



Università degli Studi di Salerno

CIRPA – Centro Interdipartimentale per la ricerca di Diritto, Economia e
Management della Pubblica Amministrazione

Prof. Aggr. Gaspare Dalia

Ricercatore di Diritto Processuale Penale
Docente di Diritto Processuale Penale Comparato
Dipartimento di Scienze Giuridiche – Scuola di Giurisprudenza
UNISA

**Dispensa teorico-pratica a supporto dell'incontro svoltosi
in modalità di didattica a distanza su piattaforma
Microsoft Teams il 3 luglio 2023.**

Nozioni e principi del Regolamento UE 679/2016

Nella realtà contemporanea assistiamo al
mutamento del concetto di privacy

Non più, o non solo, inteso come il diritto di proteggere la propria sfera privata, ma soprattutto come il diritto di controllare l'uso e la circolazione dei propri dati personali da parte di altri soggetti.

Tali dati costituiscono il bene primario dell'attuale società dell'informazione

Il mondo virtuale è ormai diventato un vero e proprio luogo in cui si esplica la propria personalità

Risultato → non si ha più una persona virtuale contrapposta alla persona reale, ma si tratta di un intreccio che restituisce la persona reale come connotata dal digitale.

Il diritto dell'interessato a controllare come vengono trattati i propri dati significa pretendere dal titolare del trattamento:

– livelli di sicurezza commisurati alla natura e alla finalità della raccolta.

Da ciò deriva la disciplina della “**Data protection**”

L'uso del termine “privacy” è frequente nel linguaggio corrente; tuttavia, in campo giuridico viene utilizzata la locuzione “**protezione dei dati personali**” proprio al fine di evidenziare la finalità della normativa dettata al riguardo.

Ciò consente di **distinguere il concetto di “riservatezza” da quello di “privacy”** spesso utilizzati, erroneamente, come sinonimi.

E quindi, il diritto alla **riservatezza** è da intendersi in senso ampio come **la possibilità di godere appieno della propria intimità;**

mentre il termine **privacy** non identifica più il semplice diritto ad essere lasciati indisturbati ma simboleggia **l'insieme delle libertà che sono coinvolte nel trattamento dei dati personali.**

Il motivo per cui l'Unione Europea si è dotata di un nuovo quadro normativo in tema di Data protection si evince dalla lettura dei **considerando 6 e 7 del Regolamento.**

(6) La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. **La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati**

personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che le riguardano.

La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.

(7) Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. **È opportuno che le persone fisiche abbiano il controllo dei dati personali che le riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche.**

Il regolamento UE 679/2016 consta di 173 considerando e 99 articoli ed è suddiviso in 11 capitoli.

Il Regolamento conferma i principi posti a fondamento del sistema di data protection così come introdotti dalla direttiva del 95/46/CE modificandone le modalità di applicazione.

Quali sono questi principi?

1) **principio dell'accountability**, art. 5 par. 2. **Il titolare del trattamento è competente per il rispetto dei principi applicabili al trattamento dei dati personali e deve essere in grado di provarlo.**

In virtù di questo principio, il Regolamento dispone che il titolare del trattamento adotti politiche ed attui misure adeguate a **garantire ed essere in grado di dimostrare che il trattamento dei dati personali sia conforme allo stesso Regolamento.**

Il Termine anglosassone, anche se tradotto con il termine “responsabilità” fa riferimento più ad un

principio di “**rendicontazione**” ossia alla necessità in capo al titolare del trattamento di introdurre meccanismi di responsabilizzazione interna mediante l’elaborazione di un idoneo sistema documentale di gestione della privacy anche attraverso l’elaborazione di specifici modelli organizzativi analoghi a quelli utilizzati nell’applicazione della disciplina del D.lgs. n. 231/2001¹.

¹ Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300.

In ambito pubblicitario il concetto di accountability è strettamente collegato a quello di trasparenza.

I corollari di tale principio, li riveniamo nell'art. 5, par. 1 e sono:

- a) «liceità, correttezza e trasparenza»;
- b) «limitazione della finalità»: i dati devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;

c) «**minimizzazione dei dati**»: i dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

d) «**esattezza**» e se necessario, aggiornati: devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

e) «**limitazione della conservazione**»: conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo **non superiore al conseguimento delle finalità** per le quali sono

trattati. I dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato;

f) «integrità e riservatezza» garantite attraverso l'adozione di misure tecniche e organizzative adeguate.

2) La data protection impact assessment, art. 35.

È un istituto cardine all'interno del nuovo regolamento europeo. L'art. 35 del Regolamento parla di valutazione d'impatto sulla protezione dei dati che deve essere effettuata dal titolare del trattamento e prima di procedere al trattamento quando lo stesso, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

3) La data breach notification, art. 33

Il Regolamento introduce, in capo ai titolari del trattamento, un obbligo generalizzato di comunicazione delle violazioni dei dati personali.

La *ratio* della disciplina si evince dal considerando n. 85 dove si afferma che una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni materiali o immateriali alle persone fisiche come la perdita del controllo dei dati personali o limitazione dei loro diritti, discriminazioni,

usurpazione di identità, perdite finanziarie, decifature non autorizzate della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale alla persona fisica interessata.

Non appena venga a conoscenza di una violazione dei dati personali il titolare del trattamento deve notificare la violazione dei dati personali all'autorità di controllo competente senza ingiustificato ritardo e ove possibile entro 72 ore dal momento che ne è venuto a conoscenza, a

meno che non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Oltre il termine delle 72 ore la notifica dovrebbe essere corredata dalle ragioni del ritardo e le informazioni potrebbero essere fornite in fase successive senza ulteriore ingiustificato ritardo.

Il responsabile del trattamento informa il titolare del trattamento, senza ingiustificato ritardo,

dopo essere venuto a conoscenza della violazione.

La notifica deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, per attenuarne gli effetti negativi.

Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale

documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

4) la privacy by design e by default, art. 25.

La disciplina in materia di protezione dei dati personali va considerata ed applicata fin dalla sua primissima fase di progettazione. Ogni progetto ad impatto privacy deve nascere ed essere costruito con impostazioni di default, che rispettino la disciplina in tema di protezione dei dati personali.

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Questi 4 elementi rappresentano gli assi portanti per un sistema corretto di tutela della privacy.

Ambito di applicazione soggettivo del Regolamento

Il Regolamento europeo si applica alle persone fisiche.

Infatti, l'art. 1 definisce l'ambito soggettivo di applicazione del Regolamento dichiarandone la sua

finalità alla protezione dei diritti e delle libertà fondamentali delle persone fisiche (art. 1, par. 2).

Ne consegue che il regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare ad imprese dotate di personalità giuridica.

Inoltre, il Regolamento non si applica alle persone fisiche solo quando si è in presenza di un trattamento per finalità esclusivamente personali o domestico e quindi senza connessione con attività professionale o commerciale.

Tuttavia, il regolamento si applica ai titolari o responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico.

Infine, il presente regolamento non si applica ai dati personali di persone decedute, salvo che gli Stati membri prevedano norme in tal senso.

Ambito di applicazione territoriale

L'art. 3 del regolamento rivede la concezione tradizionale del **principio di stabilimento del territorio** e sancisce che il Regolamento si applica al

trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento di un titolare del trattamento o di un responsabile del trattamento nell'Unione, **indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.** Inoltre, il regolamento si applica al trattamento di dati personali di interessati che si trovano nell'Unione effettuati da un titolare del trattamento o responsabile del trattamento che non è stabilito nell'Unione quando le attività di trattamento riguardano:

- l'offerta di beni o le prestazioni di servizi ai
suddetti interessati nell'Unione

indipendentemente dall'obbligatorietà di un pagamento dell'interessato,

- oppure il controllo del loro comportamento all'interno dell'Unione europea. Infine, il regolamento si applica anche al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione ma in un luogo soggetto al diritto nazionale di uno Stato membro in virtù del diritto internazionale pubblico.

Le figure della privacy e il concetto di “trattamento”

La corretta implementazione delle figure privacy all'interno dell'organizzazione è una *condicio sine qua non*, per il corretto trattamento dei dati personali.

All'interno del Regolamento europeo n. 679/2016, si parla del **Titolare del trattamento** come figura di “data controller” e **Responsabile del trattamento** come figura del “data processor”.

IL TITOLARE DEL TRATTAMENTO (persona fisica o giuridica, autorità pubblica, servizio o altro organismo) rappresenta il centro di imputazione giuridica del trattamento dei dati personali, che a norma dell'art. 4 del Regolamento assume, anche unitamente ad altro titolare (contitolarità), le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Il potere decisionale è l'elemento fondamentale che consente di individuare la figura del Titolare del trattamento.

Esempio

Il Garante con il provvedimento del 29 aprile 2009 ha individuato in Poste italiane la figura del Titolare del trattamento anche in caso di appalto, proprio in ragione del potere decisionale della società.

Sotto il profilo soggettivo la norma si riferisce sia a persone fisiche che giuridiche, tenuto conto che l'art. 28 del Codice privacy ora abrogato, precisava che quando il trattamento era effettuato da una persona giuridica, il titolare del trattamento era rappresentato dall'entità nel suo complesso.

A tal riguardo, anche il Garante ebbe modo di precisare che il riferimento alla persona fisica che compare nella definizione del titolare non riguarda coloro che amministrano o rappresentano la persona

giuridica, la pubblica amministrazione, o l'ente ma concerne gli individui che effettuano un trattamento di dati a titolo personale.

Qualora il trattamento sia effettuato nell'ambito di una persona giuridica, una pubblica amministrazione, un ente o organismo, il titolare è l'entità nel suo complesso (società, ministero, ente pubblico) **anziché le singole persone fisiche che compongono l'ente.** Al massimo tali soggetti individuali potrebbero assumere la qualifica di Responsabili.

Altro esempio riguarda gli istituti scolastici:



INFORMATIVA EX ART 13-14 DPGR 2016/679 E ART. 13 DLGS 196/2003

Prima che Lei ci fornisca i dati personali che La riguardano, in armonia con quanto previsto dal Regolamento Europeo sulla protezione dei dati personali n° 2016/679 e dal D.lgs. 30 giugno 2003, n. 196 c.d. Codice Privacy, il cui obiettivo è quello di proteggere i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali, è necessario che Lei prenda visione di una serie di informazioni che La possono aiutare a comprendere le motivazioni per le quali verranno trattati i Suoi dati personali, spiegandole quali sono i Suoi diritti e come li potrà esercitare. I dati saranno trattati in ottemperanza art 5 del DPGR 2016/679 secondo i principi di: liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza. Inoltre sono state adottate le misure e gli accorgimenti necessari al rispetto del principio di responsabilizzazione del titolare.

Chi è il Titolare del trattamento?

E' L'Istituto Comprensivo di [redacted] rappresentato dal Dirigente Scolastico [redacted] a cui lei potrà in ogni momento rivolgersi per esercitare i suoi diritti o semplicemente richiedere informazioni relative al trattamento dei suoi dati utilizzando questi recapiti diretti [redacted] email: [redacted] [redacted] ha nominato, come previsto dal DPGR 679/2016 [redacted]

Con la **sentenza n. 246/2019** la Corte dei Conti - Sezione Giurisdizionale per il Lazio – ha ritenuto responsabile il Dirigente scolastico per il danno indiretto causato all'Istituto, a seguito del pagamento di una sanzione amministrativa, irrogata dal Garante della privacy per la pubblicazione su internet di una **circolare contenente dati riguardanti scolari affetti da disabilità.**

Nella vicenda in esame l'Autorità Garante per la Protezione dei dati Personali veniva adita dal genitore di un alunno disabile, il cui nominativo era stato divulgato in rete.

L'Autorità, stante la diffusione su internet di dati idonei a rivelare lo stato di salute di minori di età, in violazione della normativa in esame, irrogava all'Istituto scolastico la sanzione amministrativa di € 20.000,00.

Tale sanzione veniva pagata con i fondi della scuola, con conseguente danno al bilancio dell'Istituto, le cui casse risultavano quindi depauperate ad opera della condotta gravemente negligente del Dirigente scolastico.

Dal giudizio era infatti emerso che il Dirigente scolastico aveva adottato la circolare interna avente

per oggetto la “Convocazione GHL (Gruppo di Lavoro per l’Handicap operativo)”, nella quale era contenuto un elenco dei nomi degli scolari minori dell’Istituto affetti da disabilità.

La circolare ovviamente doveva essere comunicata solamente alle famiglie degli studenti in forma riservata, sia in ragione della particolare situazione di salute degli alunni interessati, sia in quanto trattavasi di una comunicazione ad uso interno, contenendo un calendario di riunioni dei consigli delle classi con presenza di alunni con Handicap (GLH).

Malgrado ciò il Dirigente scolastico consentiva la divulgazione nella rete internet della circolare in forma integrale, non avendo prescritto alcun divieto di pubblicazione, né in ultimo controllato che la circolare non venisse pubblicata sul sito *web* dell'Istituto.

La Corte dei Conti nella pronuncia in esame riconosceva la responsabilità del Dirigente scolastico per aver violato la normativa in materia di protezione dei dati personali, in base alla quale il trattamento dei dati sensibili ad opera dei soggetti pubblici deve conformarsi “secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della

dignità dell'interessato", e svolgersi secondo alcuni principi espressamente indicati.

La sentenza affermava poi la responsabilità esclusiva del Dirigente scolastico, escludendo quella concorrente di altri docenti, in quanto il D.lgs. 30 marzo 2001 n. 165 attribuisce loro la responsabilità della organizzazione e gestione scolastica, da ciò ne consegue che sul Dirigente incombevano gli obblighi di verificare la correttezza e la legittimità della circolare sottoscritta e di monitorarne le sorti anche nei successivi passaggi, al fine di impedirne la

pubblicazione.

Posizione di garanzia/responsabilità oggettiva

RESPONSABILE DEL TRATTAMENTO: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che **tratta dati personali per conto del titolare del trattamento.**

La sua designazione si ritiene indispensabile quando per esigenze organizzative, la struttura abbia

dimensioni importanti sebbene dal punto di vista formale la sua designazione non sia obbligatoria. **Il Titolare deve individuare il Responsabile tra soggetti che abbiano capacità ed esperienza in materia di privacy e sicurezza e deve impartirgli direttive in ordine ai fatti, ai mezzi e alle modalità del trattamento.** A sua volta, **il responsabile, nell'esercizio dell'attività di trattamento deve attenersi alle istruzioni del titolare.**

Per quanto riguarda i requisiti formali della lettera di designazione, i compiti affidati devono

essere individuati sia per iscritto che analiticamente.

Il Responsabile può essere interno o esterno e a tale riguardo il Garante ha affermato che è necessario precisare chi svolgerà l'eventuale ruolo di responsabile del trattamento, conseguentemente l'amministrazione deve decidere se prevedere tale figura ed attribuire tale responsabilità o alla struttura esterna a cui è affidata l'attività in concessione, oppure ad un dipendente di quest'ultima o ad un proprio ufficio o dipendente dell'amministrazione.

In concreto la nomina del responsabile che deve essere effettuata in forma scritta e può essere inserita in un apposito articolo della convenzione o essere oggetto di un distinto provvedimento amministrativo o atto di diritto privato.

Nelle operazioni di trattamento affidate dal titolare al responsabile quest'ultimo si potrà servire, a sua volta, di un altro soggetto per il compimento di specifiche attività nell'ambito del trattamento che compie per conto del titolare. In questo caso, **il**

responsabile – previa autorizzazione scritta del titolare – procederà a nominare tale soggetto quale **sub-responsabile del trattamento obbligandolo ad osservare gli stessi obblighi, in materia di protezione dei dati, che gravano su di lui nel rapporto con il titolare.** Qualora il responsabile non provveda ad impartire al sub-responsabile le istruzioni previste, così come nel caso in cui il sub-responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

Resta inteso che eventuali modifiche, circa l'aggiunta o la sostituzione di altri sub-responsabili, debbano essere notificate al titolare (art. 28 par. 2 GDPR).

AUTORIZZATO AL TRATTAMENTO

La lettera h) dell'art. 4 del TU Privacy definiva gli incaricati del trattamento come “**le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile**”.

Il nuovo Regolamento europeo non ha disciplinato tale figura, pertanto allo stato attuale abbiamo all'interno del Regolamento solo le due figure del

titolare del trattamento e del responsabile del trattamento.

Tuttavia, a seguito della modifica introdotta dal **D.lgs 101/2018**, il TU Privacy ha visto l'introduzione dell'art. **art. 2-quaterdecies** **“Attribuzione di funzioni e compiti a soggetti designati”**.

La norma dispone che:

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.

La lettera di designazione dovrà permettere di capire la natura dei dati personali ai quali accede il soggetto incaricato e la tipologia di trattamento consentito.

Sull'argomento, il Garante ha sottolineato che la mera assegnazione di una persona ad una struttura

interna non soddisfa di per sé i requisiti previsti dalla legge, dovendo risultare chiaro a quale tipologia di dati hanno accesso le persone preposte alla struttura, al limite attraverso l'integrazione della originaria mansione. **È opportuno precisare che la nomina degli incaricati è obbligatoria.** Il Garante ha affermato che senza una formale designazione degli incaricati al trattamento, i dipendenti che nello svolgimento dei loro compiti vengono a conoscenza dei dati personali dovrebbero essere considerati soggetti terzi rispetto all'amministrazione con evidenti limiti alla comunicazione e utilizzazione dei dati.

La definizione di “terzo” è attualmente contenuta nell’art. 4, par. 1, n. 10) del Regolamento ossia: **la persona fisica o giuridica**, l'autorità pubblica, il servizio o altro organismo **che non sia** l'interessato, il titolare del trattamento, il responsabile del trattamento e **le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.**

CONTITOLARI DEL TRATTAMENTO – Art. 26
GDPR

È possibile che coesistano più titolari del trattamento che decidono congiuntamente di trattare i dati per una finalità comune.

1. Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di

comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati.

2. L' accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. **Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.**

3. Indipendentemente dalle disposizioni dell'accordo di cui al paragrafo 1, **l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento.**

Cosa si intende per trattamento?

Art. 4, par. 1, n. 2 Regolamento 2) **«trattamento»**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come **la raccolta, la registrazione,**

l'organizzazione, la strutturazione, la
conservazione, l'adattamento o la modifica,
l'estrazione, la consultazione, l'uso, la
comunicazione mediante trasmissione,
diffusione o qualsiasi altra forma di messa a
disposizione, il raffronto o l'interconnessione, la
limitazione, la cancellazione o la distruzione.

Elemento identificativo del trattamento è la finalità, che costituisce lo scopo effettivo per il quale i dati personali sono raccolti e gestiti. A ciascuna finalità corrisponde uno specifico trattamento.

I dati personali costituiscono una macro-categoria all'interno della quale la legge distingue due sottocategorie:

- dati sensibili,
- dati di natura giudiziaria.

Sono dati sensibili quelli che riguardano informazioni concernenti gli aspetti più intimi della vita di un individuo e sono tassativamente indicati dalla norma.

Il legislatore ha inteso, quindi, fornire garanzie rafforzate per quei dati che se non trattati con liceità

e correttezza potrebbero arrecare gravi danni all'interessato.

Mentre i dati personali comuni come il nome, il cognome, l'indirizzo mail hanno la finalità di identificare un individuo, quelli sensibili rivelano le condizioni religiose, gli orientamenti politici e sindacali, così come sono considerati dati super sensibili quelli idonei a rivelare lo stato di salute e la sfera sessuale delle persone. **Per la corretta configurazione di un modello di gestione privacy deve sempre essere eseguito un puntuale e**

preliminare censimento delle diverse tipologie di dati sensibili.

Un tema importante è quello relativo alla cosiddetta area di sensibilità, nel senso che la sensibilità dell'informazione personale dovrà essere intesa in modo relativo e valutata caso per caso con riferimento al contesto ed alla natura intrinseca dell'informazione.

Esempio

In passato il Garante ha vietato la comunicazione all'amministrazione di appartenenza della diagnosi da infezione da HIV accertata nei riguardi di una dipendente pubblica da parte della commissione medica preposta agli accertamenti sull'inabilità al lavoro.

Alla proposta della commissione di rilasciare un processo verbale con l'*omissis* sul punto relativo alla diagnosi, il Garante ha fatto rilevare come la non menzione del giudizio diagnostico in chiaro non sarebbe stato sufficiente in quanto essendo attualmente l'unico caso di diagnosi omessa,

avrebbe potuto consentire di desumere l'effettiva malattia diagnosticata.

Nella disciplina tracciata dal nuovo Regolamento UE **l'art. 9, par. 1** dispone che **è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiosi o filosofiche o l'appartenenza sindacale, nonché trattare dati genetici, biometrici intesi ad indentificare in modo univoco una persona fisica, dati relativi alla salute, alla vita sessuale oppure all'orientamento sessuale della persona.**

In sostanza viene riprodotta la nozione contenuta nella direttiva “madre” della comunità europea con l'introduzione di dati biometrici e genetici.

Tuttavia, la norma precisa che **il divieto non si applica se:**

a) l'interessato ha prestato il proprio **consenso esplicito** al trattamento di tali dati personali **per una o più finalità specifiche**, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;

b) il trattamento è necessario per assolvere gli **obblighi ed esercitare i diritti specifici** del titolare del trattamento o dell'interessato **in materia di diritto del lavoro e della sicurezza sociale e protezione sociale**, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

c) **il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra**

persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano

comunicati all'esterno senza il consenso dell'interessato;

e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualevolta le autorità giurisdizionali esercitano le loro funzioni giurisdizionali;

g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere

proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista

della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;

i) **il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica**, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri **che prevede misure appropriate e specifiche per tutelare i diritti e le libertà**

dell'interessato, in particolare il segreto professionale;

j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

3. I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale² conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza³ conformemente al diritto dell'Unione o

² Art. 622 c.p. “Rivelazione di segreto professionale” - Chiunque, avendo notizia, per ragione del proprio stato o ufficio, o della propria professione o arte, di un segreto, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto, è punito, se dal fatto può derivare nocumento, con la reclusione fino a un anno o con la multa da euro 30 a euro 516. La pena è aggravata se il fatto è commesso da amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci o liquidatori o se è commesso da chi svolge la revisione contabile della società. Il delitto è punibile a querela della persona offesa.

³ Art. 326 c.p. Rivelazione ed utilizzazione di segreto di ufficio - Il pubblico ufficiale o la persona incaricata di un pubblico servizio, che, violando i doveri inerenti alle funzioni o al servizio, o comunque abusando della sua qualità, rivela notizie di ufficio, le quali debbano rimanere segrete, o ne agevola in qualsiasi modo la conoscenza, è punito con la reclusione da sei mesi a tre anni.

Se l'agevolazione è soltanto colposa, si applica la reclusione fino a un anno.

degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.

I **dati giudiziari** sono quei dati personali idonei a rivelare i provvedimenti iscritti nel casellario giudiziario, le sanzioni amministrative dipendenti da reato ed i relativi carichi pendenti, i dati personali idonei a rivelare la qualità di indagato o di imputato. Sono esclusi dalla nozione i provvedimenti relativi a cause civili di ogni tipo e giudizi amministrativi,

Il pubblico ufficiale o la persona incaricata di un pubblico servizio, che, per procurare a sé o ad altri un indebito profitto patrimoniale, si avvale illegittimamente di notizie di ufficio, le quali debbano rimanere segrete, è punito con la reclusione da due a cinque anni.

Se il fatto è commesso al fine di procurare a sé o ad altri un ingiusto profitto non patrimoniale o di cagionare ad altri un danno ingiusto, si applica la pena della reclusione fino a due anni.

mentre sono dati giudiziari i provvedimenti definitivi di condanna penale relativi a delitti e i provvedimenti di espulsione e riabilitazione dei minori.

Il Regolamento UE tratta i dati personali relativi a condanne penale e reati all'interno dell'**art. 10**, stabilendo che il trattamento di dati personali relative alle condanne penale e ai reati o le connesse misure di sicurezza sulla base dell'art. 6, par. 1 deve avvenire soltanto sotto il controllo dell'autorità pubblica oppure se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri e che preveda

garanzie appropriate per i diritti e le libertà degli interessati. L'eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo da parte dell'autorità pubblica.

Il regolamento ha introdotto un livello ben superiore di responsabilità del titolare del trattamento rispetto alla direttiva 95/46/CE sulla protezione dei dati.

L'articolo 25 e l'articolo 32 del regolamento prevedono che i titolari del trattamento tengano conto “della natura, dell'ambito di applicazione, del

contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche”.

Anziché imporre un obbligo di risultato, tali disposizioni introducono obblighi di mezzi, il che significa che il titolare del trattamento deve condurre le valutazioni necessarie e giungere alle opportune conclusioni.

Una norma chiave è l'art. 32 «**Sicurezza del trattamento**»: Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del

trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, **il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:**

a) la pseudonimizzazione⁴ e la cifratura dei dati personali;

⁴ Art. 4, par. 1, n. 5) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal

trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non

tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

In ipotesi di omissione di tali misure di sicurezza o nel caso di inadeguatezza delle stesse ne consegue che:

(146) Il titolare del trattamento o il responsabile del trattamento dovrebbe risarcire i danni cagionati a una persona da un trattamento non conforme al presente regolamento ma dovrebbe essere esonerato da tale responsabilità se dimostra che

l'evento dannoso non gli è in alcun modo imputabile.

Il concetto di danno dovrebbe essere interpretato in senso lato alla luce della giurisprudenza della Corte di giustizia in modo tale da rispecchiare pienamente gli obiettivi del presente regolamento. Ciò non pregiudica le azioni di risarcimento di danni derivanti dalla violazione di altre norme del diritto dell'Unione o degli Stati membri. Un trattamento non conforme al presente regolamento comprende anche il trattamento non conforme agli atti delegati e agli atti di esecuzione adottati in conformità del presente regolamento e alle disposizioni del diritto degli Stati

membri che specificano disposizioni del presente regolamento.

Gli interessati dovrebbero ottenere pieno ed effettivo risarcimento per il danno subito. Qualora i titolari del trattamento o i responsabili del trattamento siano coinvolti nello stesso trattamento, ogni titolare del trattamento o responsabile del trattamento dovrebbe rispondere per la totalità del danno. Tuttavia, qualora essi siano riuniti negli stessi procedimenti giudiziari conformemente al diritto degli Stati membri, il risarcimento può essere ripartito in base alla responsabilità che ricade su ogni titolare del trattamento o responsabile del

trattamento per il danno cagionato dal trattamento, a condizione che sia assicurato il pieno ed effettivo risarcimento dell'interessato che ha subito il danno.

Il titolare del trattamento o il responsabile del trattamento che ha pagato l'intero risarcimento del danno può successivamente proporre un'azione di regresso contro altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento.

Il caso del liceo Montale

In data 31 marzo 2022 diverse testate giornalistiche pubblicavano articoli relativi ad una vicenda di cronaca che ha coinvolto la dirigente di un liceo romano – identificata con il nome e cognome e con alcune sue fotografie – e uno studente del liceo, diciottenne, successivamente alla rivelazione di una relazione sentimentale che sarebbe intercorsa tra i due sulla quale erano in corso accertamenti da parte dei competenti uffici scolastici.

Gli articoli pubblicavano diversi stralci dei messaggi che si sarebbero scambiati la dirigente e lo studente

riportando dettagli relativi ai rapporti personali tra gli interessati, anche attinenti alla sfera sessuale, indugiando sulle frasi che si sarebbero scambiati e sulle circostanze dei loro incontri.

Immediatamente, in data 2 aprile 2022, interveniva l'Autorità Garante con provvedimento n. 115 del 1° aprile 2022 [9759795] e disponeva in via d'urgenza, nei confronti di La Notizia S.r.l., in qualità di titolare del trattamento, la misura della limitazione provvisoria di ogni ulteriore diffusione, anche online, dei contenuti dei messaggi acquisiti e riportati nell'articolo sopra indicato, nonché in ogni eventuale

ulteriore articolo pubblicato dalla medesima o da altre testate editate dalla medesima società.

Le motivazioni:

“VISTO l’art. 137, comma 3, del Codice, il quale dispone che in caso di diffusione o di comunicazione di dati personali per finalità giornalistiche restano fermi i limiti del diritto di cronaca a tutela dei diritti di cui all’articolo 1 del medesimo Codice (dignità umana, diritti e libertà fondamentali della persona) e, in particolare, il limite dell’essenzialità dell’informazione riguardo a

fatti di interesse pubblico;

CONSIDERATO che tale principio richiamato in termini generali anche nelle Regole deontologiche (relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica" (G.U. del 4 gennaio 2019, n. 3), artt. 5 e 6) deve essere interpretato con particolare rigore con riferimento ad informazioni relative alla sfera sessuale (art. 11 delle Regole deontologiche);

RITENUTO che i dettagli descritti (e commentati) rinvenibili nei numerosi stralci di conversazioni e di messaggi riportati negli articoli nulla aggiungono in

merito alla necessità di fare chiarezza sulla vicenda e sulla regolarità delle condotte ascrivibili alla dirigente scolastica, sulle quali sono in corso i dovuti accertamenti;

CONSIDERATA dunque la necessità di garantire la riservatezza e la dignità delle persone coinvolte attraverso un intervento in via d'urgenza al fine di limitare l'ulteriore diffusione di dati personali”.

Tant'è che l'Autorità Garante disponeva ulteriori blocchi alla pubblicazione delle chat. Dopo La Repubblica, i provvedimenti riguardarono

Openonline.it, Letto quotidiano, Il Giornale, Il
Riformista, Skuola.net e La notizia giornale.

Responsabilità civile

Un angolo di visuale interessante per approfondire il tema del danno civile è quello degli artt. dal 15 al 22 del Regolamento che contengono i diritti dell'interessato la cui violazione determina la responsabilità civile per illecito trattamento dei dati personali.

Da ritenersi ancora attuali sono i principi sanciti dalla giurisprudenza di legittimità anche prima dell'emanazione del Regolamento UE.

La Suprema Corte ha chiarito che “il diritto ad esigere una corretta gestione dei propri dati personali, pur rientrando nei diritti fondamentali di cui all’art. 2 Cost. non è un totem al quale possano sacrificarsi altri diritti altrettanto rilevanti sul piano costituzionale (Cass. civ. sez. III, 20 maggio 2015, n. 10280), sicché le norme sulla tutela dei dati personali vanno coordinate e bilanciate con le norme costituzionali che tutelano altri e prevalenti diritti e con le norme ordinarie applicabili al singolo caso.

La sentenza appena illustrata in massima costituisce orientamento consolidato ed è un angolo di visuale interessante per approfondire il tema della responsabilità civile.

Sempre secondo (Cass. civ. sez. III, 20 maggio 2015, n. 10280) stabilire dunque se un soggetto pubblico o privato abbia o meno violato le regole legali sulla gestione dei dati altrui impone di interpretare queste ultime bilanciando gli interessi da esse tutelati con gli altri interessi costituzionalmente protetti potenzialmente in conflitto col diritto alla riservatezza.

Questo delicato equilibrio costituisce la bussola per orientare l'interprete al fine della qualificazione di una determinata fattispecie di presunto illecito trattamento dei dati personali come responsabilità civile o meno.

Nella medesima prospettiva, il legislatore comunitario specifica nel nuovo Regolamento europeo sulla protezione dei dati che “il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta ma va considerato alla luce della funzione sociale e va temperato con altri

diritti fondamentali, in ossequio al principio di proporzionalità (considerando n. 4).

Vi è un approccio pragmatico, operativo, funzionale da parte della giurisprudenza, in base al quale i giudici non si soffermano sulla natura della responsabilità civile (es. oggettiva o per colpa), ma è concentrato sul nesso di causalità e sull'onere della prova. **Vi è un atteggiamento di favore nei confronti del danneggiato. Il convenuto è onerato della prova di aver adottato tutte le misure idonee ad evitare il danno.**

(Cass. civ. sez. I, 25 gennaio 2017, n. 1931):
“ricostruita in termini di colpa presunta o di responsabilità oggettiva, non vi è dubbio che l'affermazione della responsabilità dell'esercente l'attività pericolosa, ai sensi dell'art. 2050 c.c.⁵, richieda comunque l'accertamento della sussistenza di un nesso di causalità tra l'attività e il danno patito dal terzo”; Cass., 23 maggio 2016, n. 10638; Cass., 10 marzo 2006, n. 5254.

⁵ Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno.

Sebbene la giurisprudenza italiana non assuma una posizione univoca in merito alla natura pericolosa delle operazioni di trattamento dei dati (la sentenza del 2017 ritiene che sia orientamento maggioritario la ricostruzione in termini di colpa presunta della responsabilità di cui all'art. 2050), il ragionamento di quella più sensibile al tema può trovare rappresentazione nel passo riprodotto

“il diritto alla riservatezza (o all'intimità della sfera privata dell'individuo) appare, ben più di altri aspetti di tutela della personalità, strettamente collegato alle profonde trasformazioni operate dalla società industriale e post-industriale [...] Ma è soprattutto

l'incessante progresso tecnologico, con il perfezionamento (e la pericolosità) dei mezzi di comunicazione di massa e degli strumenti di raccolta dei dati e notizie che, attraverso inedite, per il passato del tutto impensabili, e talora gravissime, aggressioni agli aspetti più intimi della personalità, richiede necessariamente l'individuazione di più adeguate ed efficaci difese" (Cass. civ, sez. I, 19 maggio 2014, n. 10947, Cass. civ., sez. I, 13 maggio 2015, n. 9785).

E abbiamo visto come il nuovo Regolamento aggrava la responsabilità del titolare del trattamento in ragione dell'incessante progresso tecnologico.

Responsabilità penale

Art. 167 (Trattamento illecito di dati) – TU Privacy

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129

arreca nocumento all'interessato, **è punito con la reclusione da sei mesi a un anno e sei mesi.**

2. 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 misure di garanzia di cui all'articolo 2-septies ((...)) arrecando nocumento all'interessato, è punito con la reclusione da uno a tre anni.

3. Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 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 nocimento all'interessato.

4. Il Pubblico ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante.

5. Il Garante trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al più tardi al termine dell'attività di accertamento delle violazioni delle disposizioni di cui al presente decreto.

6. Quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è

stata riscossa, la pena è diminuita.

Art. 167-bis (Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala).

1. Salvo che il fatto costituisca più grave reato, chiunque comunica o diffonde al fine di trarre profitto per sé o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli

2-ter, 2-sexies e 2-octies, è punito con la reclusione da uno a sei anni.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, è punito con la reclusione da uno a sei

anni, quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione.

3. Per i reati di cui ai commi 1 e 2, si applicano i commi 4, 5 e 6 dell'articolo 167.

Art. 167-ter (Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala)

1. 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.

2. Per il reato di cui al comma 1 si applicano i commi 4, 5 e 6 dell'articolo 167.

Art. 168 (Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante)

1. 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.

2. 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.

Art. 170 (Inosservanza di provvedimenti del Garante).

1. 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.

Art. 171(Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori).

1. La violazione delle disposizioni di cui agli articoli 4, comma 1, e 8 della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della medesima legge.

Art. 172

(Pene accessorie)

1. La condanna per uno dei delitti previsti dal presente codice importa la pubblicazione della sentenza, ai sensi dell'articolo 36, secondo e terzo comma, del codice penale.

TRIBUNALE DI NOCERA INFERIORE
sezione unica penale
ORDINANZA DI RIGETTO DELLA RICHIESTA DI ARCHIVIAZIONE
A SEGUITO DI OPPOSIZIONE
(art. 409 e 410 c.p.p.)

Il G.I.P., dott. [REDACTED]
a scioglimento della riserva assunta all'udienza camerale del 7.4.2022, nel procedimento penale a carico di
IGNOTI, in cui p.o. [REDACTED], iscritto per il reato di cui all'art. 323 c.p.;
precisato come l'udienza camerale sia stata fissata a seguito di opposizione a seguito di richiesta di archiviazione
del 29.7.2021.

All'udienza camerale, il P.M. non compariva, la Difesa della p.o. si riportava sostanzialmente all'atto di
opposizione e ne chiedeva l'accoglimento; il Giudice si riservava.

OSSERVA

Al termine delle indagini preliminari, il P.M. chiedeva l'archiviazione formulando condivisibili considerazioni
in ordine al reato di cui all'art. 323 c.p. (peraltro, nemmeno contestate dal difensore nell'atto di opposizione).
Di contro, poco convincenti appaiono le considerazioni da questi svolte in ordine a possibili illeciti relativi al
T.U. Privacy in relazione all'utilizzo di dati sanitari della [REDACTED] nell'ambito del procedimento disciplinare
contro di lei intentato dal Comune di [REDACTED] e, soprattutto, non condivisibile l'affermazione di non
poter iscrivere alcun nominativo al registro notizie di reato.

In particolare, il P.M. si limitava a prendere in considerazione esclusivamente il disposto dell'art. 167, co. 1,
obliterando, tuttavia, ogni valutazione in ordine alla più pertinente ipotesi di cui al successivo co. 2, da leggersi
in combinato disposto con l'art. 9 del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio
del 27 aprile 2016 e con l'art. 2-septies T.U. Privacy.

Orbene, lo scrivente ritiene di non poter allo stato accogliere la richiesta del P.M., dovendo questi, procedere
all'acquisizione di tutta la documentazione concernente l'avvio del procedimento disciplinare, anche al fine di
individuare i promotori responsabili, e procedere alla loro eventuale iscrizione al registro delle notizie di reato,
avendo questi utilizzato, per fini non legittimi, i dati riservati della p.o. (in particolare, al di fuori dei casi di
utilizzabilità elencati dall'art. 9, § 2 del richiamato Regolamento).

P.Q.M.

Letti gli artt. 409 e 410 c.p.p., rigetta, allo stato, la richiesta di archiviazione, ordinando al Pubblico Ministero
di svolgere le nuove indagini di cui alla parte motiva, anche alla luce delle valutazioni in diritto svolte, nel termine
di mesi 3 dalla comunicazione del presente atto.