto nel passaggio dalla normativa abrogata a quella attuale il legislatore ha effettuato delle importanti modifiche parziali, con la conseguenza che la violazione sul tema del consenso avrà rilevanza giuridica come illecito amministrativo cosi come espressamente disciplinato dall'art. 83 del Regolamento.[164]

Il secondo comma dell'articolo 167 codice privacy prevede invece, che «*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, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2 sexies e 2 octies, o delle*

---

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.

[162] Art. 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* 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 (...).

[163] Art. 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».*

[164] D'AGOSTINO L., *op. cit.*, p. 31

misure di garanzia di cui all'articolo 2 septies arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni».[165]

Nel predetto comma salvo che il fatto non costituisce una fattispecie di reato più grave, con l'applicazione di una sanzione proporzionalmente più grave, ne consegue che chiunque trae profitto per sé o per gli altri ovvero arreca danno all'avente diritto dall'utilizzo o dal trattamento di dati personali o non mette in atto misure idonee a garantire la protezione alla privacy arrecando danno all'avente diritto è punito con la reclusione da uno a tre anni.

Il sopra citato secondo comma, riguarda la violazione del trattamento dei dati relativi alle modalità e ai principi espressamente previsti dal codice privacy in particolar modo a quei dati definiti particolarmente sensibili e giudiziari.

Dai principi poc'anzi menzionati sono l'art. 2 *octies* relativo alle condanne penali e ai reati, l'art. 2 *septies* in ordine ai dati biometrici, genetici e relativi alla salute, invece l'art. 2 *quinquiesdecies* relativo ai trattamenti eseguiti per realizzare un compito di interesse pubblico che comportava elevati rischi è stato abrogato dal D.l. n. 139/2021.

Infine, il terzo comma dell'articolo 167 prevede che "*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".*

Il comma terzo sopra enunciato stabilisce l'applicazione della stessa sanzione espressamente prevista al comma precedente nella fattispecie in cui i dati personali vengono trasferiti al di fuori del territorio economico europeo, violando gli articoli 45, 46 e 49 del Regolamento.

---

[165] CADOPPI A., CANESTRARI S., PAPA M., CYBERCRIME, MILANO, 2019,

A tal proposito è bene precisare che l'articolo 167 codice *privacy* oggetto della nostra analisi possiede una clausola di sussidiarietà espressa, che ha come scopo di risolvere eventuali concorsi con altri reati penali, la predetta clausola dovrà dirimere un eventuale conflitto ad esempio tra il reato di rivelazione di comunicazioni informatiche o telematiche ex articolo 617 *quarter* codice penale e il reato di rivelazione del contenuto di documenti segreti espressamente previsto dall'articolo 621 del codice penale.[166]

Per quanto riguarda le condotte sopra rappresentate possono essere ricoperte dal titolare del trattamento che viene chiamato *data controller* dal responsabile del trattamento che prende il nome di *Data Processor* o da una persona che può essere delegata dal responsabile chiamata incaricato.

Sul punto la suprema Corte di Cassazione[167] ha ritenuto che sarà comunque responsabile della predetta fattispecie criminosa anche il soggetto privato che abbia effettuato il trattamento anche se normalmente non ricopre le predette funzioni di soggetto attivo.

In particolare la sezione penale della suprema Corte di Cassazione[168], stabilisce che costituisce illecito non soltanto l'utilizzazione dei dati che fuoriescono dalla sfera personale, ma anche la condotta che pur realizzata per fini esclusivamente personali consista nella diffusione dei dati ancorché in maniera non sistemica.

Per quanto riguarda l'elemento psicologico soggettivo che consiste nel dolo o nella colpa, la norma nel caso del dolo specifico richiede "…*al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato*", l'agente in questo caso deve agire con il fine specifico di avere un profitto per sé o per altri ovvero di arrecare danno all'interessato, i due elementi possono coesistere ma è sufficiente che ci sia soltanto il profitto o il danno altrui.

Si tratta di un dolo che si configura nel soggetto agente al fine di raggiungere come fine ultimo la realizzazione di un profitto, anche se poi in

---

[166] LAMUZZI M., Tutela penale della Privacy, Diritto on-line 2019 Treccani. 366

[167] Cass. pen., Sent. 19.10.2016, n. 6587

[168] Cass. Pen., Sent. 17.02.2011, n. 21839.

realtà alla prefigurazione non segue l'effettiva realizzazione dell'evento che era comunque voluto.[169]

Pertanto, nella predetta circostanza il reo agisce con lo specifico scopo di trarre un profitto per sé stesso o per altre persone ovvero di arrecare un danno all'interessato o realizzare entrambe le circostanze.

In questa maniera se da un lato si stringono le condotte penalmente rilevanti, nello stesso tempo nel nuovo testo non vi è più la contestualità l'indicazione dell'ingiustizia del profitto e del danno altrui.

Le modalità di redazione della norma si basano sul rinvio ad altre norme del codice o del GDPR ai fini di una definizione della condotta penalmente rilevante o si rinviano anche a provvedimenti del Garante.

Il ricorso ad altre normative presta il fianco a situazioni di precarietà, poiché tale principio di indeterminatezza porta necessariamente all' integrazione con altre norme e presta il fianco a situazioni di difficoltà interpretative.

Nella norma si rileva inoltre, l'accettazione proposta dalle relative Commissioni Parlamentari di prevedere come illecito anche le fattispecie in cui l'autore del reato cagioni soltanto danno altrui anche senza trarne alcun profitto.[170]

In tale prospettiva il concetto di danno nella nuova formulazione è diretto all'interessato, ossia il pregiudizio si deve perpetrare nella sfera degli interessi della persona danneggiata a differenza della precedente formulazione normativa, nella quale era previsto non soltanto che l'autore del reato avesse cagionato un danno altrui ma che avesse tratto contestualmente profitto per sé o per altri.

---

169 PANETTA R., Decreto di adeguamento GDPR, cit.

170 Il tutto con la specifica finalità di garantire una forte tutela contro i fenomeni criminogeni quali il "Revenge porn", ad esempio, rispetto al quale, spesso accade, che la diffusione di un certo tipo di immagini o di video pornografici, segua la fine di una relazione sentimentale e venga utilizzata come strumento di vendetta nei confronti delle vittime che sono prevalentemente donne. Ebbene, si tratta di un esempio particolare di come le odierne tecnologie possano consentire di esercitare un fortissimo potere di controllo sulle altre persone, dando luogo a gravissimi episodi cui conseguono gravi ripercussioni psicologiche, fino a spingere in alcuni casi, le vittime, a compiere gesti di suicidio**.**

Oggi ciò che deve essere presente per la configurazione del reato è il reale e concreto nocumento nei confronti dell'avente diritto.[171]

La giurisprudenza[172] di legittimità sul punto si riferisce al danno come al pregiudizio di carattere anche non patrimoniale che l'avente diritto subisce in conseguenza dell'illecito trattamento dei dati personali.

Pertanto il concetto di danno o nocumento cessa di essere considerato come un elemento obiettivo di punibilità per diventare parte integrante del reato, ossia si inserisce nella struttura tipica del delitto ritenendolo ormai come un reato di evento.[173]

In tale maniera il concetto di nocumento che abbiamo poc'anzi evidenziato rappresenta, giova ribadire, uno degli elementi costitutivi del reato con la conseguenza di un restringimento dei fatti penalmente rilevanti, poiché è necessario che ci sia l'oggetto di rappresentazione e violazione posta in essere dall'autore del reato.[174]

In conclusione il legislatore ha voluto inserire la possibilità che il reato si configuri anche in presenza del solo danno altrui, poiché il nostro ordinamento giuridico non è in grado sempre di contrastare la diffusione, ad esempio dei video per vendetta, e quindi per tale motivo le Commissioni Parlamentari, nonché il Garante hanno insistito affinché il dolo della fattispecie di cui all'articolo 167 codice della privacy potesse prevedere la fattispecie di reato anche soltanto con la realizzazione da parte del soggetto attivo del danno altrui senza alcun profitto per sé o per altri.[175]

---

[171] PANETTA R. Decreto di adeguamento GDPR, cit.

[172] Cass. Pen., Sez. III, 24 ottobre 2019, n. 30134.

[173] MANES V, MAZZACUVA F, GDPR e *nuove disposizioni penali del Codice privacy*, Diritto penale e Processo, fasc. 2, 2019.

[174] Secondo la Corte, infatti, «*Riconosciutane la natura di elemento costitutivo del reato, (..), ai fini della punibilità non è sufficiente che il nocumento si ponga quale conseguenza non voluta, ancorché prevista o prevedibile della condotta, essendo necessario che sia previsto e voluto dall'agente come conseguenza della Cass. Pen., Sez. III, Sent. 24 ottobre 2019, n. 30134propria azione o quanto meno previsto e accettato in tutte quelle ipotesi in cui non si identifichi con il fine dell'azione stessa in quanto finalizzata, ad esempio, a trarre profitto dall'illecito trattamento dei dati».*

[175] Cass. Sez. pen., Sent. 13.3.2019, n. 2013 che inquadra il danno come «*un qualsiasi pregiudizio purché giuridicamente rilevante».*

386 Cass. Sez. pen., Sent. 7.2.2017, n. 29549 che inquadra il nocumento come «*una conseguenza negativa qualsiasi, ivi comprese eventuali ripercussioni sgradevoli o disonorevoli».*

Infine, sempre relativamente all'art.167 codice della privacy il legislatore ha inserito oltre al comma 3 sopra argomentato, anche i commi 4 e 5 nei quali è previsto che qualora il pubblico ministero sia a conoscenza *notitia criminis* dei reati di cui sopra, deve immediatamente darne comunicazione al Garante, il quale dovrà redigere una relazione motivata ed allegare eventuale documentazione raccolta nella fase istruttoria e rinviarla al pubblico ministero.

8. art. 168 codice privacy: notificazioni e dichiarazioni false al Garante

L'art. 168 del Codice della *Privacy* nella formulazione novellata prevede sostanzialmente due fattispecie delittuose, nella prima punisce il delitto di falso relativamente alle dichiarazioni false rivolte al Garante, nella seconda punisce l'interruzione dell'esercizio delle funzioni svolte dal Garante.

Tale nuova formulazione si allontana molto dalla precedente, poiché si basa su un'incriminazione totalmente differente, in quanto mira a sanzionare tutte quelle condotte che anche se non si concretizzano in un vero e proprio falso comunque ostacolano la tempistica delle procedure relative agli accertamenti svolti dal Garante.[176]

Il reato, infatti, è rubricato "*Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante*".

Il legislatore nazionale attraverso l'articolo 168 codice della privacy,[177] ha voluto tutelare il buon andamento della giustizia e della pubblica amministrazione punendo con la reclusione da sei mesi fino a tre anni qualsiasi

---

[176] D'AGOSTINO L., op. cit., pp. 37 e 38.

[177] Art. 168 D.lgs. 196/2003 «Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante»: 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.
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.

soggetto che attesti falsamente alcune notizie o circostanze in maniera tale che vengano prodotti dei documenti falsi all'interno di un procedimento svolto innanzi al Garante, ostacolando di fatto l'attività dello stesso, il quale è preposto ad un'attività di garanzia e di tutela dei dati personali e dei diritti fondamentali dell'essere umano,[178] tranne nel caso in cui non ci sia un fatto che costituisca un reato più grave, allora la pena sarà aumentata.

La norma sopra rappresentata all'art. 168 codice della *privacy* possiede un campo applicativo molto esteso, poiché comprende anche le semplici omissioni informative svolte sempre con riferimento ad un accertamento o durante un procedimento, indipendentemente dalla reale capacità della condotta di danneggiare il bene giuridico in oggetto.[179]

Il predetto articolo, inoltre prevede che se il soggetto volontariamente provochi interruzione o turbi la regolarità del procedimento condotto dal Garante possa soggiacere all'applicazione della pena della reclusione fino ad un anno.

La prima fattispecie punibile è denominata a titolo di dolo generico che si concretizza nel momento in cui il soggetto agente con consapevolezza e volontà fornisce informazioni false con l'obiettivo di ingannare, in questa maniera si configura un reato di condotta e di pericolo, poiché la predetta fattispecie criminosa si configura durante le dichiarazioni false o nel momento in cui vengono realizzati gli atti falsi, caratterizzandosi dalla presenza di un elemento soggettivo e da un elemento materiale.

Anche l'articolo 168 codice della privacy nel rapporto con gli altri reati possiede una clausola di riserva, per cui in presenza di concorso con altri reati più gravi sarà questa a prevalere qualora ci siano i presupposti adeguati.

Pertanto rispetto agli elementi costitutivi sopra enunciati, l'art. 168 del codice della privacy, come novellato dal decreto legislativo n. 101/2018 non

---

[178] PANETTA R., DECRETO DI ADEGUAMENTO GDPR, CIT.

[179] BOLOGNINI L. Codice privacy: tutte le novità del d.lgs. 101/2018, Milano, 2019. L'autore definisce la fattispecie in esame, come particolarmente insidiosa, in considerazione del fatto che, nella sua formulazione, potrebbe coinvolgere, ad esempio, anche colui che abbia rappresentato il falso durante ispezioni o in risposta a richieste del Garante.

si discosta molto dalla precedente normativa, anzi in alcuni punti ne conferma i contorni.

Rispetto alla precedente normativa le novità che vengono perseguite riguardano le condotte di falso materiale o ideologico, infatti nella nuova formulazione dell'art. 168 sono stati abrogati tutti i collegamenti relativi alle falsità dichiarate all'interno delle comunicazioni di cui all'articolo 32 *bis* e all'articolo 37 del codice della *privacy* relativo alla previa notificazione.

Il D.lgs. n. 101/2018, nei confronti della seconda fattispecie incriminatrice sopra illustrata, apporta delle novità molto diverse rispetto la precedenza norma, poiché ha il particolare obiettivo di sanzionare tutte quelle azioni ed omissioni che pur non concretizzandosi in un falso siano lo stesso indirizzate ad impedire la speditezza e gli accertamenti svolti dall'Autorità Garante e più in generale il buon andamento dei procedimenti.

La predetta fattispecie incriminatrice è chiaro che è stata posta in essere per tutelare l'azione del Garante e proteggere con la massima trasparenza e veridicità l'acquisizione di informazioni dichiarative e documentali dell'avente diritto.

Qualora le predette dichiarazioni siano invece, il frutto di fuorvianti e false comunicazioni per creare una circostanza di falsità, il soggetto autore del reato soggiace alla pena massima prevista per tale circostanza.

Tale circostanza è la funzione di garanzia e di controllo posta in essere dal Garante attraverso la sua attività che non può essere in alcun modo limitata ed essere il risultato di una documentazione falsa.

La struttura della fattispecie di reato esaminata si configura come un reato comune, poiché può essere posta in essere da qualsiasi soggetto attivo, infatti, l'articolo inizia con il termine chiunque, mentre secondo una parte della dottrina[180], il reato in esame deve essere considerato proprio, poiché chi lo commette è soltanto colui che ha l'obbligo di notificare al Garante determinate informazioni, ossia il titolare del trattamento dei dati personali e quindi una persona specifica e non chiunque.

---

[180] D'AGOSTINO L., *op. cit.,* 37 e ss., MARTORANA M., BARBERISI A., PIZZETTI F., *op. cit.,* 130; CADOPPI A., CANESTRARI S., MANNA A., PAPA M., *op. cit.,* 973 e ss.

Inoltre, nella predetta fattispecie delittuosa è necessaria la consapevolezza dell'agente del reato *dell'immutatio veri,* ovvero nel momento in cui quest'ultimo rilascia delle dichiarazioni o delle attestazioni di cui è consapevole non essere corrispondenti al vero e che sono capaci di ingannare il soggetto ricevente, si configura l'elemento psicologico del dolo, poiché sussiste la volontà di porre in essere una condotta caratterizzata da un *animus nocendi*.

Nella nuova formulazione dell'articolo 168 codice della privacy viene introdotto il dolo intenzionale,[181]il quale in relazione alla combinazione dell'elemento oggettivo e soggettivo del reato si evidenzia un campo applicativo più ampio, poiché l'illecito si realizza anche in presenza di semplici omissioni informative commesse nell'ambito del procedimento e nella fase dell'accertamento, indipendentemente dalla capacità della condotta di ledere effettivamente il bene giuridico finale.

9. art. 170 codice privacy: L'inosservanza di provvedimenti del Garante

Dando seguito all'analisi degli illeciti penali espressamente previsti dal codice della privacy l'articolo 170 «Inosservanza dei provvedimenti del Garante», riguarda la condotta incriminatrice di colui che non ha osservato i provvedimenti emessi dal Garante, annoverando il reato in argomento tra quelle fattispecie incriminatrici punibili a querela della persona offesa.

I provvedimenti di cui fa riferimento l'articolo 170 nello specifico sono quelli adottati dal Garante ai sensi dell'articolo 58 comma 2, lettera f e l'articolo 2 *septies* del Regolamento, i quali riguardano rispettivamente le

[181] Secondo l'Autore la fattispecie è costruita secondo lo schema dei reati a forma libera; l'evento è descritto facendo leva su elementi più precisi rispetto all'indeterminato concetto di "ostacolo" proprio delle disposizioni da ultimo richiamate. La previsione di un dolo particolarmente intenso supplisce alla scarsa selettività delle modalità di offesa sul piano oggettivo, limitando l'ambito operativo della fattispecie alle sole condotte intenzionali, dotate dunque di maggior disvalore.

limitazioni che possono essere imposte al trattamento dei dati personali sui dati genetici, biometrici o relativi alla salute.[182]

Il novellato articolo 170 Codice della Privacy sostanzialmente ribadisce il precedente aggiungendo un maggiore campo di azione del reato.[183]

Inizialmente nel decreto precedente la proposta di aumentare il raggio di azione del reato era stata respinta, ma le Commissioni Parlamentari e l'Autorità Garante hanno insistito affinché venisse ripristinata tale modifica, per il fatto che la norma in argomento risulta essere a presidio del buon andamento dell'azione del Garante e in genere dell'azione della pubblica amministrazione.

Nella fattispecie in esame si tratta di un reato proprio, poiché può essere posto in essere soltanto da parte di chi riveste una determinata funzione rispetto al trattamento dei dati personali e pertanto il soggetto agente potrà essere soltanto ed esclusivamente il destinatario di un provvedimento emesso dal Garante.[184]

L'elemento psicologico soggettivo della fattispecie incriminatrice in esame si configura nel dolo generico poiché l'autore del reato dovrà avere soltanto la consapevolezza di aver posto in essere una condotta non conforme al provvedimento emesso dal Garante nei propri confronti.

Inoltre, per quanto riguarda il bene giuridico tutelato dalla norma la prevalente dottrina [185] ritiene che si sia conferito una rilevanza penale eccessiva, poiché si tratta di tutelare un bene giuridico intermedio, ossia il buon andamento dell'azione della pubblica amministrazione e non gli interessi dell'avente diritto di preminente interesse.[186]

---

[182] Art 170 Codice *Privacy*, «*inosservanza dei provvedimenti del Garante*»: Chiunque, non osservando 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, arreca un concreto nocumento a uno o più soggetti interessati al trattamento è punito a querela della persona offesa, con la reclusione da tre mesi a due anni».

[183] D'AGOSTINO L., op. cit., p. 41.

[184] MANNA A., *Il quadro sanzionatorio ed amministrativo del codice sul trattamento dei dati personali,* in *Il diritto dell'informazione e dell'informatica*, 2003.

[185] ADOPPI A., CANESTRARI S., MANNA A., PAPA M., *op. cit.,* 1026.

[186] MANNA A., Il quadro sanzionatorio ed amministrativo del codice sul trattamento dei dati personali, in Il diritto dell'informazione e dell'informatica, 2003.

Infine, un'altra modifica che è stata inserita dal decreto Capienze riguarda la procedibilità del predetto reato, il quale prevede che sia a querela della persona offesa, con tale limitazione si è in un certo qual modo ristretto il campo di azione e la portata sanzionatoria del reato in argomento aprendo un panorama giuridico in continua evoluzione.

10. "Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori" art. 171 C.d.P. e pene accessorie art. 172 C.d.P.

L'articolo 171 C.d.P. "*Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori"*, come per gli altri articoli anche questa fattispecie normativa si basa sulla falsariga della disposizione precedente.

L'art. 171 disciplina le fattispecie in cui sono state violate delle regole poste a tutela del controllo a distanza dei lavoratori, che in genere si basano su un accordo sindacale espressamente previsto dall'articolo 4 dello Statuto dei lavoratori.

È espressamente previsto il divieto di indagare sulla vita privata del lavoratore al fine di acquisire informazioni che non riguardano l'attitudine professionale, pertanto, indagare sulle attività riguardanti il pensiero politico, religioso, sociale e sull'orientamento sessuale del lavoratore è vietato poiché sono informazioni che sono riservate e che quindi non possono formare oggetto di indagine da parte del datore di lavoro o di altri soggetti dell'azienda.[187]

Nell'attuale contesto lavorativo la predetta norma è di particolare importanza in relazione soprattutto alle violazioni connesse al controllo a distanza dei lavoratori che ormai vengono praticate in maniera numerosa.

A tal proposito si indicano alcuni richiami giurisprudenziali. [188]

[187] Cass., Sez. III, sent. 14 dicembre 2020 (dep. 27 gennaio 2021), n. 3255, Pres. Andreazza.
[188] Sul diritto penale sanzionatorio v. in generale, per tutti, M. Catenacci, La tutela penale dell'ambiente. Contributo all'analisi delle norme penali a struttura 'sanzionatoria', Padova,

Sul punto la Suprema Corte di Cassazione ha ritenuto che nel caso in cui si vogliano installare telecamere per realizzare un sistema di videosorveglianza dei lavoratori a distanza è necessario l'accordo di tutti i dipendenti, l'accordo del datore di lavoro con le rappresentanze sindacali, altrimenti si integra il reato di cui all'articolo 171 del codice di *privacy.*[189].

A tal proposito bisogna sottolineare che ci sono state particolari difficoltà sull'interpretazione della specie incriminatrice, poiché vi sono state delle revisioni delle norme sul controllo a distanza posta in essere dal *Jobs act* mettendo in evidenza notevoli perplessità in ordine alla compatibilità con il principio di tassatività che come sappiamo è un principio cardine del nostro sistema penale italiano.[190]

Infatti, si è dato luogo alla violazione del principio della determinatezza della norma penale, poiché si è dato vita ad una fattispecie non sufficientemente precisa, così come espressamente stabilito dal sistema giuridico italiano e tutelato dall'articolo 25 della costituzione italiana.

Alla luce delle superiori argomentazioni è intervenuta una sentenza della Corte Costituzionale,[191] la quale ha stabilito che il principio di tassatività viene rispettato soltanto se la legge determina in maniera precisa la condotta e l'oggetto del reato e quindi se è ben individuabile l'integrale struttura della fattispecie criminosa.

Al fine di completare la trattazione dei reati più rilevanti del codice della privacy sul tema del trattamento dei dati personali, possiamo ricordare l'articolo 172 rubricato come "pene accessorie", il quale riguarda le fattispecie di condanna per i diritti previsti dal codice della privacy che prevedono una

---

1996, passim. Corte EDU, Grande Camera, Lopez Ribalda e altri c. Spagna, 17 ottobre 2019. In merito agli orientamenti qui richiamati si vedano da ultimo, ex multis: Cass. pen., Sez. II, 16 gennaio 2015 (dep. 22 gennaio 2015), n. 2890, in Dir. prat. lav., 2016, 12, 769 ss., con nota di S. Servidio, Controllo dei dipendenti e difesa del patrimonio aziendale; Cass. pen., Sez. III, 15 dicembre 2006 (dep. 27 febbraio 2007), n. 8042, in Dir. prat. lav., 2007, 12, 816 ss. Nella giurisprudenza civile v., di recente, tra le molte, Cass. Civ., Sez. L., 25 maggio 2018, n. 13266 in C.E.D. Cass. n. 649009-01.

[189] Cfr. Cass. Pen. n. 22148/2017

[190] BARBERISI A., op. cit., 132

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

pena accessoria, ossia la pubblicazione anche per estratto della sentenza di condanna.

La pubblicazione viene effettuata presso il Comune dove ha la residenza il condannato dove è avvenuto il delitto o dove è stato consumato, inoltre, la pubblicazione viene effettuata anche sul sito Internet del Ministero della Giustizia, anche se tale previsione risulta un po' in contrasto con la tutela dei dati personali dell'interessato poiché i dati giudiziari sono considerati dati sensibili.

11. Considerazioni finali

Tra gli elementi di rilievo rappresentati nel presente capitolo emerge in particolare l'adeguamento effettuato dal D.lgs. n. 101/2018 alle modifiche apportate al sistema sanzionatorio, le quali rivestono una particolare importanza nella normativa europea in tema di protezione dei dati personali.

A tal proposito il legislatore nazionale ha cercato di rendere più armoniosa la disciplina interna con quella comunitaria, sia per quanto riguarda la materia penale che per quanto concerne le clausole espressamente disciplinate dal legislatore europeo.

Il sistema sanzionatorio strutturato dal legislatore nazionale prevede nello specifico le modalità procedurali mediante le quali il Garante può emettere dei provvedimenti sanzionatori con la relativa abrogazione di tutte quelle sanzioni amministrative previste dal codice *privacy* prima della riforma.[192]

Il GDPR è competente soltanto delle sanzioni amministrative che rispetto al passato sono diventate più severe, facendo sì che il sistema sanzionatorio penale sia di competenza esclusiva dei singoli Stati membri.

Al fine di attuare il principio penalistico del *favor rei* vi è un'alternanza delle sanzioni amministrative, espressamente previste dal GDPR, con le sanzioni penali previste dal vecchio codice della *privacy* ciò è possibile purché

[192] PANETTA R., *Decreto di adeguamento GDPR, cit.*

non sia stata emessa nel procedimento penale una condanna definitiva passata in giudicato.

A tal proposito il legislatore nazionale prevede la depenalizzazione al fine di evitare il rischio di violazione del principio del *ne bis in idem* tra sanzioni penali ed amministrative.

Il legislatore nazionale grazie all'intervento del decreto di adeguamento ha potuto procedere ad una parziale depenalizzazione e rimodulazione di alcune fattispecie di reato già esistenti, inoltre con i nuovi concetti di trattamento su larga scala introdotti dal legislatore comunitario ha potuto inserire nel sistema penale codicistico sanzionatorio due importanti fattispecie che saranno oggetto di trattazione nel prossimo capitolo, ossia gli articoli 167 *bis* e 167 *ter* del codice della privacy.

Il regolamento europeo 2016/679/UE (GDPR) segna un punto di svolta nella creazione di un quadro regolatorio armonizzato a livello europeo per la protezione dei dati personali, che sono diventati molto importanti nella società tecnologica attuale.

La protezione dei dati personali e la privacy sono distinte, anche se simili, poiché la privacy tutela la vita privata al di fuori del trattamento dei dati, mentre la protezione dei dati tutela la corretta gestione dei dati personali.

La violazione della protezione dei dati può avere conseguenze concrete sulla vita privata e sulla salute, quindi dovrebbe essere considerata un requisito importante e non solo un obbligo giuridico.

CAPITOLO III

LE NUOVE NORME INTRODOTTE DAL D.LGS. 101/2018

SOMMARIO: 1. Riferimenti introduttivi - 2. articolo 167-*bis* D.lgs. 96/2003, trattamento dei dati su larga scala – 3. Comunicazione e diffusione secondo l'art. 167 *bis* del D. lgs 96/2003. – 4. Il rilascio del consenso nel secondo comma dell'art. 167 *bis* Codice *Privacy.* - 5. Articolo 167-*ter* D.lgs. 196/2003 acquisizione fraudolenta su larga scala di dati personali – *6. Big data*- 7. Lo scandalo Cambridge Analytica/Facebook – 8. Rischio di violazione del *ne bis in idem* nel contesto penale e amministrativo.
Conclusioni

1. Riferimenti Introduttivi

Nel presente capitolo verranno analizzate le norme incriminatrici relative al trattamento dei dati personali riferite al trattamento su larga scala, in particolare l'art. 167 *bis* e l'art. 167 *ter* codice della *privacy* con riferimento anche alle disposizioni comunitarie del Regolamento Ue 2016/ GDPR, in relazione al principio del *ne bis in idem.*

L'articolo 167-bis del Decreto Legislativo 96/2003, meglio conosciuto come Codice in materia di protezione dei dati personali, stabilisce le regole per il trattamento dei dati personali su larga scala da parte di organismi pubblici e privati. Questo articolo stabilisce le obbligazioni per le imprese e gli enti che effettuano trattamenti di dati personali su larga scala, come la raccolta, l'elaborazione, la conservazione e la diffusione di dati.

Inoltre, prevede anche le sanzioni per le violazioni delle norme sulla protezione dei dati personali.

In particolare l'articolo 167-bis mira a garantire la privacy e la protezione dei dati personali degli individui in un contesto di trattamento di dati su larga scala.

L'articolo 167-bis del D.lgs. 196/2003 prevede sanzioni per la comunicazione o diffusione illecita di dati personali da parte di organismi pubblici e privati, con pene che possono arrivare fino a sei anni di reclusione. La norma prevede due fattispecie incriminatrici: la prima è integrata da altre disposizioni non penali, la seconda si basa sull'assenza di consenso. Il consenso è un elemento essenziale per la liceità della comunicazione o diffusione dei dati personali.

Parte della dottrina, [193] ha definito di "nuova generazione" le modifiche apportate alle sanzioni amministrative, poiché in relazione ad esse si è venuto a creare il dubbio sull'applicabilità o meno delle stesse garanzie espressamente previste per il sistema sanzionatorio penale.

In base all'articolo 649 C.p.p. che prevede il principio del *ne bis in idem*, ossia il divieto per un soggetto di essere processato due volte per lo stesso reato, il punto è stabilire se tale principio può essere applicato in presenza di una condotta incriminatrice che comporta l'applicazione di una sanzione penale e amministrativa, poiché il divieto riguarda soltanto la presenza di una duplice sanzione di natura penale.

A tal proposito è opportuno precisare che nel caso in cui la sanzione amministrativa possiede un grado di afflittività particolarmente grave, può essere considerata come una sanzione penale e come tale rientrare nel principio del *ne bis in idem.*

Come più volte evidenziato il Regolamento UE 2016/679 ha dato un ampio margine di potere al legislatore nazionale, il quale attraverso il D.lgs.101/2018 che ha novellato il D.lgs. 196/2003 ha potuto operare un'attività di adeguamento al tema del trattamento dei dati personali anche se il predetto intervento non è sempre stato di facile attuazione.

Nello specifico il decreto è intervenuto a depenalizzare alcune fattispecie di cui al decreto legislativo 196/2003 con la finalità di evitare che venisse violato il principio del *ne bis in idem* tra fattispecie penali e amministrative.

[193] VIGANÒ F., garanzie penalistiche e sanzioni amministrative, in Rivista italiana di diritto e procedura penale, Anno LXIII Fasc. 4 – 2020.

Dunque, ciò posto, si evince che il legislatore italiano abbia non soltanto depenalizzato parte della normativa in argomento ma abbia anche abrogato alcune norme e novellato delle altre, introducendo un nuovo elemento rappresentato dalla previsione del danno anche non contestualizzato con l'elemento del profitto.

Ciò è avvenuto attraverso l'articolo 15 del D.lgs. 101/2018 mediante il quale da una parte ha rivisitato completamente alcune specifiche fattispecie delittuose già vigenti nell'ordinamento giuridico italiano dall'altro ne ha aggiunto di nuove.

Attualmente nel Codice *Privacy* si rinvengono cinque articoli contenenti norme incriminatrici relative al trattamento dei dati personali, di cui due riferite al trattamento su larga scala, in particolare l'art. 167 *bis* e l'art. 167 *ter*, che verranno analizzati nel presente capitolo.

Inoltre, in ordine al concetto di Big data che descrive un grande volume di dati, che inonda l'azienda e si presentano con formati destrutturati e caratteristiche eterogenee e sono spesso prodotti a velocità estrema: i fattori che li identificano sono dunque primariamente Volume, Variety, Velocity (volume, varietà e velocità).

Un caso eclatante cronaca internazionale che verrà analizzato è lo scandalo *Facebook/Cambridge Analytica*, la cui storia ha inizio nel 1993 quando il pubblicitario Nigel Oakes fondò la società *Strategic Communication Laboratories* più brevemente denominata SCL Group, la quale si occupava di comunicazioni strategiche nei confronti di particolari organismi come i Governi.

Nel 2013 il fondatore della società SCL costituì un nuovo ramo di azienda denominato *Cambridge Analytica* la quale si occupava prevalentemente di consulenza politica. [194]

[194] BBC News. (22 marzo 2018). Cambridge Analytica: The data firm's global influence. Dal momento della sua creazione, fino al 2018, Cambridge Analytica, si è occupata di oltre 200 campagne elettorali in tutto il mondo. Tra queste risulta che, nel 2013 Cambridge Analytica, alla vigilia delle elezioni politiche, abbia lavorato anche per un partito italiano; tuttavia, non venne mai divulgato quale fosse il partito in questione: le uniche informazioni che sono note riguardano il fatto che il partito aveva avuto successo per l'ultima volta negli anni '80 e che grazie alle proposte della società, elaborate a seguito di una *audience target*, alle elezioni politiche sarebbe riuscito a raggiungere un risultato oltre le aspettative.

La società *Cambridge analytica*, attraverso l'applicazione *Thisisyourdigitallifeche* si era riservata in accordo con *Facebook* di poter inviare a soggetti terzi i dati raccolti dall'applicazione stessa.

I dati venivano acquisiti attraverso un test sottoposto a tutti coloro che avevano un account *Facebook* che cliccando sullo stesso e compilando tutti i dati richiesti permettevano inconsapevolmente agli sviluppatori dell'applicazione di ottenere informazioni non solo dell'utente, attraverso l'accesso all'interno del suo profilo *Facebook*, ma acquisivano anche i dati personali degli amici dell'utente. Ciò comportò uno scandalo di dimensioni paradossali, infatti in seguito al colosso *Facebook* furono applicate pesanti sanzioni pecuniarie.

In conclusione il bene giuridico tutelato è la riservatezza come interesse del singolo e della collettività per il controllo e la corretta gestione dei dati personali.

La giurisprudenza[195] ha rafforzato la tutela della riservatezza come bene giuridico autonomo e onnicomprensivo. Il nuovo Regolamento UE 679/2016 amplia la definizione di dato informatico, considerando anche l'identità del corpo fisico come parte del concetto di identità.

Questo regolamento amplia la definizione di dato informatico per includere la nozione di identità, che comprende sia l'identità elettronica che quella fisica.

La riservatezza è quindi vista come il risultato dell'estensione normativa e prescrittiva della nozione di dato personale, e la norma è volta a proteggere la riservatezza contro le condotte di indiscrezione e ingerenza.

---

[195] Cass. Sez. II civ., Ord. n. 17665 del 5 luglio 2018: «Premesso che la definizione di «dato personale» è molto ampia (contemplando qualsiasi informazione che consenta di identificare una persona fisica) e comprende senz'altro il nome, il cognome e l'indirizzo di posta elettronica, a ben vedere il concetto di «dato identificativo» non va tenuto distinto da quello di «dato personale», rappresentando una *species* all'Interno del *genus* principale. Invero, mentre il «dato personale» è quel dato che consente di identificare, anche indirettamente una determinata persona fisica, i «dati identificativi» sono dati personali che permettono tale identificazione direttamente. In tale prospettiva si è infatti chiarito che (cfr. Cass. n. 1593/2013) ai sensi dell'art. 4 del d.lgs. 30 giugno 2003, n. 196, «dato personale», oggetto di tutela, è «qualunque informazione» relativa a «persona fisica, giuridica, ente o associazione», che siano «identificati o identificabili», anche «indirettamente mediante riferimento a qualsiasi altra informazione».

La norma in questione potenzia la tutela della riservatezza e del principio di tutela della dignità umana, poiché si riferisce a dati personali più che a dati commerciali o informatici.

Il quadro normativo per la protezione dei dati personali si basa anche su norme comunitarie con il Regolamento denominato General Data Protection Regulation (GDPR) che è stato armonizzato in Italia con il decreto n.101 del 2018.

La protezione dei dati personali è un concetto in evoluzione e in corso di definizione, che rappresenta l'espressione della libertà della persona in una società dove il trattamento dei dati assume un'importanza crescente.

Il GDPR è stato introdotto per fornire una normativa comune sulla protezione dei dati personali dei cittadini europei e promuovere un clima di fiducia per lo sviluppo dell'economia digitale in Europa. Il nuovo Regolamento europeo sulla protezione dei dati (GDPR) rappresenta una sfida epocale per la protezione dei dati personali.

La protezione dei dati è un fattore centrale nell'economia e nella società digitale a causa delle sfide sempre nuove per la sicurezza dei dati.

In Italia, le sanzioni penali hanno un ruolo importante nella salvaguardia del diritto alla protezione dei dati personali, ma nonostante questo, l'Italia è tra i dieci paesi più colpiti dal cybercrime.

La protezione dei dati deve essere al centro dell'agenda politica essendo un problema che riguarda direttamente il paese e l'individuo.

La repressione legale da sola non è sufficiente, è necessario ricorrere a misure sanzionatorie modulate e l'autodisciplina può essere un aiuto.

La differenza tra una buona protezione dei dati e una cattiva protezione dei dati può essere determinata dalle disposizioni attuative nazionali.

Le istituzioni hanno un ruolo fondamentale nell'instaurare una cultura della protezione dei dati.

Il GDPR stabilisce una cornice normativa per la protezione dei diritti, ma non basta, poiché è necessario promuovere la cultura della privacy per garantire l'effettività dei diritti sanciti.

2. articolo 167-*bis* D.lgs. 96/2003, trattamento dei dati su larga scala

Il legislatore nazionale con l'introduzione dell'art. 167 *bis* del D.lgs.196/2003,[196]così come modificato dal d.lgs.101/2018 disciplina il reato di comunicazione e diffusione illecita dei dati personali oggetto di trattamento su larga scala.

La peculiare caratteristica che determina il discrimine tra la fattispecie di reato rappresentata nel primo comma e quella indicata nel secondo è costituita dal requisito del consenso, il quale si pone come elemento tipico del reato in oggetto determinando l'illiceità della comunicazione o diffusione dei dati personali, qualora questi vengano utilizzati senza il consenso dell'avente diritto.

Pertanto, il predetto reato di cui all'art. 167 *bis* codice *privacy* si caratterizza per la presenza di una duplice fattispecie incriminatrice, poiché nel primo comma il reato per configurarsi deve essere integrato con altre disposizioni normative di natura extrapenale seguendo il concetto della norma penale in bianco[197], il secondo comma invece, si basa sulla presenza o meno del consenso dell'interessato, considerato requisito essenziale per la configurazione del reato indipendentemente dalla presenza di altri elementi che possono influire sulla condotta illecita.

Procedendo con l'esegesi del comma primo dell'articolo in argomento, notiamo che l'art. 2-*ter* Codice *privacy* prevede che il trattamento dei dati personali venga effettuato per l'esecuzione di un compito di interesse pubblico

---

196 "*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 non costituisca un reato più grave, chiunque al fine di trarne profitto per sé o per altri ovvero di arrecare danno, comunica o diffonde senza consenso…… dati personali oggetto di trattamento su scala è punito con la reclusione da uno a sei anni*. [196]

197 P. TRONCONE, La Tutela penale della riservatezza e dei dati Personali, Profili Dommatici e nuovi approdi normativi, Napoli. 2020, p. 188.

o connesso all'esercizio di pubblici poteri, invece, l'art. 2-*sexies* Codice *privacy* prevede dei trattamenti relativi a particolari categorie di dati trattati per motivi di interesse pubblico rilevante ed infine l'art. 2-*octies* Codice *privacy* disciplina i principi relativi al trattamento di dati riguardanti condanne penali e reati.

Dalla lettura dell'articolo in esame per una migliore comprensione del contenuto di tale reato che si concretizza, giova ribadire, attraverso la comunicazione e la diffusione dei dati personali è opportuno definire il concetto di comunicazione e di diffusione di cui all'articolo 2 *ter* sopra menzionato.

Comunicazione vuol dire "*dare conoscenza di alcuni dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante e dal titolare nel territorio di Unione Europea, dalle persona autorizzate, ai sensi dell'art. 2- quaterdecies, 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*".

Per "diffusione", invece deve intendersi "*il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione".*

Inoltre sul punto l'art 2 *quaterdecies* Codice *privacy* disciplina le funzioni e i compiti di particolari soggetti designati, ossia prevede che sia il titolare che il responsabile del trattamento sotto la loro responsabilità e nell'ambito delle loro competenze possano alle persone che operano sotto la loro autorità assegnare specifici compiti e funzioni in relazione al trattamento di dati personali da effettuare.

Inoltre, l'oggetto materiale dell'articolo 167 *bis* è tassativo nell'individuare che la condotta di comunicazione e diffusione deve riguardare un archivio automatizzato di dati personali o una parte sostanziale di esso.

Per archivio deve intendersi ai fini del GDPR "*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".

Più difficile è definire la frase "parte sostanziale dell'archivio" un concetto abbastanza generico che presta il fianco a contrasti interpretativi con il principio di tassatività delle norme penali presente sia nell'articolo 167 *bis* che nell'articolo 167 *ter* codice *privacy.*

La parola sostanziale potrebbe essere definita in termini quantitativi o comunque riguardare elementi particolarmente sensibili o parole chiave dell'archivio.

A riguardo, vi è da rilevare che l'articolo 167 *bis* inizia con una clausola di sussidiarietà, la quale al fine di una migliore comprensione è necessario fare un piccolo passo indietro alla formulazione della norma prima della sua modifica.[198]

Inizialmente il campo di applicazione della predetta fattispecie delittuosa limitava l'ambito soggettivo poiché era limitata a quelle comunicazioni e diffusioni illecite di dati personali che potevano essere attuate soltanto dal titolare, dal responsabile o dalla persona incaricata.[199]

Il primo a sollevare i parecchi limiti che presentava la norma con la predetta formulazione fu il Garante, poiché il restringimento soggettivo previsto dalla norma *ante* riforma escludeva in maniera illegittima altri soggetti suscettibili di poter operare sui dati anche se autorizzati al trattamento, per tali motivi il testo fu oggetto di modifiche.

Attualmente, la norma ha esteso il suo campo di azione prevedendo l'utilizzo del pronome "Chiunque", che si riferisce ai soggetti attivi del reato, i quali nella nostra fattispecie sono ben definiti.

Pertanto, l'apparente estensione dell'ambito applicativo che deriva dal termine "Chiunque" con cui inizia l'articolo in esame in realtà è in contrasto con il contenuto, il quale invece prevede che il reato si possa configurare

---

[198] M., LAMUZZI, *Tutela penale della Privacy,* in Diritto online, 2019.

[199] CADOPPI A., CANESTRARIS S., MANNA, A PAPA M., op. cit., pp. 1036 e www.garanteprivacy.it.

soltanto con la diffusione e la comunicazione di dati riguardanti specifiche violazioni, che possono essere poste in essere esclusivamente da determinati soggetti che trattano professionalmente i dati personali e che ricoprono un ruolo ben specifico all'interno del rapporto, pertanto non da "Chiunque".

Dall'analisi del quadro normativo sopra rappresentato si evince una piccola contraddizione in termini, nel senso che coloro che possono commettere il predetto reato sono soggetti ben definiti, pertanto la diffusione o comunicazione è ristretta e non ampia, poiché la violazione può essere commessa soltanto da quei soggetti che trattano dati nello svolgimento della loro professione o per obbligo della legge che gestiscono un archivio automatizzato o parte di esso, archivio che dovrà necessariamente contenere dati personali che siano oggetto di trattamento su larga scala.

Da ciò si desume chiaramente che la cerchia di soggetti che possono commettere il reato è molto ristretta, solo coloro che svolgono determinate funzioni espressamente disciplinate dalla legge in un determinato contesto possono essere autori del reato in argomento.

Per quanto riguarda invece, il secondo comma dell'art. 167 *bis* codice *privacy* si evidenzia la frase "*salvo che il fatto costituisca più grave reato",* ciò attribuisce alla norma un carattere di sussidiarietà sia per quanto riguarda altri reati penalmente rilevanti, sia per eventuali illeciti amministrativi infatti, la clausola di sussidiarietà è utilizzata per evitare eventuali violazioni del principio *ne bis in idem.*

È di palmare evidenza anche in considerazione di quanto sopra rappresentato che i nuovi reati penali introdotti dal novellato Codice *Privacy* hanno l'obiettivo di bilanciare il disvalore in relazione alla gravità di ciascuno di essi rispettando sempre i principi di sussidiarietà e di liceità della condotta incriminata allontanandosi dal precedente sistema[200].

[200] CIRILLO G. P., La tutela della privacy nel sistema del nuovo codice sulla protezione dei dati personali, Padova, 2004. L'autore mette in evidenza come il sistema precedente si era acriticamente appiattito sulla omogeneizzazione di condotte ictu oculi espressive di disvalore penale.

L'attuale norma in argomento mira a tutelare la riservatezza, intesa come bene giuridico che riguarda la tutela della corretta gestione dei dati personali nell'interesse sia del singolo avente diritto che di tutta la società.

Al fine di comprendere meglio il significato del principio di riservatezza è necessario fare un adeguato confronto tra il dato personale ed il concetto di riservatezza. [201]

Sulla scorta dell'attuale quadro normativo, il concetto di riservatezza, come sopra rappresentato ha acquisito un'estensione maggiore, poiché è diventato un bene giuridico autonomo ed omnicomprensivo, di conseguenza è cambiato anche il concetto ed il contenuto del dato personale facendo sì che il rapporto tra la riservatezza ed il trattamento dei dati sia completamente mutato.

A tal proposito anche il nuovo Regolamento UE 679/2016 amplia la definizione del dato informatico, attraverso l'inserimento dell'identità non soltanto come "corpo elettronico", ma anche come "corpo fisico"[202], in quest'ottica si crea l'identità sociale, ossia quel complesso di informazioni che riguardano la vita individuale e i rapporti sociali di un soggetto e dai quali emerge la personalità, i gusti, le preferenze e lo stile di vita di ciascun essere umano.

A tal proposito si viene a delineare un nuovo quadro normativo, in cui il dato informativo personale diventa la somma di tutto ciò che costituisce l'essenza di una determinata persona, le circostanze, le vicende della vita intima e privata, la sua immagine, tutti dati raccolti all'interno del dato

---

201 Cass. Sez. II civ., Ord. n. 17665 del 5 luglio 2018: «*Premesso che la definizione di «dato personale» è molto ampia (contemplando qualsiasi informazione che consenta di identificare una persona fisica) e comprende senz'altro il nome, il cognome e l'indirizzo di posta elettronica, a ben vedere il concetto di «dato identificativo» non va tenuto distinto da quello di «dato personale», rappresentando una species all'Interno del genus principale. Invero, mentre il «dato personale» è quel dato che consente di identificare, anche indirettamente una determinata persona fisica, i «dati identificativi» sono dati personali che permettono tale identificazione direttamente. In tale prospettiva si è infatti chiarito che (cfr. Cass. n. 1593/2013) ai sensi dell'art. 4 del d.lgs. 30 giugno 2003, n. 196, «dato personale», oggetto di tutela, è «qualunque informazione» relativa a «persona fisica, giuridica, ente o associazione», che siano «identificati o identificabili», anche «indirettamente mediante riferimento a qualsiasi altra informazione».*

202 P. TRONCONE, op. cit., p. 63.

personale, pertanto la norma deve tutelare la riservatezza personale non soltanto con l'utilizzo della rete, ma sulla base dei principi fondamentali espressamente previsti dalla Costituzione italiana. [203]

Pertanto, poiché la riservatezza è un bene giuridico da tutelare la norma penale deve potenziare la protezione della riservatezza e del principio di tutela della dignità umana da indiscrezioni ed ingerenze illegittime. [204]

Il concetto di larga scala nell'articolo 167 *bis* codice della *privacy* è particolarmente difficile da individuare con precisione, ciò comporta un elevato rischio di infrazione del principio di tassatività delle norme penali che è alla base del nostro sistema giuridico penale italiano.

Il decreto infatti, non specifica il concetto di archivio di larga scala prestando il fianco a numerose difficoltà interpretative e a tal proposito il GDPR in particolare il *considerandum* n. 91[205] fornisce utili elementi da cui prendere spunto.

Altre informazioni possono essere recuperate dal gruppo di lavoro articolo 29 al fine di valutare se un trattamento è stato effettuato su larga scala o meno prendendo in considerazione il numero dei soggetti interessati al trattamento espresso in percentuale o in termini assoluti, con riferimento alla popolazione, al volume, alle diverse tipologie di dati, alla durata e al territorio geografico.[206]

---

[203] Corte Cost. Sent. n. 38 del 5 aprile 1973, p. 4.

[204] A. Merli, Introduzione alla teoria generale del bene giudico, Esi Napoli 2006, p. 70: «*Spunti di riflessione sui nuovi beni sono dovuti alle caratteristiche del diritto penale delle società postindustriali, che, come è stato da più parti denunciato, mentre da un lato manifesta la preoccupante tendenza verso un progressivo e inarrestabile ampliamento dell'area del penalmente rilevante, indicativo di una concezione massimalista ed illimitata del diritto penale, va assumendo sempre di più il ruolo di strumento di organizzazione e di tutela di funzioni amministrative e di gestione ordinaria dei problemi sociali».*

[205] *Considerandum* 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*».

[206] 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).

Ad ogni modo il concetto di larga scala deve ritenersi non riferito alla diffusione o alla comunicazione illecita, ma ai dati contenuti nell'archivio.

A tal proposito è necessario effettuare una valutazione di impatto sulla protezione dei dati personali qualora tali dati siano stati trattati per situazioni riguardanti persone fisiche soggetti ad una valutazione basata sui dati biometrici o dati relativi a condanne penali o in relazione a misure di sicurezza.

La valutazione di impatto sulla protezione dei dati e anche necessaria nel caso in cui vengano effettuati trattamenti mediante dispositivi elettronici o altri trattamenti che possono presentare dei rischi elevati per la libertà degli interessati, poiché impediscono a questi ultimi di poter svolgere un'attività di controllo dalla quale possono emergere condotte illecite.[207]

Per quanto riguarda la procedura, il pubblico mistero al momento in cui ha notizia del predetto reato lo comunica in breve tempo al Garante, il quale trasmette una relazione motivata che includerà tutta la documentazione nella quale saranno inserite tutte le informazioni necessarie per valutare la sussistenza o meno dei requisiti richiesti ai fini della configurazione del reato acquisita durante la fase istruttoria, in questo modo l'obbligatorietà dell'azione penale è subordinata al parere del Garante.

La pena prevista per tale reato è la reclusione da uno a sei anni, ma la pena è diminuita se viene applicata una sanzione amministrativa.

3. Comunicazione e diffusione secondo l'art. 167 *bis* D. lgs. 196/2003

Dall'analisi dell'elemento oggettivo e dell'elemento soggettivo dell'articolo 167 *bis* del codice *privacy,* emerge che il legislatore delegato ha distinto due differenti condotte criminose ciascuna delle quali capace di integrare il reato.

---

[207] BOLOGNINI L. PELINO E., Codice privacy: tutte le novità del d.lgs. 101/2018, Milano, 2019.RICCIO G. M. SCORZA G. BELISARIO E., GDPR e normativa privacy, Milano, 2018

Come abbiamo già esposto in precedenza il termine comunicazione consiste "nel trasferire la conoscenza di dati personali ad uno o più soggetti determinati, diversi dall'interessato, da parte di persone autorizzate ai sensi dell'art. 2- *quaterdecies*[208] sotto l'autorità del titolare o del responsabile in qualunque maniera anche mediante la consultazione o l'interconnessione".

Invece, per quanto concerne la diffusione consiste nel dare conoscenza di dati personali a soggetti indeterminati, in qualunque maniera anche mediante la semplice messa a disposizione o consultazione.[209]

Il reato in esame potremmo considerarlo come un reato a condotta alternativa, nel senso che è possibile che si configuri in maniera alternativa alla comunicazione o alla diffusione, in questa maniera l'intervento punitivo penalistico si limita ad intervenire soltanto in determinate attività ed in presenza di particolari situazioni relative al trattamento.

In tale prospettiva possiamo affermare che il legislatore nazionale ha voluto sanzionare in maniera più severa le fattispecie in cui ci si avvale della comunicazione e della diffusione per realizzare la condotta criminosa.

Una parte della dottrina[210] ha evidenziato la differenza tra le diverse gravità di lesioni che possono verificarsi attraverso la comunicazione e la diffusione dell'archivio, certamente la diffusione dei dati personali contenuti nell'archivio ha una capacità lesiva di maggiore portata rispetto alla semplice comunicazione dei predetti dati.

La condotta criminosa si riferisce ad un archivio automatizzato o una parte sostanziale di questo, che contenga dei dati personali che sono oggetto di trattamento su larga scala.[211]

---

[208] Art 2 quaterdecies Codice privacy («*Attribuzione di funzioni e compiti a soggetti designati*»): «*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».*

[209] Articolo 2 ter, comma 4, lett. b) Codice privacy.

[210] RICCIO G. M., SCORZA G., BELISARIO E., *op. cit.,* pp. 617 e ss.

[211] P. TRONCONE, op. cit., pp. 194-195. L'Autore mette in evidenza come: «*Comunicare un intero archivio informatizzato o una parte soltanto di esso vuol dire trasferire, trasmettere, notificare a un destinatario individuato il suo contenuto. Si tratta di una definizione, se si vuole anche per il suo valore semantico, che riduce la potenzialità lesiva del mezzo*

Per la prima volta si parla di archivio automatizzato e pertanto nascono alcune difficoltà di carattere interpretativo visto che non si rinviene alcuna definizione nel codice *privacy* e neanche nella normativa europea.

L'articolo 4 n. 6 del GDPR, definisce il concetto di archivio come:" *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".*

Oltre al termine "archivio" vi è la parola "automatizzato" che secondo parte della dottrina [212] consiste in un sistema informatico di dati in serie automatizzati, che viene gestito in maniera consequenziale ed in maniera diretta del tutto slegata dal coinvolgimento fisico di una persona.

A mio modesto parere per poter comprendere al meglio il significato di archivio automatizzato, si può pensare al concetto di banca dati che è stato il precursore storico dell'attuale archivio nel quale vi è custodito una molteplicità di serie di dati che sia in maniera diretta che indiretta riguardano i dati personali delle persone e sono organizzati in maniera sistematica.[213]

Alla luce delle argomentazioni sopra esposte è evidente che i dati personali a cui fa riferimento la norma in argomento, non sono i dati che possono essere reperiti in modo confusionario su Internet, ma sono dati

comunicativo perché la rapporta alla singola entità che la riceve. Del tutto diversa invece è la condotta a forma diffusiva, destinata a una generalità indeterminata, al punto tale che neppure il responsabile del trattamento riuscirebbe a identificarla. Questa indeterminabile generalità, presente su territorio nazionale o anche internazionale, conferisce una maggiore gravità al reato, perché la diffusione è indominabile e incontenibile nei suoi effetti da parte dell'agente e la quantificazione dei destinatari risulta impossibile accertarla».

[212] Cass., Sez. II pen., Sent. n. 19855 del 9 maggio 2019: «Ai fini della configurabilità del reato di cui all'art. 167 D.Lgs. n. 196 del 2003, costituiscono illecito trattamento di dati personali effettuato da persone fisiche, sia la condotta di utilizzazione di dati che fuoriesce dalla sfera personale e domestica dell'agente e che in quanto tale non può essere ritenuta riconducibile a "fini esclusivamente personali", sia la condotta che, pur realizzata per fini esclusivamente personali, consista nella diffusione dei dati, ancorché in forma non sistematica. (In motivazione, la S.C. ha precisato che la "sistematicità" costituisce, ai sensi dell'art. 5, comma terzo, del decreto citato, un requisito della comunicazione e non anche della diffusione che, in quanto modalità estesa di propagazione del dato, realizza sempre un "vulnus" alle esigenze di protezione del dato personale)».

[213] ORLANDO S., *La tutela penale della privacy nel cyberspazio*, in Diritto penale contemporaneo Rivista trimestrale, n. 2/2019, pp. 195 e 196.

all'interno di un archivio, di una banca dati, organizzati e sistemati attraverso sistemi informatici *ad hoc*.[214]

È possibile reperire tali dati attingendo in maniera più o meno veloce all'interno dei già menzionati archivi digitali acquisendo informazioni sulla vita privata di un qualsiasi soggetto, da qui nasce il problema di tutelare in maniera corretta la diffusione e comunicazione di tali informazioni, affinché non vadano diffuse o comunicate in maniera illecita e soprattutto non autorizzata.[215]

4. Il rilascio del Consenso nel secondo comma dell'art. 167 *bis* Codice *Privacy*

Il secondo comma dell'articolo 167 *bis* codice della *privacy* disciplina tutte quelle attività relative al trattamento di dati personali in cui è necessario il consenso dell'interessato, pertanto, il consenso assume un ruolo importante, poiché diventa la base giuridica della comunicazione e diffusione dei dati personali.[216]

Alla luce della fattispecie in esame si evince come il consenso abbia una valenza proporzionale al danno causato, poiché il trattamento dei dati su larga scala abbraccia una moltitudine di dati personali e di eventuali consensi.

---

[214] L. DEAGLIO, *Il compendio sanzionatorio della nuova disciplina privacy sotto la lente del ne bis in idem sovranazionale e della Costituzione,* in Nuove Frontiere tecnologiche e sistema penale. Sicurezza informatica, strumenti di repressione, in Diritto penale Contemporaneo, 2019, 2.

[215] Art. 266 c.p.p. «*Limiti di ammissibilità*» al comma uno afferma: «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». Art. 381 c.p.p. «Arresto facoltativo in flagranza» al comma uno afferma «*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».*

[216] Diffusamente, P. Manes, Il consenso al trattamento di dati personali, Padova, 2001.

La figura di reato descritta nel secondo comma dell'art. 167 bis del Codice Privacy riguarda le operazioni di trattamento dei dati personali che vengono eseguite senza il consenso dell'interessato.

Il consenso rappresenta un elemento fondamentale per garantire una legittima comunicazione e diffusione dei dati, se presente, il consenso rende meno lesiva la fattispecie criminosa e diventa un vero e proprio requisito di tipicità del reato.

Il concetto di consenso è stato mutuato dal Regolamento UE, che definisce il "consenso dell'interessato" come una "manifestazione di volontà libera, specifica, informata e inequivocabile" da parte dell'interessato per il trattamento dei propri dati personali.

L'articolo 7 del Regolamento sul trattamento dei dati personali stabilisce che il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

La forma del consenso non è specifica, ma deve essere prestata in maniera chiara e comprensibile. Il consenso può essere revocato con le stesse forme e modalità con cui è stato prestato.

Pertanto, l'elemento fondamentale del secondo comma dell'articolo 167 *bis* è di assicurare che la comunicazione, la conservazione e la circolazione dei dati personali, avvenga in maniera corretta è lecita attraverso l'acquisizione del consenso.

Pertanto, il Regolamento UE prevede che il consenso sia informato, specifico, libero ed inequivocabile.[217]

---

[217] *Considerandum* n. 32 del Regolamento: «*Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso».*

Inoltre, il "Consenso dell'interessato", ai sensi dell'art. 4, n. 11, del Regolamento è definito come "*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento"*.

Ancora, relativamente alle disposizioni che regolano il consenso possiamo evidenziare che l'articolo 7 del Regolamento al comma 1 prevede che qualora il trattamento sia fondato sul consenso dell'interessato, il titolare del trattamento deve essere capace di provare il rilascio del consenso da parte dell'avente diritto al trattamento dei propri dati personali.

Invece, non è richiesta una forma *ad substantiam* per prestare il consenso, poiché è sufficiente dedurlo non solo dalle dichiarazioni ma anche dai comportamenti e dai fatti posti in essere.

Infine, il consenso così come viene dato, può essere revocato e questo si può evincere dall'articolo 7 comma 3 del Regolamento.[218]

5. articolo 167-*ter* D.lgs. 196/2003 acquisizione fraudolenta su larga scala di dati personali

In caso di violazione dell'art. 167 *ter* del codice della *privacy*[219], la pena prevista consiste nella reclusione da uno a quattro anni, di minore gravità rispetto l'articolo precedente, in genere nella redazione dei reati si prevede un

---

[218] *Art. 7*, comma 3 Regolamento UE 2016/679, rubricato *«Condizioni per il consenso»: «Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.*

[219] "*Chiunque al fine di trarne 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 è punito con la reclusione da uno a quattro anni"*

ordine sanzionatorio ascendente che inizia con una sanzione di minore intensità fino a giungere alla pena più grave, nel nostro caso invece, accade esattamente l'opposto, l'art. 167 *bis* disciplina una pena maggiore rispetto l'art.167 *ter* che prevede l'applicazione di una sanzione di minore entità,[220] tranne se il fatto non costituisca un reato più grave.

L'articolo 167 ter del codice di privacy prevede una sanzione penale per chi acquisisce con mezzi fraudolenti un archivio automatizzato o una parte significativa di esso che contiene dati personali soggetti a trattamento su larga scala.

La sanzione prevista è la reclusione da uno a quattro anni, a meno che il fatto costituisca un reato più grave.

Questa norma ha suscitato perplessità a causa della riduzione della sanzione rispetto alle norme precedenti. Infatti, la dottrina prevalente afferma che questa condotta già aveva rilevanza penale prima della riforma e poteva essere classificata sotto diversi titoli di reato.

La predetta fattispecie è in relazione funzionale con quella prevista dall'articolo 167 bis e mira a proteggere la privacy e la riservatezza dei dati personali.

Analizzando nel dettaglio la combinazione tra la fattispecie dell'articolo 167 *ter* e dell'articolo 167 *bis* del codice *privacy* possiamo evincere tra le due fattispecie di reato un criterio di continuità strutturale, ossia una corrispondenza nell'oggetto materiale in particolare "*nell'archivio automatizzato o in parte sostanziale dello stesso*". [221]

Inoltre, è rilevante sottolineare che i due articoli prevedono una condotta opposta, poiché nell'articolo 167 *bis* la condotta punibile è legata alla comunicazione e alla diffusione e quindi alla cessione del dato personale, nell'artico 167 *ter* la condotta che configura il reato è nell'acquisizione in maniera illecita del dato personale.

---

[220] DE BERNARDO G., Le sanzioni penali previste nel nuovo d.lgs. 101/2018, in Giurisprudenzapenale.com.

[221] ROMANO M., Commentario sistematico del codice penale, I, Milano, 2004, 58 ss.

È di tutta evidenza che il dato informatico ossia il dato personale possiede un valore commerciale e quindi è suscettibile di essere sottoposto ad una valutazione economica, a tal punto da essere molto ambito, poiché strettamente legato ad un potenziale profitto e quindi diventa di particolare rilievo la sua cessione o acquisizione.[222]

L'evoluzione della tecnologia con particolare riferimento all'utilizzo quotidiano di internet ha comportato l'evoluzione di un nuovo modo di comunicare che ha sicuramente migliorato la vita di tutti noi, ma ha determinato anche il nascere di nuove fattispecie di reato connesse all'utilizzo dei dispositivi informatici con l'inevitabile conseguenza che si sono verificati numerosi attacchi virtuali a livello digitale nei confronti di centri che contengono parecchi dati personali.

La predetta circostanza ha spinto il legislatore a creare ed a rafforzare il diritto penale nel settore dei crimini informatici, chiamati con il nome di *cibercryme* [223]che hanno come comun denominatore l'utilizzo di apparecchiature elettroniche.

Definire i *cybercrimes* non è sempre semplice, poiché tale locuzione presenta molteplici sfaccettature che vengono ricondotte a tante condotte illecite anche molto differenti fra di loro.

L'esistenza dei reati informatici non è in realtà un argomento recente, poiché già negli anni novanta e precisamente con la legge n. 547 del 1993 si era introdotta una normativa relativa ai *cibercryme,* dopo qualche anno il 23 novembre del 2021 la predetta legge subì alcune modifiche, mediante la ratifica italiana della Convenzione di Budapest sul *cybercrime.*

Gli attacchi di cui parliamo sono attacchi ad una società informatizzata, quindi mirano a destabilizzare il sistema pubblico con l'intrusione attraverso dei virus, chiamati *malware* all'interno dei sistemi informatici, come ad

---

222 FALCINELLI D., Tempi moderni e cultura digitale: il valore patrimoniale dell'identità umana "on line", in Indice pen. 2015, p. 297.

223 VACIAGO G., L'attuazione della Direttiva 2016/1148/UE sulla sicurezza delle reti e dei sistemi informativi: i punti di contatto con il Regolamento UE 2016/679, in Aa.Vv., I dati personali nel diritto europeo cit., p. 1147, l'Autore sottolinea che tale questione rientra come materia nel novero del concetto di sicurezza nazionale.

esempio l'intrusione all'interno di *hardware* appartenenti a strutture sanitarie, al fine di sottrarre dati personali relativi alla salute dei pazienti.

La predetta condotta è finalizzata nel caso del superiore esempio ad acquisire informazioni utili ad esempio per le case farmaceutiche e la produzione dei relativi farmaci, le quali invece di attendere lunghi periodi e di investire ingenti capitali acquisiscono illecitamente informazioni e dati personali in breve tempo procurando un profitto sia all'autore del reato che in questo caso all'azienda farmaceutica.

Negli ultimi tempi infatti, si registrano molti reati commessi *online* di carattere patrimoniale, poiché molti *haker* soggetti competenti nel settore informatico, utilizzano le loro conoscenze per introdursi e sottrarre dati dagli archivi informatizzati di grandi aziende, al fine di restituirli dietro pagamento di ingenti somme di denaro o mediante la vendita a terzi soggetti, una vera e propria estorsione informatica.

Le predette aggressioni ai sistemi informatici creano dal punto di vista giuridico una serie di problematiche legate a stabilire, non solo l'autore del reato, ma anche il luogo in cui è stato commesso il reato, affinché venga individuato il tribunale competente, tutte conseguenze relative al principio del *locus commessi delcti,* poiché nel mondo digitale non esistono confini geografici o limitazioni che possono impedire il trasferimento di dati in luoghi diversi da dove sono stati sottratti diventando veramente difficile e farraginoso stabilire con certezza i predetti elementi.

Infatti, la difficoltà riguarda inizialmente l'individuazione dell'autore del reato al fine di poter perpetrare l'applicazione della sanzione che spesso diventa di difficile attuazione.

Nel settore informatico la fisicità non viene concepita come siamo soliti pensarla poiché nel modo virtuale è più difficile individuare il *locus commissi delicti* in quanto gli illeciti non si svolgono in un campo territorialmente limitato e ben definito.[224]

[224] FLOR, La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative, CADOPPI, CANESTRARI, MANNA, PAPA (diretto da), Cybercrime, Torino, 2019, 143.

Per una corretta collocazione spazio/temporale della fattispecie criminosa informatica riconoscere il luogo di commissione del reato è indispensabile sia per la determinazione dell'aspetto processuale che sostanziale.

I criminali informatici possono programmare un'azione criminosa che si svolgerà automaticamente con varie tempistiche e in posti virtuali lontani e anche diversi tra di loro, rispetto al luogo di partenza dell'attacco *haker,* divenendo a volte impossibile la loro identificazione. La realtà cibernetica si caratterizza per la de-localizzazione delle risorse, per cui i principi di base dello spazio e del tempo sono completamente cambiati.

Gli addetti ai lavori informatici ormai si muovono attraverso l'elaborazione di una serie di bit che viaggiano nello spazio cibernetico, un mezzo di immissione, gestione e comunicazione di informazioni tramite impulsi elettronici.

Alla luce delle argomentazioni sopra esposte si evince che il fenomeno dei crimini informatici per le loro peculiarità, come sopra detto, non hanno confini geografici ben precisi, per cui necessita un'armonizzazione delle normative sia nazionali che internazionali, poiché le azioni dei *cybercriminal* si basano sul principio di ubiquità.

Un'ulteriore caratteristica dell'articolo 167 *ter* è l'acquisizione fraudolenta dei dati personali che si caratterizza per la presenza di una clausola sussidiaria, poiché in presenza di altri reati più gravi, ossia quando vi siano due norme di cui una ha un maggior disvalore giuridico rispetto all'altra, viene applicata nel caso di specie la norma che ha il maggior disvalore, ossia quella che prevede l'offesa maggiore nella violazione dei dati personali[225].

Invece, l'articolo disciplinato nella normativa *ante* riforma prevedeva l'applicazione della sanzione soltanto nel caso in cui l'acquisizione fraudolenta di dati personali riguardava un numero elevato di persone e la punibilità era estesa in presenza non soltanto del profitto ma anche del danno.

[225]LAMANUZZI M., *Tutela penale della Privacy*, in Diritto online 2019. Si pensi, a titolo di esempio, all'abuso d'ufficio di cui all'art. 323 c.p., alla rivelazione e utilizzazione di segreti d'ufficio ex art. 326 c.p., alla rivelazione di comunicazioni informatiche o telematiche di cui al secondo comma dell'art. 617 quater c.p., nonché alla rivelazione del contenuto di documenti segreti di cui all'art. 621 c.p.

Ritornando alla disamina dell'attuale articolo 167 *ter*, si tratta di un reato pluri offensivo realizzato al fine di tutelare la riservatezza dell'individuo e l'interesse patrimoniale del soggetto che gestisce l'archivio automatizzato.

Pertanto la finalità del reato in argomento è da ritrovare non soltanto nella tutela della riservatezza dei dati del singolo, ma anche nell'interesse generale della collettività, una tutela dei sistemi automatizzati che si pongano in maniera sicura prevedendo eventuali intrusioni e intromissioni esterne e applicando la giusta pena.

Come abbiamo già rappresentato in precedenza, la fattispecie in argomento ruota attorno alla condotta illecita relativa all'acquisizione fraudolenta dei dati personali che si trovano custoditi in un archivio su larga scala.

L'articolo 167 *ter* si occupa pertanto dell'acquisizione di dati personali in maniera illecita che può avvenire con due diverse modalità, una prima modalità consiste nell'acquisizione attraverso la sottrazione dell'archivio da parte dell'autore del reato con una perdita totale da parte di colui che lo deteneva legittimamente, la seconda modalità può avvenire attraverso la ricopiatura del contenuto degli archivi dei dati personali, per cui una copia rimane al legittimo possessore e l'altra invece viene acquisita illegittimamente dall'autore del reato.[226]

A questo punto non essendoci una locuzione ben precisa di "acquisizione di dati personali" neanche da parte del decreto legislativo n. 101/2018 e neanche all'interno del Regolamento del 2016/679 è opportuno utilizzare il linguaggio tecnico- giuridico per cui quando si parla di acquisizione di dati si fa riferimento a tutti quegli strumenti utilizzati in maniera subdola con artifici, raggiri, inganni e reticenze al fine di acquisire i predetti dati personali.

---

[226] TRONCONE P., op. cit., p. 216: «*È evidente che la scoperta di norme analoghe spinge a verificare che non si punisca, con le regole di un concorso materiale di reati, due volte la stessa identica fattispecie concreta, oltre alla eventuale chiamata in causa di illeciti amministrativi contenuti nella stessa legge».*
Invero, la lesione è rivolta ad una nuova e più pregnante oggettività giuridica – prima sconosciuta, e di nuova emersione alla luce dei nuovi utilizzi dei mezzi informatici e digitali –inquadrabile nell'interesse generale dei consociati al corretto utilizzo delle piattaforme digitali, contenitori automatizzati di innumerevoli dati personali: queste ultime – nell'ottica di una maggiore efficienza del sistema integrato di tutela – necessitano di un controllo giuridico più stringente, che può giungere anche all'inflizione della sanzione penale.

Infatti, come abbiamo più volte enunciato la norma in esame punisce colui che si procura in qualsiasi maniera il contenuto di un archivio automatizzato, o anche una parte sostanziale di esso, in maniera illecita.

L'acquisizione dei dati personali può avvenire non soltanto attraverso una condotta commissiva, ma anche attraverso una condotta omissiva in questa maniera si ampliano le ipotesi di configurabilità del reato in argomento.

La fattispecie più volte esaminata dell'articolo 167 *ter* codice *privacy*, configura un reato commissivo o punibile a titolo di dolo specifico alternativo, poiché finalizzato alla protezione della riservatezza dei dati personali, come già si è più volte rappresentato anche per il precedente articolo 167 *bis* a salvaguardia non soltanto dell'interesse del singolo ma anche dell'interesse della collettività e del legittimo possessore dell'archivio automatizzato.

Gli elementi essenziali del delitto di cui all'art. 167-ter [227]sono i medesimi dell'art. 167-bis, 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 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.

---

[227] 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».

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.

6. *Big Data*

I Big Data sono grandi quantità di dati, generati da molte fonti diverse, che possono essere analizzati per scoprire informazioni utili e supportare decisioni aziendali.

La recente normativa riguardante i big data è il Regolamento Generale sulla Protezione dei Dati (RGPD), entrato in vigore in Europa nel maggio 2018, questa normativa stabilisce un quadro giuridico per la protezione dei dati personali dei cittadini dell'UE e impone alle aziende di adottare misure adeguate al fine di proteggere i dati dei loro clienti.

Ciò include la necessità di ottenere il consenso esplicito degli individui per il trattamento dei loro dati personali, la notifica alle autorità in caso di violazioni dei dati e l'obbligo di nominare un responsabile per la protezione dei dati.

La parola "*Big Data*", fu utilizzata come espressione per la prima volta nel 2011 dal *McKinsey Global Institute,* i *Big data* consistono in un "set di dati" riguardanti l'acquisizione, l'archiviazione, la gestione e l'analisi di informazioni, di dimensioni talmente grandi da essere maggiore della capacità di un *database.*

Infatti i Big Data posseggono un patrimonio di dati, sia in termini di quantità che in volume, talmente ampio e veloce da avere bisogno per

l'elaborazione degli stessi di particolari ed innovative capacità tecnologiche.[228]

Il concetto di Big Data risale agli anni '60 e '70 con l'inizio dei data center e del database relazionale.

Nel 2005, l'enorme quantità di dati generati da Facebook, YouTube e altri servizi online ha attirato l'attenzione, portando allo sviluppo di Hadoop, un framework open source per l'archiviazione e l'analisi dei Big Data.

Con l'avvento dell'Internet of Things e del machine learning, la quantità di dati continua a crescere.

La crescita dei Big Data è stata supportata dallo sviluppo di framework open source come Hadoop e Spark.

Il cloud computing ha ampliato ulteriormente le possibilità dei Big Data, offrendo scalabilità elastica. I database grafici stanno diventando importanti per la visualizzazione di grandi quantità di dati.

I Big Data si descrivono attraverso l'analisi delle 3 V, ossia, Volume Velocità, e Varietà.

Per quanto riguarda il volume, questo equivale alla quantità dei big data, sia che essi siano stati generati dagli utenti come ad esempio le transazioni bancarie e movimenti sui mercati finanziari assumono naturalmente valori mastodontici che non possono in alcun modo essere gestiti con i tradizionali strumenti database.

Possiamo ricondurre il volume dei dati generati da una azienda all'ordine di grandezza di terabyte o petabyte.

Invece la seconda caratteristica dei big data, riguarda la diversità dei formati e, spesso, l'assenza di una struttura rappresentabile attraverso una tabella in un database relazionale.

La varietà dei big data è dovuta anche alla loro mancata strutturazione, poichè tra essi sono infatti inclusi anche documenti di vario genere (txt, csv,

---

[228] WP29, opinione 1/2010, p. 16.
BOLOGNINI L., BISTOLFI C., PELINO E., Il regolamento, cit., 125.
BOLOGNINI L., BISTOLFI C., PELINO E, Il regolamento, cit., 126.

PDF, Word, Excel, ecc.), blog post, commenti sui social network o sulle piattaforme di microblogging come Twitter.

I big data sono vari anche nelle fonti, infatti, alcuni sono generati automaticamente da macchine, come i dati provenienti da sensori o i log di accesso a un sito web o quelli del traffico su un router, altri sono generati dagli utenti del web.

Infine il terzo fattore di identificazione dei big data è la velocità con cui i nuovi dati si rendono disponibili, e proprio in funzione di questo parametro è necessario l'utilizzo di strumenti in grado di garantirne il corretto immagazzinamento.

Tra le tecnologie capaci di gestire i dati "ad alta velocità" vi sono i database historian (per l'automazione industriale) e quelle denominate streaming data o complex event processing (CEP), come Microsoft StreamInsight, un framework per lo sviluppo di applicazione di complex event processing che consente di monitorare più fonti di dati, analizzando questi ultimi in modo incrementale con una bassissima latenza.

Ad oggi, i Big Data possono essere caratterizzati da tre ulteriori discriminanti:

variabilità: una caratteristica riferita alla possibile inconsistenza dei dati analizzati;

complessità: che aumenta in maniera direttamente proporzionale alla dimensione del dataset;

veridicità: relativa al valore informativo che è possibile estrarre dai dati.

Volendo tuttavia rappresentare graficamente l'universo dei dati disponibili possiamo utilizzare, come dimensione d'analisi, i parametri di volume e complessità:

Rispettivamente l'enorme Volume, riguarda la grandezza della raccolta dei dati; la Velocità, ossia la rapidità con cui i dati vengono trattati; la Varietà intesa come eterogeneità di tipologie di dati raccolti.

In realtà, nonostante il trattamento e la gestione dei Big Data, questi non riguardano soltanto i dati personali anche se vi è fra di loro una stretta connessione, poiché i Big Data trattano una enorme quantità di dati e di altre

informazioni di carattere personale che consentono tramite essi di poter acquisire altri dati.[229]

Infatti, attraverso l'utilizzo di un unico *dataset* è possibile avere profili completi mediante i quali effettuare un'analisi in ordine a specifici soggetti.

A tal proposito è necessaria una tutela relativa al rischio di cessione di tali archivi a soggetti terzi, i quali attraverso un'operazione di incrocio dei dati acquisiti con quelli già in possesso, potrebbero implementare le loro informazioni e completare i dati personali di un soggetto, anche a sua insaputa.

Sull'argomento il legislatore nazionale ha effettuato una nuova novellazione attraverso il decreto legislativo 101/2018, inserendo nel sistema sanzionatorio penale già disciplinato dal decreto legislativo 196/2003 due articoli e precisamente l'articolo 167 *bis* e l'articolo 167 *ter* che riguardano rispettivamente "Comunicazione e diffusione illecita dei dati personali oggetto di trattamento sul larga scala" e "Acquisizione fraudolenta di dati personali oggetto di trattamento sul larga scala" che verranno analizzati nei capitoli seguenti.

Alla luce delle argomentazioni sopra esposte, acquisiscono una luce differente i cosiddetti *Big Data analytics*, che consistono in una serie di metodologie e modalità che riguardano le analisi realizzate con tecnologie avanzate e finalizzate a cercare una vasta quantità di dati, con l'obiettivo di acquisire degli schemi che apparentemente non sono visibili.

Il Regolamento GDPR non fornisce una definizione precisa del concetto di "larga scala", ma il Gruppo di lavoro Articolo 29 ne fornisce un'analisi nella linee-guida sui responsabili della protezione dei dati.

Il concetto di larga scala viene stabilito tenendo in considerazione fattori specifici come la quantità di dati personali trattati, l'impatto su un vasto numero di interessati e il rischio elevato.

---

[229] PANETTA R., Circolazione, cit., 652-653.
BOLOGNINI L., BISTOLFI C., PELINO E, Il regolamento, cit., 103. 184 BOLOGNINI L., BISTOLFI C., PELINO E., Il regolamento, cit., 104.

Il Gruppo di lavoro fornisce anche alcuni esempi concreti, come il trattamento dei dati dei pazienti in ospedale, il tracciamento degli spostamenti degli utenti del trasporto pubblico, la geolocalizzazione in tempo reale e la sorveglianza su larga scala.

Una valutazione d'impatto sulla protezione dei dati su larga scala che presentano un rischio elevato per i diritti e le libertà degli interessati.

A tal proposito anche il sopra detto Gruppo di lavoro articolo 29 ha messo in luce come l'aumento crescente della disponibilità e dell'utilizzo dei dati ha creato la necessità di analizzare in maniera più specifica l'incremento dei rischi che sono strettamente connessi alla protezione dei dati personali.[230]

Per tali motivi i *Big Data* sono inseriti sia nel settore pubblico che in quello privato, sanitario e commerciale grazie al grande movimento che generano mediante la loro attività di analisi e trattamento dei dati personali.

I dati personali e le informazioni acquisite dalle predette operazioni devono trovare un giusto equilibrio tra l'interesse della collettività e l'interesse del privato.

Pertanto, i dati personali, essendo strettamente connessi alla persona, hanno necessità di trovare un bilanciamento degli interessi, tra la libertà di iniziativa economica privata, la tutela del trattamento dei dati personali dell'interessato alla *privacy*.

È di palmare evidenza che dall'analisi dei Big Data, si possano creare dei dati nuovi al momento dell'acquisizione del profilo, dunque è necessario che il titolare presti attenzione nella predisposizione ed esecuzione del trattamento dei Big Data.

L'attività relativa al trattamento dei Big Data deve avvenire secondo i principi espressamente stabiliti dal GDPR, ossia secondo requisiti di

---

230 TURILLI M., FLORIDI L., *the ethics of information transarency,* in *Ethics and Information Tecnology, 2009,* 2, 11 e 105.
190 TOSI E., SORO A., FRANCESCHELLI V., BUTTARELLI G., BATTELLI E., *Privacy digitale*, cit., 465. 191 Wp 29, *Statement on statement of the wp29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU,* Settembre 2012.

correttezza e liceità, basandosi su norme giuridiche e su tecniche e modalità trasparenti. [231]

Anche se il principio di trasparenza non è semplice da attuare nei confronti degli interessati, poiché vengono utilizzate delle metodologie e delle tecniche talmente complicate che non è sempre semplice spiegarle a chi non è un addetto ai lavori, come nel caso degli interessati.

Per tali motivi è difficile a volte ottenere il consenso da parte degli aventi diritto, poiché è difficile spiegare loro, l'attività che il sistema di analisi collegato ai Big Data normalmente è deputato a svolgere.

Un altro aspetto importante da tenere in considerazione sono le finalità del trattamento, ossia l'utilizzo di quei dati solo ed esclusivamente per raggiungere gli obiettivi che hanno reso necessaria l'acquisizione degli stessi.

Pertanto, un utilizzo differente dallo scopo autorizzato è frutto di un illecito e come tale punibile dall'ordinamento giuridico italiano.

Altrettanto delicato è l'aspetto relativo alla conservazione dei dati per un tempo determinato relativo alla finalità da conseguire, oltre il quale si crea un conflitto rispetto alla loro natura e all'obiettivo per cui erano stati acquisiti.[232]

Un altro importantissimo requisito del trattamento dei Big Data consiste nella minimizzazione dei dati personali, rispetto ai metodi tradizionali, per i quali in precedenza alcuni dati non venivano presi in considerazione, poiché ritenuti non utili all'acquisizione di informazioni.

---

231 McKinsey Global Institute nel 2011, WP29, opinione 3/2013, 4.
NUNZIANTE E., Big Data. Come proteggerli e come proteggerci. Profili di tutela della proprietà intellettuale e protezione dei dati personali, Law and Media Working Paper Series, 2017, 6.
TOSI E., SORO A., FRANCESCHELLI V., BUTTARELLI G., BATTELLI E., Privacy digitale, cit., BOLOGNINI L., BISTOLFI C., PELINO E., Il regolamento, cit., 103.

232 TOSI E., SORO A., FRANCESCHELLI V., BUTTARELLI G., BATTELLI *Privacy digitale, cit., 464- 465.*
TURILLI M., FLORIDI L., the ethics of information transarency, in Ethics and Information Tecnology, 2009, 2, 11 e 105.
TOSI E., SORO A., FRANCESCHELLI V., BUTTARELLI G., BATTELLI *E. Privacy digitale, cit., 465.*
191 Wp 29, Statement on statement of the wp29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU, Settembre 2012.
W.p. 29, Op. 3/2013 cit.

Invece, l'attuale *modus procedenti* del trattamento di Big Data è molto diverso in quanto, anche i dati che possono sembrare non importanti vengono acquisiti in considerazione del fatto che attraverso informazioni incrociate si possono ricavare comunque altre informazioni che poi diventeranno utili.

Pertanto, le tecniche adoperate per l'analisi del trattamento da parte dei Big Data consistono in un'attività automatizzata, ossia acquisire tutto l'insieme dei dati senza fare una selezione a priori, poiché tutto è utile per acquisire informazioni.

Le predette modalità di analisi del trattamento dei dati da parte dei Big Data sono un po' in contrasto con alcuni principi del GDPR però tale criticità è in parte risolta mediante il principio di *accountability* che fa riferimento alla responsabilità del titolare del trattamento.

Infatti, il titolare può attuare attività tecniche ed organizzative tali da garantire un lecito e corretto trattamento dei dati personali dell'interessato.

7. Lo scandalo *Cambridge Analytica / Facebook*

La società moderna in cui viviamo si può definire una società dell'informazione e della comunicazione ciò avviene attraverso sistemi informatici sempre più sofisticati su cui ruotano svariate attività sociali ed economiche e con esse i dati personali di ciascuno di noi.

Attraverso i sistemi informatici possiamo navigare su internet e svolgere delle attività che altrimenti non potremmo effettuare superando barriere spaziotemporali.

La rete è ormai lo strumento con il quale si comunica e si forniscono informazioni agli altri senza confini o limitazioni sia nei rapporti sociali che economici.[233]

[233] PIZZETTI F., op. cit., pp. 10 e ss.Come evidenziato dall'autore, partendo dalla consapevolezza che l'uomo è un animale sociale e come tale al centro di una rete di relazioni «rinunciare alla protezione dei dati personali da ogni indebita ingerenza, significa rischiare di vanificare ogni altra forma di libertà e mettere in pericolo tutti i diritti fondamentali».

I sistemi informatici hanno ormai preso campo anche nei servizi pubblici, in cui per snellire e velocizzare le farraginose procedure della macchina burocratica pubblica vengono ormai adoperate quasi esclusivamente procedure online, comportando determinati obblighi a carico di alcuni soggetti che diventano responsabili, come abbiamo visto, della conservazione, utilizzo e circolazione dei dati personali raccolti.[234]

In questo nuovo panorama, emerge la totale digitalizzazione della nostra società ed un ruolo di preminente importanza viene attribuito ai *social network* che ci accompagnano durante la giornata poiché ormai fanno parte del nostro *modus vivendi*, aiutando le persone all'abbattimento delle distanze e a velocizzare i tempi di attesa di parecchie procedure.[235]

Un aspetto di particolare rilievo è l'apparente attività ludica che spinge l'utente a navigare su determinate piattaforme inserendo i propri dati personali o semplicemente effettuando delle ricerche che favoriscono l'identificazione del soggetto.

Tutto ciò favorisce l'esposizione ad essere sottoposti a dei rischi ed essere facile preda di usurpazione d'identità e di dati personali, pregiudicando a volte anche la reputazione personale ed economica della vittima.[236]

Un caso di cronaca internazionale che a tal proposito può essere citato è il *data gate Cambridge Analytica e Facebook.*

Il pubblicitario Nigel Oakes nel 1993 fondò la società denominata *Strategic Communication Laboratories* più brevemente denominata SCL

---

[234] RODOTÀ S., Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione, Roma, 1997.

[235] PAPA A., Espressione e diffusione del pensiero in Internet. Tutela dei diritti e progresso tecnologico, Torino, 2009; CARETTI P., Diritto dell'informazione e della comunicazione. Stampa, radiotelevisione, telecomunicazioni, teatro e cinema, Bologna, 2005; RODOTÀ S., *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma, 1997

[236] Al *considerandum* 4) del Regolamento europeo relativo allo stesso oggetto di analisi, dichiara che «*Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica».*

Group, la quale si occupava di comunicazioni strategiche nei confronti di particolari organismi come i Governi, le personalità politiche e gli eserciti, nonché le pubbliche relazioni, e le ricerche comportamentali.

Nel 2013 il fondatore della società SCL costituì un nuovo ramo di azienda denominato Cambridge Analytica, la quale si occupava di consulenza politica. [237]

L'Amministratore delegato della Cambridge Analytica[238] Alexander Nix gestiva l'azienda attraverso un particolare *modus operandi*, ossia utilizzava direttamente i social media per fare la campagna elettorale scegliendo in maniera accurata gli elettori giusti a cui far pervenire determinate informazioni.

Sempre nel 2013 la *Cambridge analytic*a ha lavorato anche per un partito italiano che però non si è mai saputo quale fosse e che ha avuto un successo inaspettato rispetto al solito.

Nel giugno del 2016 la predetta società inizia la campagna elettorale di Donald Trump e di oltre 200 campagne elettorali in tutto il mondo sino al 2018.

La fama della società con il tempo, venne però ridimensionata anche alla luce della testimonianza di un ex dipendente Christopher Wylie, il quale nel 2018, raccontò del lavoro e dei metodi non sempre corretti utilizzati dalla società.

La predetta società nel 2015 si avvalse di alcuni dati acquisiti attraverso un'applicazione denominata *Thisisyourdigitallife* creata dal ricercatore Alexandr Kogan dell'Università di Cambridge.

---

[237] BBC News. (22 marzo 2018). Cambridge Analytica: The data firm's global influence. Dal momento della sua creazione, fino al 2018, Cambridge Analytica, si è occupata di oltre 200 campagne elettorali in tutto il mondo. Tra queste risulta che, nel 2013 Cambridge Analytica, alla vigilia delle elezioni politiche, abbia lavorato anche per un partito italiano; tuttavia, non venne mai divulgato quale fosse il partito in questione: le uniche informazioni che sono note riguardano il fatto che il partito aveva avuto successo per l'ultima volta negli anni '80 e che grazie alle proposte della società, elaborate a seguito di una *audience target*, alle elezioni politiche sarebbe riuscito a raggiungere un risultato oltre le aspettative.

[238]Reuters. (21 marzo 2018) What are the links between Cambridge Analytica and a Brexit campaign group? www.reuters.com.

L'acquisizione dei dati avvenne per mezzo di un test che veniva sottoposto a tutti coloro che avevano un account su Facebook e che volevano partecipare.

Il predetto test aveva ad oggetto cinque profili chiamati *Big five* attinente alla personalità del partecipante, il predetto test veniva effettuato dagli utenti attraverso il proprio account di Facebook, in questa maniera gli sviluppatori ottennero un profilo psicometrico ed una grande quantità di dati personali anche attraverso l'accesso all'interno dei vari profili Facebook.

La compilazione del predetto questionario fece acquisire alla predetta Società un elevato quantitativo di informazioni relative ai dati personali, ossia circa 270 milioni di utenti di Facebook costruendo un ingente archivio.

Oltre ai dati acquisiti direttamente dagli utenti che sceglievano di fare il test, l'archivio si riempiva anche di contatti indiretti, ossia degli amici degli utenti che avevano adoperato l'applicazione in argomento.

In quel periodo infatti, Facebook permetteva agli sviluppatori di utilizzare delle applicazioni che potevano fornire informazioni anche sugli amici delle persone che avevano utilizzato l'applicazione senza che fosse richiesto il loro consenso.[239]

L'anomalia che si venne a registrare, a seguito dell'utilizzo dell'applicazione e del relativo test furono i dati personali degli utilizzatori del predetto test e dei loro amici con l'ottenimento di circa 87 milioni di utenti e dei loro dati personali, per tale motivo il *social network* intimò alla *Cambridge analytica* (società che aveva acquisito illecitamente i dati personali), di cancellarli senza cederli a terzi, ma di tale effettiva cancellazione non si ebbe mai nessuna prova.

Facebook in relazione alla predetta fattispecie adottò una politica severa consistente nel divieto ai proprietari di applicazioni di condividere i dati ottenuti con terze persone prevedendo l'applicazione di gravi sanzioni come la sospensione dell'account che per le società *online* consiste in un grave pregiudizio.

[239] Channel 4 News. (20 marzo 2018). Cambridge Analytica: Undercover Secrets of Trump's Data Firm.

Nella realtà, Facebook non applicò mai le sanzioni che aveva intimato alla *Cambridge,* infatti dopo poco tempo *la Cambridge analytica* avviò le procedure per dichiarare la bancarotta della propria azienda, a seguito di tali avvenimenti l'autorità per la tutela della *privacy* applicò a Facebook una prima multa per la violazione della protezione dei dati personali denominata *Information Commissioner's Office Ico,* per una somma complessiva di circa 565 mila euro. [240]

Facebook per mettere fine a quello che fu chiamato lo scandalo di *Cambridge analytica* a seguito di indagini svolte dall'Antitrust Statunitense, patteggiò con la *Federal Trade Commission (Ftc)* la cifra di 5 miliardi di dollari, per chiudere la controversia che era nata a seguito della violazione della *privacy* dei dati personali degli utenti coinvolti nello scandalo *Cambridge Analytica.*

Facebook subì sanzioni particolarmente gravose ma di natura civile senza avere alcun risvolto in ambito penale, anche se nel 2018 furono calcolati ben 88 milioni di utenti di cui 2,7 milioni si trovavano nell'Unione Europea a cui furono sottratti senza il loro consenso i loro dati personali.

Facebook fu citata davanti il Parlamento Europeo al fine di fare chiarezza sulla questione e sulla gestione dei dati in modo che la società rispettasse la normativa europea espressamente stabilita dal Regolamento UE 2016/679 che per quanto riguarda l'Unione Europea sarebbe entrato in vigore il 25 maggio 2018.[241]

Inoltre, tornando con il discorso dei confini spazio/temporali, l'art 3 del Regolamento, prevede che le norme del GDPR hanno efficacia non solo alle

---

[240] WAGNER K., Here's how Facebook allowed Cambridge Analytica to get data for 50 million users, 2018, www.recode.net.
SCHOOEPFER M., Facebook Newsroom. An update on our plans to restrict data access on Facebook, 2019, su newsroom.fb.com.

[241] www.europarl.europa.eu.
A seguito di tale intervento Facebook ha aggiornato le proprie impostazioni relative alla privacy per consentire agli utenti di sottrarsi alla targhetizzazione, ivi inclusi la pubblicazione di messaggi pubblicitari sulla base di informazioni ottenute da terzi e l'uso delle loro informazioni personali raccolte da Facebook per pubblicare messaggi pubblicitari su altri siti o piattaforme.

fattispecie in cui il titolare ed il responsabile del trattamento dei dati personali siano stabili all'interno dell'Unione Europea, ma indipendentemente dal fatto che il trattamento dei dati avvenga all'interno o meno del territorio europeo.

Infatti, le predette norme espressamente stabilite all'articolo 3 del Regolamento si applicano anche a tutte quelle attività che riguardano dati personali relativi a soggetti che si trovano in europea anche se il responsabile del trattamento non si trova all'interno di uno Stato europeo.

Pertanto, nel caso di *Cambridge analytica* è stato applicato il GDPR al reato penale relativo al trattamento dei dati personali riguardanti soggetti presenti sul territorio dell'Unione, anche se il titolare ed il responsabile non operavano nei paesi del territorio dell'Unione Europea.

Dunque, alla luce di quanto sopra rappresentato, l'articolo 3 del Regolamento ha recepito l'orientamento della Corte di Giustizia Europea e del Gruppo di lavoro Articolo 29 ed ha ampliato il principio di stabilimento,[242] poiché viviamo in un'epoca dal gusto transfrontaliero in cui l'applicazione della norma non viene determinata in base al luogo di stabilimento del soggetto che fornisce il servizio, in quanto vige il principio della smaterializzazione ed il fulcro è diventato il bene giuridico da tutelare e proteggere, ossia il dato personale.

---

[242] della direttiva n.95/46/CE ruotava essenzialmente intorno al tradizionale principio di stabilimento. Ai sensi dell'art. 4, par.1, lett. a) le norme nazionali di recepimento della direttiva operavano in caso di trattamenti effettuati «*nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro*». In tal senso, l'applicabilità del quadro normativo dipendeva dallo svolgimento di un'attività realizzata da un'impresa stabilmente presente all'interno di uno degli Stati europei. Nel caso di soggetti extra-europei, le regole operavano solo nel caso il responsabile disponesse di «*strumenti, automatizzati o non automatizzati, situati nel territorio di detto Stato membro*». Con lo straordinario incremento dell'utilizzo della rete Internet e, soprattutto, dei social network che della a-territorialità fanno il proprio punto di forza, tale approccio in vista di una effettiva tutela dei dati personali è risultato via via sempre meno efficiente. Dal campo di applicazione della normativa sfuggivano, infatti, proprio i grandi colossi extra-europei che da anni dominano il panorama mondiale del mercato delle comunicazioni. Supportato dal parere n. 8/2010 dell'Article 29 Working Group e dalle sentenze *Google Spain* e *Weltimmo* entrambe orientate ad un'estensione dell'applicabilità delle norme europee al di là del principio di stabilimento, il legislatore europeo ha ampliato l'ambito di efficacia della nuova disciplina, dichiarando in maniera specifica al considerandum 23) che tale scelta è finalizzata ad evitare che una persona fisica possa essere privata dalla protezione cui ha diritto ogni volta che il trattamento venga effettuato da un soggetto non stabilito dell'Unione e si connetta all'offerta di beni o servizi indipendentemente dal fatto che vi sia pagamento correlato ovvero al monitoraggio del comportamento di interessati che si trovano nell'Unione.

Il legislatore comunitario pertanto è giunto alla considerazione di tutelare la persona umana, visto che non ci sono confini ben definiti con i quali poter determinare una legge all'interno di uno Stato geografico, per cui si tutela l'essere umano e i suoi dati personali, la sua riservatezza come diritto fondamentale espressamente tutelato e previsto dalla Costituzione italiana.

Come poc'anzi rappresentato la vicenda dello scandalo *Cambridge analytica* inizia non per una violazione dei sistemi di sicurezza della piattaforma Facebook da parte di coloro che gestivano l'applicazione e che mediante la stessa hanno acquisito i dati personali di coloro che utilizzavano l'applicazione e dei loro amici, ai quali peraltro non è stato mai chiesto il consenso, ma dalla divulgazione a terze persone dei dati ottenuti attraverso la predetta applicazione senza alcuna autorizzazione da parte degli interessati.

Pertanto, l'illecito commesso non era da inquadrarsi in relazione ad un illecito utilizzo dei dati da parte di coloro che hanno sviluppato l'applicazione, ma piuttosto in relazione alla trasmissione successiva senza consenso dei predetti dati a società terze.

Da svariate indagini e soprattutto dalle audizioni che i rappresentanti di Facebook hanno dovuto sostenere innanzi il Parlamento Europeo è emerso che la piattaforma social era a conoscenza di tali irregolarità poiché indicate come clausole contrattuali.

Infatti, l'applicazione *Thisisyourdigitallife* prevedeva la possibilità da parte della società *Cambridge analytica* di poter inviare a soggetti terzi i dati raccolti dall'applicazione stessa.

Alla luce di ciò si può affermare che Facebook era consapevole che gli sviluppatori dell'applicazione in argomento si erano riservati il diritto di cedere i dati raccolti a terze società.

Per tali motivazioni dato che Facebook era il titolare del trattamento dei dati personali è stato ritenuto responsabile dell'accaduto e di conseguenza è stato giudicato colpevole, di aver permesso la predetta circostanza violando il diritto in materia di protezione dei dati.

Un'altra caratteristica che ha comportato una maggiore gravità del *data Gate Cambridge analitica Facebook* è stato determinato dalla staticità

dell'amministratore delegato di Facebook, il quale era a conoscenza dell'illecito che si stava perpetrando sulla violazione dei dati personali dei suoi utenti, e non ha fatto nulla per impedirlo.

Infatti, l'amministratore delegato di Facebook, Mark Zuckerberg,[243] venendo a conoscenza dell'illecito già nel 2015 non avvertì le autorità competenti ponendo in essere soltanto una diffida alla società di profilazione politica cioè alla *Cambridge analytica,* richiedendo la distruzione delle informazioni dei dati personali ottenuti in maniera non lecita senza in realtà adoperarsi ad un effettivo controllo relativo alla distruzione del materiale che la società *Cambridge analytica* aveva carpito.

Qualora fosse stato già in vigore il Regolamento europeo il mancata sollecito e controllo da parte dell'amministratore delegato di Facebook, avrebbe comportato una grave violazione della normativa in questione, ponendosi in conflitto il sistema degli obblighi generali previsti dall'articolo 33 del GDPR, in capo al titolare del trattamento, con il dovere di notifica all'autorità di controllo.[244]

Infatti, l'articolo 33 del GDPR pone l'obbligo al titolare del trattamento di attivarsi entro 72 ore, specificando la natura della violazione, della tipologia dei dati, del numero di soggetti interessati effettuando una descrizione per quanto possibile dettagliata di eventuali conseguenze dannose che la violazione del trattamento dei dati può avere generato o può generare.

La comunicazione effettuata con tempestività è considerata di particolare rilievo dal legislatore europeo, in quanto è finalizzata a limitare i danni che in impotenza si potrebbero verificare.

Facebook pertanto, se avesse denunciato tale condotta in maniera tempestiva avrebbe limitato i danni ed attuato dei rimedi più efficaci per la tutela dei dati personali violati.

---

[243] Ilsole24ore.it. Zuckerberg, in occasione delle due udienze presso il Congresso americano, ha pubblicamente ammesso di non aver effettuato alcun controllo successivo circa l'effettiva avvenuta distruzione dei dati illecitamente sottratti e trasferiti dalla società che ha sviluppato l'applicazione a Cambridge Analytica.

[244] Risoluzione del Parlamento Europeo del 25 ottobre 2018 n. 2020/C 345/10, Pubblicata sulla Gazzetta Ufficiale dell'UE del 16/10/2020.

Il Regolamento UE per quanto riguarda il trattamento dei dati personali risulta violato anche nell'articolo 34, il quale impone al titolare di informare in maniera dettagliata gli interessati in relazione all'avvenuta violazione dei propri dati personali.

Pertanto, se ritorniamo all'esempio dello scandalo di *Cambridge analytica di Facebook* la piattaforma social contrariamente a quanto in realtà è stato fatto avrebbe dovuto con una certa celerità informare singolarmente del fatto accaduto tutti gli utenti coinvolti sulla violazione dei dati personali, cosa che in realtà non è mai stata fatta.

Infatti, qualora fosse stato in vigore il GDPR, Facebook essendo nel caso di specie il trattamento di tipo automatizzato, per cui particolarmente invasivo nei confronti della *privacy* dei soggetti interessati, avrebbe dovuto effettuare come prima cosa un'analisi preventiva della gestione e del trattamento dei dati riguardanti le persone fisiche.

Pertanto, risulta di palmare evidenza, che Facebook, avrebbe dovuto compiere una previsione valutativa di impatto relativamente al trattamento dei dati personali dei propri utenti prevedendo che l'utilizzo continuo di nuove tecnologie comporta un impatto considerevole sui diritti e sulle libertà fondamentali dei soggetti che ne vengono coinvolti al fine di prevenire situazioni di violazione della sfera d'identità degli utenti.

Infatti, il continuo utilizzo di tecniche sempre più sofisticate avrebbe dovuto obbligare la piattaforma social a norma dell'articolo 36 GDPR (se fosse stato in vigore) a consultare l'Autorità di controllo e a individuare possibili rischi legati all'utilizzo dei *social* in tale forma, rifiutandosi di imbarcarsi in circostanze poco chiare, cercando, invece, sistemi di tutela più adeguati alle predette circostanze.

Non bisogna dimenticare che Facebook svolge un'attività di trattamento di dati che per le sue caratteristiche, stabilisce il monitoraggio svolto in maniera sistematica di tutti gli interessati sia su larga scala, sia categorie specifiche i cui dati spesso e volentieri sono più sensibili di altri.

Pertanto, la presenza del GDPR avrebbe comportato anche l'applicazione dell'articolo 9 il quale avrebbe previsto la nomina di un *data protection*

officer, il quale sarebbe stato di supporto al titolare e al responsabile con specifiche funzioni collaborative nell' ambito tecnico giuridico in relazione alla tutela dei dati personali.

Da ciò si evince che il sistema elaborato dal GDPR ha carattere più preventivo che punitivo, poiché si basa su una collaborazione delle figure principali, che sono l'Autorità di Controllo e il Garante, al fine di tutelare a priori i dati personali trattati onde evitare l'illecito trattamento degli stessi.

Giova ribadire, che se all'epoca dello scandalo, se il Regolamento UE fosse stato in vigore avrebbe invitato Facebook ad effettuare un primo step di controlli basati sulla collaborazione da parte dell'Autorità di Controllo e da parte dei soggetti tecnici, quali ad esempio il DPO al fine di effettuare in via preventiva e non a posteriori, come invece è successo, l'utilizzo di mezzi di tutela più efficaci.

Dal punto di vista sanzionatorio se fosse stato vigente il Regolamento, sarebbe stata applicata la nuova fattispecie espressamente prevista dall'articolo 83 paragrafo 4, che avrebbe comportato l'applicazione della sanzione amministrativa con un massimo edittale di 10.000.000 euro, nonché fino al 2% del fatturato mondiale, totale annuo dell'esercizio precedente.

In relazione al predetto caso di *Cambridge analityca*, l'Italia ha applicato a Facebook una sanzione di 1 milione di euro in ordine agli illeciti commessi.

L'Autorità italiana ha accertato che attraverso la funzione *Facebook login* molti utenti italiani si scaricarono l'applicazione T*hisisyourdigitallife,* e mediante la stessa *la società Cambridge analityca* acquisì i dati di miliardi di utenti italiani, tra coloro che avevano usato direttamente la piattaforma e coloro che non l'avevano usata ma che erano amici di questi ultimi, poiché l'applicazione consentiva di condividere i profili degli amici anche se questi ultimi non avevano dato il loro consenso e di conseguenza non erano a conoscenza che i loro dati sarebbero stati ceduti a terzi.[245]

---

[245] Cambridge Analytica: il Garante privacy multa Facebook per 1 milione di euro", in garanteprivacy.it.

Ad ogni modo dal 25 maggio 2018, data di entrata in vigore del GDPR in tutti i paesi dell'Unione, come si evince anche dalla relazione biennale presentata dalla Commissione europea, il Regolamento UE ha comportato un vero e proprio mutamento della normativa di protezione dei dati personali a tal punto che anche i paesi al di fuori dell'Unione Europea hanno voluto fare riferimento alla normativa europea GDPR, diventata il loro punto di riferimento per la tutela dei dati personali a livello mondiale.

La strada certamente è ancora lunga e tortuosa soprattutto nei riguardi del *big tech companies*, infatti il numero di sanzioni applicate fino a dicembre 2021 nei vari paesi membri dell'Unione Europea è andato aumentando per un totale di 927 sanzioni comminate.

8. Rischio di violazione del principio *ne bis in idem* nel contesto penale e amministrativo

Alla luce dell'analisi compiuta sino ad ora sulla normativa relativa alla tutela penale del dato personale è emerso che il centro su cui le modifiche sono state apportate e su cui il GDPR trova la garanzia della sua effettiva applicazione è l'apparato sanzionatorio che ha coinvolto sia l'ambito penale che amministrativo.

Il legislatore europeo attraverso il Regolamento UE 2016/679 ha ben delineato un quadro normativo riguardante l'ambito amministrativo, prevedendo in proporzione alla violazione commessa le relative sanzioni pecuniarie.

In coerenza con il superiore assunto, il Regolamento all'art. 84 da interpretare congiuntamente con *il considerandum* n. 149, affida ai Paesi membri la libertà nel rispetto della normativa comunitaria, di poter introdurre nel proprio ordinamento giuridico delle disposizioni che abbiano una corrispondente valenza in ambito penale.

A tal proposito è opportuno valutare quali siano le modalità permesse dal Regolamento agli Stati membri in relazione ad un adeguato sistema

sanzionatorio penale che possa coordinarsi ed integrarsi con l'apparato sanzionatorio amministrativo senza entrare per questo in contrasto.

La risposta normativa a tale interrogativo è rappresentata dalla lettura del *considerandum* n. 149 il quale prevede che: «*Gli Stati membri dovrebbero poter stabilire disposizioni relative a sanzioni penali per violazioni del presente regolamento, comprese violazioni di norme nazionali adottate in virtù ed entro i limiti del presente Regolamento. 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».*

In buona sostanza sulla base del predetto *considerandum* n. 149 gli Stati membri avrebbero il compito di creare una normativa che disciplini l'impianto sanzionatorio penale all'interno del proprio ordinamento giuridico in armonia con le disposizioni di natura amministrativa indicate nel Regolamento, poiché gli organi che costituiscono l'Unione Europea non hanno competenza ad introdurre norme di natura penale c all'interno di uno Stato membro, per tali motivi nasce la delega affinché ciascun Paese membro si attivi per poter attuare il predetto precetto.

Infatti, in materia di legislazione criminale l'Unione Europea secondo l'articolo 83 TFUE riconosce soltanto una competenza generale.[246]

---

[246] 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

Il Governo italiano ha introdotto all'interno del nostro ordinamento giuridico la normativa vigente in materia di tutela dei dati personali adeguandola a quanto previsto dall'articolo 84 del Regolamento, con la precisa finalità che le sanzioni introdotte dagli Stati membri, fossero proporzionate, effettive e dissuasive.

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, in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie ex articolo 83[247].

---

stessa procedura legislativa ordinaria o speciale utilizzata per l'adozione delle misure di armonizzazione in questione, fatto salvo l'articolo 76.

[247] 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

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[248].

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 imponendole come norme interne.

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"

Inoltre, l'imposizione di sanzioni penali e amministrative per violazione di norme nazionali, secondo quanto contemplato nel *considerandum n. 149,* devono fare riferimento all'art. 50 [249]della Carta dei Diritti fondamentali Dell'UE nonché all'articolo 4 del Protocollo n. 7 [250]della Convenzione Europea, per la salvaguardia dei diritti dell'uomo e delle Libertà fondamentali che prevedono il diritto di non essere giudicati o puniti due volte per il

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».

[248] BOLOGNINI L., BISTOLFI C., PELINO E., Il regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali, Milano, 2016

[249] Articolo 50 Carta dei diritti fondamentali UE («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».

[250] Articolo 4 Protocollo addizionale n.7 («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».

medesimo reato chiamato principio del *ne bis in idem,* letteralmente non due volte per la stessa cosa.

L'articolo 649 c.p.p. prevede che l'imputato che sia stato condannato con sentenza o con decreto penale divenuti irrevocabili o che sia stato prosciolto, non può essere nuovamente perseguito penalmente per il medesimo fatto neanche se viene modificato il titolo, il grado o alcune circostanze, con tale articolo si statuisce il principio del *ne bis in idem*, principio di civiltà che garantisce sia sul piano processuale che su quello sostanziale che un soggetto non possa per uno stesso reato essere processato due volte.

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.[251], 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.

Il predetto principio del *ne bis in idem* si applica all'ambito penale, ossia ai procedimenti e le sanzioni penali anche se a tal proposito la Corte di Giustizia si è più volte pronunciata ritenendo che in presenza di finalità repressive perseguite con l'applicazione di gravi e specifiche sanzioni amministrative, queste ultime possano essere considerate di natura sostanzialmente penale.[252]

Per tali motivi è bene sottolineare che eventuali sanzioni penali ed amministrative applicate ai medesimi fatti illeciti possono prestare il fianco a

---

[251] 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».

[252] *Ex multis*: Corte EDU, 4.3.2014, Grande Stevens e altri contro Italia; Corte EDU, 8.6.1976, Engels e altri contro Paesi Bassi; Corte di Giustizia Dell'Unione Europea, Grande Sezione, causa C-524/15, Sentenza 20.3.2018.

delle ingerenze dell'uno nei confronti dell'altro, dando luogo alla violazione del principio del *de bis in idem* che alla base del sistema penale italiano.

Dunque può accadere che in una medesima fattispecie di reato si configuri la necessità di applicare una normativa sanzionatoria di tipo penalistico ed una normativa sanzionatoria di tipo amministrativo, creando una convergenza nell'applicazione delle sanzioni penali ed amministrative, in cui queste ultime se particolarmente gravi si possono ritenere sanzioni sostanzialmente penali.[253]

Pertanto, al fine di risolvere il problema della compatibilità con il principio del *de ne bis in idem* è importante leggere uno dei principi fondamentali del sistema penale, espressamente sancito dall'articolo 27 della Costituzione italiana e dall'articolo 40 del codice penale[254] che prevedono che l'imputato non è considerato colpevole sino alla condanna definitiva e che la responsabilità penale è personale.

Le sanzioni inflitte non possono essere lesive della dignità umana e contrarie al senso di umanità e devono tendere alla rieducazione e risocializzazione del condannato finalizzate alla reintegrazione dello stesso nel tessuto sociale.

Infatti, uno dei principi cardine su cui si basa il nostro sistema giuridico penale consiste nella circostanza che soltanto una persona fisica può essere sottoposta ad un procedimento penale non anche una persona giuridica.

Invece, la responsabilità amministrativa, secondo il decreto legislativo 231/ 2000 può essere attribuita sia alle persone fisiche che agli Enti pertanto alla luce di tale riflessione possiamo affermare che nel caso in cui il responsabile della violazione sia soltanto il titolare del trattamento come nel caso delle *Big Tech Companies***,** che in genere è una persona giuridica ossia una società, l'illecito sarà da ascrivere esclusivamente nell'ambito amministrativo e non penale, mentre nel caso in cui il trasgressore del

---

[253] *Ex multis*: Corte EDU, 4.3.2014, Grande Stevens e altri contro Italia; Corte EDU, 8.6.1976, Engels e altri contro Paesi Bassi; Corte di Giustizia Dell'Unione Europea, Grande Sezione, causa C-524/15, Sentenza 20.3.2018.

[254] Trattasi, nella maggior parte dei casi, di forme giuridiche sociali che escludono completamente una identificazione soggettiva e personale tra l'imprenditore, persona fisica e l'impresa (società per azioni, società a responsabilità limitata).

trattamento dei dati personali sia una persona fisica l'illecito commesso può essere configurato sia nell'ambito amministrativo che penale.[255]

La giurisprudenza ha emesso svariate sentenze sul doppio binario sanzionatorio amministrativo-penale relativamente all'esistenza o meno di un reale rischio di duplicazione sanzionatoria nell'ambito della *privacy* in particolare i giudici della Corte EDU nella sentenza Grande Stevens[256], in palese contrasto con il principio del *ne bis in idem* avviarono un processo penale dopo che gli erano state comminate da parte della Consob, sanzioni di carattere amministrativo particolarmente afflittive da poter essere considerate di natura penale.

Inoltre, successivamente la sentenza A e B c. Norvegia[257], escluse la sussistenza della violazione del principio *ne bis in idem* in argomento, poiché tra i due procedimenti vi fu una connessione sostanziale e temporale abbastanza stretta "*a sufficiently close connection in substance and time" [258]*

Relativamente al punto della connessione sostanziale vi è da mettere in evidenza alcuni elementi primo fra tutti il perseguimento di obiettivi complementari e quindi di un'analisi non solo astratta ma anche concreta delle diverse sfaccettature della condotta illecita oggetto di esame.

Un altro elemento è la prevedibilità che la stessa condotta possa dare vita giuridicamente a due diversi procedimenti (penale e amministrativo), infatti, per evitare il rischio di una duplicazione di prove è necessaria un'adeguata

---

[255] FANELLI A., Le sanzioni penali correlate al GDPR, in cyberlaws.it.

[256] Corte Europea dei diritti dell'uomo, Seconda Sezione, sent. 4 marzo 2014, *Grande Stevens e altri c. Italia*, ric. n. 18640, 18647, 18663, 18668 e 18698/2010.

[257] Corte EDU, Grande Camera, 15 novembre 2016, A e B c. Noervegia, ric. nn.24130/11 e 29758/11.

[258] Cote EDU, *A e B c. Norvegia*, cit., paragrafo 132: «whether the different proceedings pursue complementary purposes and thus address, not only in abstracto but also in concreto, different aspects of the social misconduct involved; - whether the duality of proceedings concerned is foreseeable consequence, both in law and in practice, of the same impugned conduct (idem); - whether the relevant sets of proceedings are conducted in such a manner as to avoid as far as possible any duplication in the collection as well as the assessment of the evidence, notably through adequate interaction between the various competent authorities to bring about that the establishment of facts in one set is also used in the other set; - and, above all, whether the sanction imposed in the proceedings which become final first is taken into account in those which become final last, so as to prevent that the individual concerned is in the end made to bear an excessive burden, this latter risk being least likely to be present where there is in place an offsetting mechanism designed to ensure that the overall amount of any penalties imposed is proportionate».

collaborazione tra le varie autorità competenti, le quali stabiliranno di comune accordo che alcuni fatti accertati in uno dei due procedimenti possano essere adoperati anche nell'altro procedimento.

Pertanto, diventa necessario in sede di irrogazione della seconda sanzione tenere in considerazione il principio di compensazione, ossia di valutare gli effetti della prima affinché la seconda sanzione sia proporzionata.

Per quanto riguarda, invece, l'aspetto temporale dell'applicazione delle sanzioni, la predetta sentenza A e B c. Norvegia, non pretende che ci sia una simultaneità dei due procedimenti ma una connessione temporale più o meno vicina poiché l'obiettivo e proteggere l'individuo dal rischio di essere sottoposto ad un procedimento per un tempo molto lungo e di violare il principio del *ne bis in idem.*

Sul punto anche la Corte di giustizia si è adoperata circa le limitazioni da adottare al principio del *ne bis in idem,* ritenendo di essere concorde in linea di massima nel non applicare due sanzioni per il medesimo fatto.[259]

Giova ribadire che secondo i giudici europei la violazione dell'articolo 50 della Carta di Nizza e del principio del *ne bis in idem* si verifica nel caso in cui le sanzioni che vengono per prima applicate non rispettino nel complesso i caratteri della dissuasivita, effettività e proporzionalità, ed inoltre, il giudice nazionale che ha la competenza a giudicare della fattispecie del caso concreto non effettui una valutazione del cumulo sanzionatorio complessivo e non tenga in considerazione l'applicabilità dei criteri normativi sopra richiamati.[260]

Secondo i giudici comunitari nel caso in cui il doppio binario si concretizzi in una sorta di sistema penale-amministrativo integrato, capace di inquadrare i diversi aspetti del fatto illecito in maniera differente, ma riconducibile ad un'unica azione e non vi sia una pura duplicazione delle

[259] Corte di Giustizia UE, Grande Sezione, 26.2.2013, c/617-10; CGUE, 20 marzo 2018, Garlsson Real Estate SA et al., C-537/16; CGUE, 20 marzo 2018, C-524/15, C-596/16
[260] Corte di Giustizia Dell'Unione Europea, Grande Sezione, causa C-524/15, Sentenza 20.3.2018.

accuse non si configurerebbe alcuna violazione del principio del *ne bis in idem.*[261]

Cosicché, i procedimenti dovranno essere condotti in maniera da evitare duplicazioni tra la valutazione sanzionatoria del primo procedimento con la valutazione del secondo procedimento in modo tale da garantire un'effettiva unitarietà.

Ad ogni modo l'interpretazione del principio del *ne bis in idem* espressa dal giudice europeo e prevista dall'articolo 50 della Carta di Nizza consiste in una guida in ordine all'interpretazione del *considerandum* n. 149 del Regolamento, il quale prevede che le sanzioni penali applicate dai legislatori nazionali nell'ordinamento giuridico interno, non possono contrastare con il principio del *ne bis in idem* così come è stato anche enunciato dalla Corte di Lussemburgo.[262]

Sulla predetta tendenza si è creata anche una corrente giurisprudenziale comunitaria sostenuta dalla Corte EDU compatibile con l'articolo 50 della Carta di Nizza in base alla quale è possibile secondo i Paesi membri iniziare un procedimento penale a carico di un soggetto che abbia già subito l'applicazione di una sanzione amministrativa, purché ci sia un'armonizzazione dei due ambiti sanzionatori e comunque ci sia un interesse generale affinché le predette sanzioni tra loro abbiano un ruolo di completamento.

Il predetto orientamento giurisprudenziale richiede che all'interno dell'ordinamento giuridico di uno Stato membro, le norme che garantiscano questa coordinazione devono consentire che l'applicazione della sanzione complessiva sia proporzionata alla gravità del fatto posto in essere.

Per cui è necessario che ogni fattispecie sia valutata dal giudice nazionale caso per caso affinché valuti la proporzionalità della sanzione comminata in relazione al fatto commesso e alla gestione del cumulo dei procedimenti nei confronti dell'individuo.

---

[262] CASSANO G., COLAROCCO V., GALLUS G.B., MICOZZI F.P., SORO A., BARBAROSSA M., *op. cit.,* pp. 424 e 425.

A tal proposito, bisogna valutare in che maniera viene disciplinata la combinazione tra le nuove disposizioni relative alle sanzioni amministrative disciplinate dal Regolamento e come queste ultime siano coordinate in relazione alle sanzioni penali già esistenti di natura nazionale contenute nel decreto legislativo 196/2003, il quale stabiliva un apparato sanzionatorio amministrativo che poteva essere perfettamente sovrapponibile alle clausole del GDPR.[263]

La predetta integrazione è stata per lo più esercitata a seguito della già citata delega conferita al Parlamento con la legge n. 163/2017 e grazie all'esercizio della predetta, il Governo con il decreto legislativo numero 101/2018 mediante il legislatore nazionale ha adeguato ed armonizzato la normativa interna a quella comunitaria, ossia al Regolamento UE 679 del 2016.

Infatti, se in un primo momento il Governo pensava di abrogare completamente il decreto legislativo numero 196/2003, grazie all'intervento delle Commissioni Parlamentari e del Garante della *Privacy* che sono intervenuti in senso contrario è stato possibile effettuare un opportuno adeguamento del vecchio codice, attraverso il decreto legislativo 101/2018 il quale si è armonizzato con la normativa europea attraverso la tecnica della novellazione.[264]

Infatti, in ambito penale, come abbiamo potuto constatare il decreto legislativo n. 101/2018 ha apportato alcune modifiche abrogando e novellando il D. Lgs 196/2003 ed introducendo nuovi reati.

Invece, nell'ambito amministrativo l'art. 15 del decreto legislativo n. 101/2018 ha novellato l'art. 166 del Codice *Privacy* con la conseguenza che

---

[263] RATTI M., *Il regime sanzionatorio previsto dal Regolamento per l'illecito trattamento dei dati personali,* in FINOCCHIARO G., *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna 2017, pp. 610 e 611. L'autrice metteva in evidenza, in un momento in cui ancora il legislatore nazionale non aveva provveduto a dar corso ad una armonizzazione della normativa interna con quella Europea, che nel caso di contrasto della normativa comunitaria con quella interna in materia di *privacy* si sarebbe dovuto propendere per la diretta applicabilità delle norme del Regolamento con conseguente disapplicazione della normativa interna.

[264] FINOCCHIARO G., *La protezione dei dati personali in Italia: regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna 2019, diffusamente.

potevano essere applicate le sanzioni pecuniarie espressamente previste dal GDPR comportando l'introduzione di un quadro sanzionatorio molto più rigido rispetto alla normativa precedente.[265]

Al fine di comprendere il piano sanzionatorio amministrativo e penale che vige nel nostro ordinamento giuridico in relazione al trattamento dei dati personali e al principio del *ne bis in idem* è necessario analizzare l'art. 167 del D.lgs. n. 196/2003 novellato dal D.lgs. n. 101/2018.

L'articolo 167 del codice della privacy, prevede che qualora il Pubblico ministero venga a conoscenza di una *notitia criminis*, in ordine ai reati riguardanti il trattamento dei dati personali, secondo i commi 1 e 3, deve dare immediata comunicazione al Garante, in quest'ottica il legislatore ha voluto dare l'idea di una convivenza del procedimento amministrativo e di quello penale.[266]

Successivamente il comma 5 prevede che il Garante una volta acquisita la *notitia crimini* ha il compito di trasmettere al Pubblico ministero una relazione motivata che faccia riferimento a tutta la documentazione acquisita durante la fase di accertamento ed istruttoria, nella quale emergono i fattori che hanno consentito o meno la configurazione dell'illecito penale.

Pertanto, nell'attuale fattispecie che vede coinvolti il Pubblico ministero ed il Garante si evince in maniera chiara che vi è un obbligo di cooperazione tra le superiori figure rispetto alla precedente normativa.

La predetta circostanza crea un doppio binario su cui scorrono parallelamente il procedimento amministrativo ed il processo penale creando

---

[265] VALLEFUOCO V., ALAMPI A., *Nuove tutele in materia di privacy, regime sanzionatorio e questioni di diritto transitorio,* in *Fisco,* 2018, pp. 2254 e ss.

[266] Cfr. Protocollo di intesa tra Procura della Repubblica di Roma e Autorità Garante per la protezione dei dati personali, 8.1.2019. Il protocollo individua nell'avvenuta notifica della conclusione delle indagini preliminari, all'indagato ed al difensore di questi, il momento a partire dal quale deve essere effettuata, senza ritardo, la comunicazione al Garante in ordine agli elementi essenziali e necessari ai fini dell'accertamento di eventuali illeciti in materia di protezione dei dati personali correlati al fatto di reato. Tale scansione temporale consente di rispettare nella maniera più rigorosa il segreto investigativo in relazione al procedimento penale in corso, nonché l'efficienza dell'azione del Garante, limitando la comunicazione ai casi nei quali gli elementi acquisiti siano idonei a sostenere l'accusa in giudizio.

una complementarietà dei due apparati sanzionatori penale ed amministrativo, senza che per questo si creino dei conflitti di incompatibilità.

Continuando con il comma 6 sempre dell'articolo 167 del codice della *privacy*, possiamo evincere che è possibile che ci sia una diminuzione della pena nel caso in cui per lo stesso fatto sia stata comminata l'irrogazione di una sanzione amministrativa pecuniaria all'imputato relativa al Regolamento o al codice *privacy* da parte del Garante e questa sia stata già riscossa.

Tale meccanismo di complicità e di complementarietà consente di garantire l'applicazione di una sanzione penale ispirata alla proporzionalità e alla ragionevolezza di un sistema che prevede un processo penale e un procedimento amministrativo nel quale possono interagire fra di loro.[267]

Pertanto, il giudice penale gioca un ruolo fondamentale, poiché dovrà stare attento all'entità della sanzione amministrativa già combinata e riscossa nei confronti del soggetto agente a seguito del procedimento svolto innanzi al Garante per poter combinare una sanzione penale proporzionata ed adeguata al caso concreto.

Il nuovo quadro normativo relativo all'ambito sanzionatorio comporta un divieto effettivo di doppia sanzione, pertanto, nel caso in cui un soggetto per il medesimo illecito abbia già subito un procedimento amministrativo giunto al termine con l'applicazione della relativa sanzione e per lo stesso fatto è pendente un ulteriore giudizio di natura penale, il giudice quando quantificherà la sanzione penale sia essa detentiva o pecuniaria, dovrà tenere conto della sanzione amministrativa già applicata allo stesso autore del reato nel precedente procedimento amministrativo[268].

Qualche difficoltà invece sorge nell'ipotesi opposta, ossia qualora il procedimento penale dovesse finire prima di quello amministrativo con sentenza irrevocabile di condanna per cui l'applicazione della sanzione penale sarebbe precedente all'irrogazione della sanzione amministrativa.

---

[267] CADOPPI A., CANESTRARI S., MANNA A., PAPA M., *op. cit.,* p. 1014.

[268] NOTARO L.*, Il doppio binario in materia di protezione dei dati personali: sanzioni penali e sanzioni amministrative, fra ne bis in idem "europeo" e primato del diritto UE,* in *Diritto penale e privacy*, a cura di MASSARO A., Pisa, 2020, p.128.

A tal proposito il codice *privacy* è privo di una disposizione che sia capace di regolare il successivo procedimento sanzionatorio amministrativo davanti al Garante nel caso in cui il processo penale è già terminato con sentenza penale passata in giudicato ed irrevocabile, poiché manca una normativa speculare a quella prevista dall'articolo 167 comma 6 del codice.

Probabilmente sarebbe necessario un maggiore collegamento tra i testi normativi così da poter garantire il rispetto del principio del *ne bis in idem* e adottare delle normative interne in armonia con quelle europee ed internazionali.

L'articolo 167 *terdecies* TUF, rubricato "*applicazione ed esecuzione delle sanzioni penali ed amministrative",* prevede che nella fattispecie in cui per lo stesso fatto illecito, l'imputato subisca due procedimenti di natura penale ed amministrativa, l'autorità che applicherà la seconda sanzione dovrà valutare la precedente sanzione sia essa di natura penale o amministrativa affinché sia proporzionata all'illecito commesso e alla prima sanzione applicata.

Alla luce di quanto rappresentato sino ad ora la disciplina della *privacy* contempla il doppio binario che riguarda l'assetto sanzionatorio penale ed amministrativo.

Una parte della dottrina[269] ha valutato la connessione sostanziale temporale e si può escludere che la duplice applicazione di una sanzione possa violare il principio del *ne bis in idem*, in questa maniera viene sicuramente rispettato il criterio della prevedibilità relativamente all'applicazione di una sanzione amministrativa/ penale.

La coordinazione dei procedimenti di cui ai commi 4 e 5 dell'articolo 167 codice *privacy* che abbiamo già citato, prevedono una conversazione iniziale tra l'Autorità Garante e il Pubblico Ministero non prevedendo in alcun modo

[269] DEAGLIO L., *Il compendio sanzionatorio della nuova disciplina privacy sotto la lente del ne bis in idem sovranazionale e della Costituzione, in Nuove Frontiere tecnologiche e sistema penale. Sicurezza informatica, strumenti di repressione,* in *Diritto penale Contemporaneo,* 2019.
MANES, V. E MAZZACUVA, F. (2019), "*GDPR e nuove disposizioni penali del codice privacy", Diritto penale e processo*, 2, pp. 167-171.

niente sulla minimizzazione del rischio di duplicazioni nell'acquisizione e nella valutazione delle prove.

Diversamente per la connessione temporanea non può essere stabilita in precedenza ma deve essere analizzata volta per volta dal giudice.[270]

In conclusione possiamo affermare con certezza che all'articolo 167 comma 6 del codice *privacy* è previsto il rispetto e la proporzionalità della pena tenuto conto che il giudice penale dovrà valutare e ridurre proporzionalmente l'entità della pena da applicare in presenza di una condanna intervenuta già in sede amministrativa e già conclusasi a sfavore dell'autore del reato.

Nella predetta circostanza non si crea più una violazione del principio del *ne bis in idem* poiché si mira a raggiungere un trattamento sanzionatorio compatibile col principio di proporzionalità della pena.

Il giudice penale ridurrà sensibilmente in maniera proporzionale l'entità della sanzione in presenza di una condanna intervenuta precedentemente in sede amministrativa, in questo modo non potrà mai verificarsi la violazione del principio del *ne bis in idem* in quanto viene messo in atto un meccanismo finalizzato a rendere il trattamento sanzionatorio compatibile col principio di proporzionalità nel complessivo trattamento sanzionatorio.

In buona sostanza, nel caso di una sanzione formalmente amministrativa ma sostanzialmente penale, secondo la Convenzione CEDU, comminata all'imputato successivamente condannato in sede penale per il medesimo fatto illecito, il giudice dovrà applicare la pena tenendo conto di quella già irrogata secondo il criterio di ragguaglio previsto dall'articolo 135 codice penale, prendendo eventualmente in considerazione le circostanze attenuanti generiche e valutando la situazione economica del reo.[271]

Viceversa non è possibile applicare la fattispecie contraria, ossia qualora la condanna penale avvenga prima dell'applicazione della sanzione

---

[270] Corte di Giustizia UE, *Menci*, cit.

[271] Cassazione Penale, Sez. III, 20 gennaio 2022 (ud. 15 ottobre 2021), n. 2245. 555 MARTORANA M., BARBERISI A., PIZZETTI F., OP. CIT., P. 141.

amministrativa, generando in tale fattispecie il rischio di irrogare una duplice sanzione.

Conclusioni

Con il presente elaborato si è affrontato un delicato argomento relativo alla tutela penale del trattamento dei dati personali anche su larga scala sia nazionale che internazionale.

Lo stile di vita dell'attuale società è profondamente cambiato rispetto al passato e con esso anche il concetto di *privacy*.

Inizialmente si parlava di "diritto a essere lasciati soli" e godere del proprio privato, considerando la vita dal punto di vista intellettuale ed emotivo ritenendo che i pensieri, le emozioni e le sensazioni hanno pari dignità e necessità di essere tutelati alla stessa stregua dei beni materiali.

Piano piano il concetto di privacy si evolve acquisendo la veste di diritto a non subire ingerenze nella propria sfera intima, sino ad assumere la valenza positiva di diritto al controllo delle proprie informazioni.

Oggi il termine "dato personale" viene definito *data protection,* poiché la nostra società è fondata sulla tecnologia che è diventata ormai di uso comune e quotidiano con risvolti sociali ed economici, poiché si avvale della digitalizzazione basata su un utilizzo sistematico di dati, per cui nasce la necessità di una normativa basata sulla protezione e sulla correttezza del trattamento dei dati personali, ciò comporta un diritto alla trasparenza e alla liceità nell'interesse del singolo e della collettività.

A tal proposito, l'Italia si è adeguata all'evoluzione della normativa in ordine al trattamento dei dati personali, attraverso l'introduzione del D.lgs. n. 101 del 10 agosto 2018 che ha novellato ed ampliato il Codice *privacy* D. lgs. 96/2003, con fattispecie penali finalizzate a tutelare il corretto trattamento di dati anche su larga scala, disciplinate dagli articoli167 *bis* e 167 *ter*[272]*,* un esempio ne è il recente caso di cronaca internazionale *Cambridge Accademy*, relativo ai dati personali ottenuti in maniera illegale da parte di Facebook.

[272] LAMANUZZI M., Diritto penale e trattamento dei dati personali, cit., p. 223. 595 Ibidem. Considerandum n. 7 del GDPR.

Inoltre, si è illustrato il sistema sanzionatorio amministrativo e penale ed il principio del *ne bis in idem.*

Da quanto sopra rappresentato, si evince che il rapporto tra le sanzioni penali e quelle amministrative, qualora queste ultime siano particolarmente afflittive, possono essere considerate sostanzialmente di natura penale, creando un meccanismo di compensazione tra le une e le altre affinché il principio del *ne bis in idem* venga [273]salvaguardato.

Inoltre a livello europeo vi è stata l'introduzione del nuovo Regolamento UE 679/2016 che amplia la definizione del dato informatico attraverso l'inserimento dell'identità non soltanto come "corpo elettronico" ma anche come "corpo fisico"[274], in quest'ottica si crea l'identità sociale, ossia quel complesso di informazioni che riguardano la vita individuale e i rapporti sociali di un soggetto e dai quali emerge la personalità, i gusti, le preferenze e lo stile di vita di ciascun essere umano.[275]

Il diritto alla protezione dei dati personali è un diritto autonomo e distinto dal diritto alla riservatezza e dal diritto all'identità personale, comprende anche la *privacy* ma ne presuppone un *quid pluris.*[276]

Il diritto alla *privacy* tutela la vita privata anche al di fuori del contesto del trattamento dei dati, invece, la protezione dei dati personali tutela la correttezza del trattamento dei dati stessi indipendentemente dalla sfera privata dell'avente diritto.

Al proposito sì è pronunciata la Corte di Giustizia che ha precisato che le due nozioni sono distinte e separate, poiché il diritto alla *privacy* comporta il diritto ad avere uno spazio privato immune da ingerenze invece, il diritto alla protezione dei dati personali consiste nel diritto ad un corretto trattamento dei propri dati secondo la normativa vigente nazionale ed europea.

---

[273] RICCIO G. M., SCORZA G., BELISARIO E., op. cit., pp. 618 e ss.
[274] P. TRONCONE, op. cit., p. 63.
[275] RESTA F., I reati in materia di protezione dei dati personali, in CADOPPI A., CANESTRARIS S., MANNA A., PAPA M., Cybercrime, cit., p. 1019 ss.
[276] L'articolo 1 codice privacy riproduce esattamente la disposizione contenuta nell'articolo 8 della Carta di Nizza.

Tale distinzione è facilmente individuabile anche osservando il bene oggetto di tutela, poiché, il diritto alla *privacy* ha una portata esclusivamente individualistica, invece nel diritto alla protezione dei dati personali persiste non soltanto l'interesse dell'individuo ma anche quello della collettività. [277]

Come affermava il professore Rodotà[278] nella società digitale noi siamo i nostri dati passando *dall'habeas corpus all'habeas data* il denominatore comune rimane il controllo sui dati personali.

I predetti principi non si sono cristallizzati soltanto nell'ambito nazionale, poiché il quadro normativo si è evoluto anche nel campo comunitario, con l'entrata in vigore del regolamento europeo 2016/679/UE o GDPR, che è considerato una pietra miliare nello sviluppo di un quadro regolatore europeo in uno dei settori più sensibili della tutela dei diritti umani, quella dei dati personali, armonizzato nel nostro Paese con il decreto n.101 del 10 agosto 2018.[279]

Spesso, ancora oggi, accade che il concetto di protezione dei dati personali non è sempre ben definito, poiché è un diritto ancora in forte evoluzione ed in corso di definizione, a tal proposito, bisogna sempre ricordare che i diritti umani sono diritti storici e come tali si evolvono e cambiano in relazione alle mutevoli necessità della società.

La *ratio* ispiratrice del GDPR mira, pertanto, a dare all'Europa una normativa comune sul trattamento dei dati personali alla luce dell'innovazione tecnologica ed economica degli ultimi anni, promuovendo «*la certezza giuridica e operativa tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche, poiché l'obiettivo dichiarato del Regolamento è quello 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».*[280]

---

[277] 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.
[278] RODOTÀ S., Il mondo nella rete. Quali i diritti, quali i vincoli, Roma – Bari, 2014

[280] FINOCCHIARO G., prefazione in NIGER S., Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali, Padova, 2006.

In Italia la normativa sulla privacy ha assunto un ruolo fondamentale per la salvaguardia del diritto alla protezione dei dati personali, ciò è stato possibile attraverso l'adeguamento del codice della *privacy* del 2003 mediante l'intervento del D. lgs. 101/2018 e del GDPR che hanno modificato l'arsenale sanzionatorio introducendo nuove fattispecie di reato e lasciando inalterate altre già esistenti.

Il diritto alla protezione dei dati dovrebbe essere posto al centro dell'attenzione di ogni Governo nella consapevolezza che su di esso si misura la qualità della democrazia e da esso dipende la libertà della collettività.[281]

Per tali motivi, 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 riguarda un soggetto ma la tutela va posta in essere anche nell'interesse del Paese, e pertanto di tutta la collettività.[282]

La disciplina (normativa sulla protezione dei dati personali) è corretta, ma a volte la legge e la sola repressione sono insufficienti a proteggere gli interessi del soggetto interessato, per cui è necessario modulare le misure sanzionatorie e ricorrere a strumenti alternativi, come l'autodisciplina, per garantire una piena ed effettiva tutela.

Anche le disposizioni attuative nazionali sono importanti nella protezione dei dati personali, oltre al Regolamento europeo che rappresenta il testo base.

Occorre saper modulare le misure sanzionatorie in modo da consentire una piena ed effettiva tutela degli interessi in gioco.[283]

Il nuovo Regolamento europeo sulla protezione dei dati (GDPR) [284]costituisce una sfida epocale, ma per garantire l'effettività dei diritti sanciti

---

[281] BUTTARELLI G., Roma, 2019.

[284] BOLOGNINI L., BISTOLFI C., PELINO E., Il regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali, Milano, 2016

dal Regolamento, serve la diffusione di una cultura della privacy che riconosca il legame tra libertà, dignità e privacy, così come professato dal Professor Rodotà.

A volte è necessario ricorrere agli strumenti alternativi rispetto a quelli espressamente stabiliti dal legislatore e saper dosare le misure sanzionatorie affinché possano essere applicate con una giusta tutela.

L'Italia è promotrice della tutela e della cultura della protezione dei dati e le istituzioni in tale situazione hanno un ruolo fondamentale, per cui anche il nuovo regolamento europeo costituisce una cornice normativa fondamentale, poiché contribuisce a garantire l'effettività dei diritti sanciti dal regolamento e dalle altre normative.

La protezione dei dati personali e la privacy sono concetti legati, ma con una distinzione: la privacy riguarda la sfera privata individuale, mentre la protezione dei dati personali ha una natura sia individuale che collettiva.

La salvaguardia dell'autodeterminazione informativa è essenziale per mantenere il controllo sulla propria identità digitale e la propria libertà.

Le violazioni della protezione dei dati personali possono avere conseguenze concrete, come l'esposizione non desiderata della propria persona o la salute, se i dati manipolati sono quelli di una cartella clinica.

La capacità di proteggere i dati personali dovrebbe essere vista non solo come un obbligo giuridico, ma anche come un asset competitivo.

A mio modesto parere ritengo che per garantire l'effettività dei diritti sanciti dal Regolamento e di tutta la normativa ad essa attinente bisognerebbe promuovere la cultura della *privacy* e del dato personale, affinché vi sia un reale riconoscimento del legame profondo tra libertà, dignità e *privacy* da parte di tutta la collettività.

In conclusione, il diritto alla protezione dei dati personali può essere visto sotto l'ottica di un incredibile risorsa che può conferire alla persona la sua libertà pur mantenendola al centro della società digitale.[285]

---

[285] 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.

ANTONINI E., Il *Trattamento illecito di dati personali nel Codice della Privacy: inuovi confini della tutela penale,* in Dir. pen. proc., 2005, 338 ss.

ANGIONI, *Condizioni di punibilità e principio di colpevolezza*, in Riv. It. Dir. Proc. Pen., 1989, p. 733.

ARENDT H., DAL LAGO A., *Vita activa. La condizione umana*, Milano, 2001.

ANTONINI E., *Il Trattamento illecito di dati personali nel Codice della Privacy: i nuovi confini della tutela penale*, in *Dir. pen. proc.,* 2005, 338 ss

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., *Privacy, Poverty, and the Constitution, Berkeley*, 1966.

BERGHELLA R., BLAIOTTA P., *Diritto penale dell'informatica e beni giuridici, in Cassazione Penale, 1995, 7, 1463*

BOLOGNINI L., *DL Capienze, ecco le sanzioni privacy per la responsabilità socialed'impresa*, in *agendadigitale.eu*, 2 dicembre 2021.

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.

BONFANTI M. E., *Il diritto alla protezione dei dati personali nel Patto internazionale sui diritti civili e politici e nella Convenzione europea dei diritti umani: similitudini e difformità di contenuti*, in *Dir. um. Dir. int.,* 2011, 445 ss.

BORGHI G., *Conversione Decreto capienze in G.U. luci e ombre in ambito privacy,* in *Quotidiano Giuridico*, 9 dicembre 2021.

BRIZZI F., *Privacy: la tutela dei dati personali*, Milano, 2020

BLAIOTTA R., *Le fattispecie penali introdotte dalla legge sulla privacy*, in Cass. Pen., 1999, p. 806.

CADOPPI A., CANESTRARI S., MANNA A., PAPA M., *Cybercrime,* Milano, 2019.

CALIFANO, COLAPIETRO, *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017.

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;

CARETTI P., *Diritto dell'informazione e della comunicazione. Stampa, radiotelevisione, telecomunicazioni, teatro e cinema*, Bologna, 2005.

CASSANO G., COLAROCCO V., GALLUS G.B., MICOZZI F.P., SORO A., BARBAROSSA M*., Il processo di adeguamento al GDPR: aggiornato al d.lgs. 10 agosto 2018, n. 101,* Milano, 2018.

CERRI A., *Identità personale*, in *Enc. giur.*, vol. XV, Roma, 1995, 6 ss.

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

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.

234

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.

COSTANTINI F., *Il Regolamento (UE) 679/2016 sulla protezione dei dati personali,* nel *Quotidiano Giuridico*, 28 giugno 2018.

COTELLI M., *Pornografia domestica, sexting e revenge porn fra minorenni. Alcune osservazioni dopo la pronuncia delle Sezioni Unite n. 51815/18***,** in *Giurisprudenza Penale Web*, 9 marzo 2019.

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., D'ORAZIO R., E., SORO A., FRANCESCHELLI V., BUTTARELLI G., BATTELLI E., *I dati personali nel diritto europeo*, Torino, 2019.

D'ACQUISTO G. et al., *Privacy by design in big data. An overvew of privacy enbancing technologies in the era of big data analytics,* in *enisa.europa.eu*, 17 dicembre 2015.

D'AGOSTINO L., *La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al D.Lgs. 10 agosto 2018, n. 101*, in *Arch. Pen.*, 2019, 24 ss.

DEAGLIO L., *Il compendio sanzionatorio della nuova disciplina privacy sotto la lente del ne bis in idem sovranazionale e della Costituzione, in*

Nuove Frontiere 188 *tecnologiche e sistema penale. Sicurezza informatica, strumenti di repressione,* in *Dir. pen. cont. – Riv. Trim.,* 2/2019, 201 ss.

DE BERNARDO G., *Le sanzioni penali previste nel nuovo d.lgs. 101/2018,* in *Giur. pen. Web*, 19 febbraio 2019.

DE MINICO G., *Costituzione. Emergenza e terrorismo*, Napoli, 2016.

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.

FABRIS F., *Il diritto alla privacy tra passato, presente e futuro*, in *Tigor*: *rivista di scienze della comunicazione – A.I*, 2009, 94 ss.

FALCINELLI D., *Tempi moderni e cultura digitale: il valore patrimoniale dell'identità umana "on line*", in *Indice pen.,* 2015, 297 ss.

FIANDACA G., MUSCO E., *Diritto penale. Parte generale*, Bologna, 2019.

FINOCCHIARO G., *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017.

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.

FINOCCHIARO G.*, La protezione dei dati personali in Italia: regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019.

GAGLIARDI M., *Diritto all'oblio,* in COMANDÈ G., MALGIERI G. (a cura di), *Guida al trattamento e alla sicurezza dei dati personali. Le opportunità e le sfide del Regolamento UE e del codice italiano riformato*, Milano, 2018, 50 ss.

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

235

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. I reati previsti dal Codice della privacy e la responsabilità amministrativa degli enti alla luce del regolamento 2016/679/UE,* in *IusOnline*, 1/2017, 218 ss.

LAMANUZZI M., *Tutela penale della Privacy,* in *Diritto on-line*, 2019.

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.

MACALUSO F., PURIFICATI J., *Dizionario della privacy: 53 brevi saggi sulla protezione dei dati personali*, Milano, 2021.

MANES P., *Il consenso al trattamento di dati personali*, Padova, 2001.

MANES V, MAZZACUVA F, *GDPR e nuove disposizioni penali del Codice privacy*, in *Dir. pen. proc.*, 2019, 171 ss.

MANNA A. *Beni della personalità e limiti della protezione penale*, Padova ,1989.

MANNA A., *Codice della privacy: nuove garanzie per i cittadini nel Testo unico in materia di protezione dei dati personali*, in *Dir. pen. proc.*, 2004, 17 ss.

MANNA A., *Il quadro sanzionatorio ed amministrativo del codice sul trattamento dei dati personali,* in *Dir. inform.*, 2003, 727 ss.

MANNA A., *La protezione penale dei dati personali nell'ordinamento italiano*, in *Riv. trim. dir. pen. econ.,* 1993, 188 ss.

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.

MARATONA M., *Decreto Capienze: come è intervenuto sul codice della Privacy. Il rapporto tra il trattamento dei dati personali dei cittadini e le finalità di interesse pubblico, le modifiche ai poteri del Garante, le misure in tema di revenge porn,* in *altalex.it*, 13 ottobre 2021.

MARTORANA M., BARBERISI A., PIZZETTI F., *GDPR e Decreto Legislativo 101/2018: vademecum del professionista: obblighi, adempimenti, strumenti di tutela,* Milano, 2019.

MERLI A., *Introduzione alla teoria generale del bene giudico*, Napoli, 2006.

MILLER A., *The assault of privacy*, in *DePaul L. Rev.*, 1971, 1062 ss.

MORTATI C., *Istituzioni di diritto pubblico*, Padova, 1975.

MUMFORD L., *La cultura delle città*, trad. it. Labò E. e M., Milano, 1967.

NICOTERA M., *Cambridge Analytica e usi illeciti di dati social, che cambia con il GDPR,* in *agendadigitale.eu*, 20 marzo 2018.

NEGROPONTE N. Being digital, 1995

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

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

NOTARO L*., Il doppio binario in materia di protezione dei dati personali: sanzioni penali e sanzioni amministrative, fra ne bis in idem "europeo" e primato del diritto UE,* in MASSARO A. (a cura di), *Diritto penale e privacy*, Pisa, 2020, 99 ss.

NUNZIANTE E., *Big Data. Come proteggerli e come proteggerci. Profili di tutela della proprietà intellettuale e protezione dei dati personali*, in *Law and Media Working Paper Series*, 2017.

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

ORLANDO S., *La tutela penale della privacy nel cyberspazio*, in *Dir. pen. cont. – Riv. Trim.*, n. 2/2019, 177 ss.

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

PANETTA R., *Circolazione e protezione dei dati personali, tra libertà e regole del mercato, Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018*, Milano, 2019.

PANETTA R., *Decreto di adeguamento GDPR: come cambiano le sanzioni e gli illeciti penali del Codice Privacy,* Milano, 2018.

PAPA A., *Espressione e diffusione del pensiero in Internet. Tutela dei diritti e progresso tecnologico*, Torino, 2009.

PERRI P., *Privacy, diritto e sicurezza informatica*, Milano, 2007.

PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati,* in PICOTTI L. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, 21 ss.

PIZZETTI F., *Codice privacy italiano dopo il Gdpr: come leggerlo e applicarlo ex decreto 101/2018*, in *agendadigitale.it*, 14 settembre 2018.

PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati personali*. *Dalla Direttiva 95/46 al nuovo Regolamento europeo,* Torino, 2016.

PLANTAMURA V., *La tutela dei dati personali*, in *Dir. inform*., 2007, 645 ss.

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

RATTI M., *Il regime sanzionatorio previsto dal Regolamento per l'illecito trattamento dei dati personali,* in FINOCCHIARO G. (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, 595 ss.

RESTA F., *I reati in materia di protezione dei dati personali*, in CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (a cura di), *Cybercrime*, Milano, 2019, 1020 ss.

RICCIO G. M., SCORZA G., BELISARIO E., *GDPR e normativa privacy*, Milano, 2018.

RODOTÀ S., *Elaboratori elettronici e controllo sociale*, Bologna 1973.

RODOMONTE P., *Banca dati della Polizia e diritti della persona*, in *Telem. e dir.* 1986, 879 ss.

RODOTÀ S., *Tecnologie e diritti*, Bologna, 1995.

RODOTÀ S., *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma, 1997.

RODOTÀ S., *Discorso di presentazione della Relazione annuale del Garante al Parlamento*,
17 luglio 2001.

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.

SCAGLIARINI (a cura di), *Il "nuovo" codice in materia di protezione dei dati personali. La normativa italiana dopo il d.lgs. 101/2018*, Torino, 2019.

SICA S., *Danno e nocumento nell'illecito trattamento di dati personali*, in *Dir. inform.*, 2012, 4-5, 715 ss.

SICA S., D'ANTONIO V., RICCIO, G. M., *La nuova disciplina europea della privacy*, Padova, 2016.

SIMONETTA B., *Cambridge Analytica fallisce, ma i personaggi chiave si spostano in Emerdata*, in *ilsole24ore.it*, 5 maggio 2018.

TOSI E., SORO A., FRANCESCHELLI V., BUTTARELLI G., BATTELLI E., *Privacy digitale: riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019.

TRONCONE P., *La Tutela penale della riservatezza e dei dati Personali, Profili Dommatici e nuovi approdi normativi*, Napoli, 2020.

TURILLI M., FLORIDI L., *The ethics of information transarency,* in *Ethics and Information Tecnology*, 2009, 105 ss.

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

VACIAGO G., *L'attuazione della Direttiva 2016/1148/UE sulla sicurezza delle reti e dei sistemi informativi: i punti di contatto con il Regolamento UE 2016/679*, in CUFFARO V., D'ORAZIO R., RICCIUTO V. (a cura di), *I dati personali nel diritto europeo*, Torino, 2018, 1147 ss.

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.

VALLEFUOCO V., ALAMPI A., *Nuove tutele in materia di privacy, regime sanzionatorio e questioni di diritto transitorio,* in *Fisco,* 2018, 2254 ss.

VIGANÒ F., *Garanzie penalistiche e sanzioni amministrative*, in *Riv. it. dir. e proc. pen.*, 2020, 4, 1775 ss.

WAGNER, K., *Here's how Facebook allowed Cambridge Analytica to get data for 50 million users*, in *www.recode.net*, 17 marzo 2018.

WARREN S. D., BRANDEIS L. D., *The Right to privacy. The implicit made explicit*, in *Harward Law Review*, 1890, 193 ss.

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.

ZENCOVICH Z., *Una lettura comparatistica della l. n. 675/96 sul trattamento dei dati personali*, in *Riv. trim. dir. e proc. civ.*, 1998, 734 ss.

ZICCARDI G., *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Milano, 2015.