avv. RICCARDO SALOMONE

(Foro di Torino)

I reati previsti dal Codice della Privacy

Gli illeciti penali relativi ai dati personali sono collocati agli artt. 167 e segg. D. Lgs. n. 196/2003 (Codice in materia di protezione dei dati personali).

Le principali fattispecie incriminatrici riguardano il trattamento illecito di dati, le falsità nelle dichiarazioni e notificazioni al Garante, le misure di sicurezza, l'inosservanza di provvedimenti del Garante e la violazione di disposizioni volte a tutelare i lavoratori.

La condanna per uno dei **delitti** previsti dal Codice importa la **pubblicazione della sentenza**: si tratta di una pena accessoria.

Il **trattamento illecito di dati** è previsto dall'art. **167** D. Lgs. n. 196/2003, che punisce 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 determinate disposizioni, se dal fatto deriva nocumento o se il fatto consiste nella comunicazione o diffusione.

Per questo delitto è comminata la **reclusione** da sei mesi a tre anni.

Occorre fin da subito precisare che il reato non è integrato se l'utilizzo dei dati avviene per **fini esclusivamente personali**, senza una loro diffusione o destinazione ad una comunicazione sistematica (Cass. pen. n. 29071/2013: fattispecie in cui è stato escluso il reato nei confronti dei delegati alla raccolta delle firme per la presentazione di liste elettorali che avevano formato un elenco di sottoscrittori con firme false, utilizzando nominativi effettivamente esistenti presso l'ufficio anagrafe).

Peraltro, è illecita la **divulgazione per finalità giornalistiche** di dati personali diversi da quelli sensibili e giudiziari senza il consenso dell'interessato, effettuata in violazione dei limiti del diritto di cronaca e della essenzialità dell'informazione ovvero dei principi stabiliti dal codice deontologico adottato dall'ordine professionale, cui deve riconoscersi natura di fonte normativa (Cass. pen. n. 7504/2013). Desta interesse, a tal proposito, una recente pronuncia del Tribunale di Bari (24/3/2015), secondo cui, in materia di diffusione dei dati personali per **finalità giornalistiche**, si configura il reato in presenza di una condotta del prevenuto che, in assenza del consenso dell'interessato, proceda alla pubblicazione, ad esempio, di immagini eccedenti rispetto alla funzione di

divulgazione della notizia seppure di interesse pubblico, così non rispettando il parametro generale della c.d. continenza, intesa nel senso di indispensabile osservanza del limite di contemperamento fra la necessità del diritto di cronaca e la tutela della riservatezza del dato.

Il reato in parola deve essere inteso come **reato proprio**, trattandosi di condotte che si concretizzano in violazioni di obblighi dei quali è destinatario in modo specifico il solo titolare del trattamento e non ogni altro soggetto che si trovi ad avere a che fare con i dati oggetto di trattamento senza essere dotato dei relativi poteri decisionali (Cass. pen. n. 5107/2013).

In relazione al **nocumento**, va osservato che esso non è soltanto quello derivato alla persona fisica o giuridica cui si riferiscono i dati, ma anche quello causato a **soggetti terzi** quale conseguenza dell'illecito trattamento (Cass. pen. n. 7504/2013: nella specie, i congiunti di minore vittima di incidente stradale, la cui fotografia, unitamente ad altri dati identificativi, era stata pubblicata a mezzo stampa). Del resto, l'art. 167 cit. punisce, in generale, chiunque effettui un trattamento illecito di dati personali: a tale fine, i dati personali possono essere anche riferiti a un **soggetto defunto**, non svolgendo la norma predetta alcuna distinzione in merito (Trib. Bologna, 26/2/2013).

In una vicenda nella quale un **dipendente di una banca**, in concorso con un **agente assicurativo**, in occasione della predisposizione di un contratto assicurativo ramo vita, aveva utilizzato illecitamente dati sensibili di due clienti, la Cassazione ha precisato che il concetto di "**nocumento**" è ben più ampio di quello di danno, volendo esso abbracciare qualsiasi effetto pregiudizievole che possa conseguire all'arbitraria condotta invasiva altrui. "Nel richiedere appunto il nocumento, la legge vuole escludere dalla sfera del penalmente rilevante quelle condotte, pure intrusive, che tuttavia siano rimaste del tutto irrilevanti nelle loro conseguenze" (Cass. pen. n. 10485/2015).

Quanto alla **natura giuridica da attribuire alla locuzione nocumento**, ovvero se elemento costitutivo della fattispecie oppure condizione obiettiva di punibilità, appare preferibile la configurazione del nocumento quale condizione obiettiva di punibilità, perché aggrava l'offesa insita nel fatto tipico del reato. Affinché il reato giunga a consumazione, non è d'altronde necessario che l'evento specificamente perseguito dall'autore si realizzi, essendo viceversa sufficiente che dal fatto derivi nocumento (Trib. Firenze, 8/1/2015).

Il delitto si connota come reato a **dolo specifico**, la cui struttura finalistica è incompatibile con la forma del dolo eventuale che postula l'accettazione solo in via

ipotetica, seppure avverabile, del conseguimento di un risultato (Cass. pen. n. 3683/2013: in applicazione del principio, la Corte ha escluso che potesse integrare l'elemento soggettivo del reato la **pubblicazione di un recapito telefonico su una rivista di annunci erotici** da parte di un soggetto che non conosceva il titolare delle utenze e pertanto ignorava se i messaggi erotici, ricevuti a causa dell'indebita divulgazione, gli fossero graditi ovvero costituissero per lui un danno).

Posto che, ai fini del delitto: *a*) il nocumento può sussistere anche quando dal trattamento di dati sensibili derivino, per la persona offesa, effetti pregiudizievoli sotto il profilo **morale**; *b*) il profitto, quale oggetto del dolo specifico richiesto dalla norma incriminatrice, può concretarsi in **qualsiasi soddisfazione o godimento** che l'agente si ripromette di ritrarre, anche non immediatamente dalla propria azione; devono ravvisarsi gli estremi del delitto di trattamento illecito di dati personali nella condotta di chi abbia registrato su un telefono cellulare le immagini di una persona spogliata e in fase delirante e quindi duplicato il filmato su un *computer* (Cass. pen. n. 28280/2013).

Non è poi configurabile il reato di trattamento illecito di dati personali a carico degli amministratori e dei responsabili di una **società fornitrice di servizi di *Internet hosting provider*** che memorizza e rende accessibile a terzi un video contenente dati sensibili (nella specie, un disabile ingiuriato e schernito dai compagni in relazione alle sue condizioni), omettendo di informare l'utente che immette il *file* sul sito dell'obbligo di rispettare la legislazione sul trattamento dei dati personali, qualora il contenuto multimediale sia rimosso immediatamente dopo le segnalazioni di altrui utenti e la richiesta della polizia. In motivazione, la Corte ha evidenziato che l'attività svolta dal *provider*, anche secondo quanto dispone il D. Lgs. n. 70/2003, consiste nell'offrire una piattaforma sulla quale i destinatari del servizio possono liberamente caricare i loro video senza che il gestore abbia alcun potere decisionale sui dati sensibili in essi inclusi e, quindi, possa essere considerato titolare del trattamento degli stessi, finché non abbia l'effettiva conoscenza della loro illiceità, non incombendo a suo carico un obbligo generale di sorveglianza, di ricerca dei contenuti illeciti o di avvertimento della necessità di rispettare la disciplina sulla *privacy* (Cass. pen. n. 5107/2013).

Partendo pertanto dall'assunto che non c'è, nel nostro ordinamento, un dovere di puntuale verifica e controllo da parte dei vertici aziendali dell'*Internet service provider* che diffonde i contenuti video nella rete, non si può tacere che resta da porsi l'interrogativo circa l'opportunità o meno di configurare responsabilità penali, nella prospettiva di un

necessario contemperamento di esigenze contrapposte ma di pari rango costituzionale: da un lato garantire la libertà di espressione e di circolazione di dati e informazioni nel *web*, dell'altro evitare che contenuti lesivi di diritti della persona vengano veicolati in *Internet*.

Se per un verso si ritiene necessario respingere l'imposizione di penetranti obblighi di controllo preventivo in capo all'ISP, che svilirebbero il diritto alla libertà di manifestazione del pensiero e che farebbero assurgere il prestatore di servizi ad improprio strumento di censura per conto dell'ordinamento, per l'altro si ritiene opportuno che dalla particolare posizione assunta dall'ISP derivino peculiari obblighi in merito all'individuazione degli autori del reato e alla eliminazione e/o riduzione delle conseguenze dannose da esso derivanti.

Quanto inoltre allo ***spamming***, si è ravvisato il reato di trattamento illecito di dati personali nell'indebito utilizzo di un ***data-base*** contenente l'elenco di utenti iscritti ad una ***newsletter*** ai quali venivano inviati messaggi pubblicitari non autorizzati provenienti da altro operatore, che traeva profitto dalla percezione di introiti commerciali e pubblicitari, con corrispondente nocumento per l'immagine del titolare della banca dati abusivamente consultata e per gli stessi utenti, costretti a cancellare i messaggi di posta indesiderata, a predisporre accorgimenti per impedire ulteriori invii e a tutelare la *privacy* dalla circolazione non autorizzata delle informazioni personali (Cass. pen. n. 23798/2012).

Infine, resta fermo che la condotta di **utilizzazione di notizie di ufficio che devono rimanere segrete** integra il solo reato previsto dall'art. 326 co. 3 c.p. e non anche quello di trattamento illecito di dati personali previsto dall'art. 167 cit., in quanto quest'ultimo ha ad oggetto il più generale trattamento di dati personali in violazione delle prescrizioni del citato Decreto ed è fattispecie residuale rispetto ad illeciti più gravi per effetto della clausola di riserva contenuta nella disposizione che lo contempla (Cass. pen. n. 9726/2013).

In relazione alle **falsità nelle dichiarazioni e notificazioni al Garante** (art. **168** D. Lgs. n. 196/2003), va ricordato che è punito con la **reclusione** da sei mesi a tre anni chiunque, in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi.

Dal canto suo, l'art. **169** del Codice sanziona con l'**arresto** sino a due anni chiunque, essendovi tenuto, omette di adottare le **misure minime di sicurezza**

(trattandosi di una **contravvenzione**, non si applica la pena accessoria della pubblicazione della sentenza).

All'autore del reato 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.

Infine, circa l'**inosservanza di provvedimenti del Garante**, l'art. **170** del Codice punisce con la **reclusione** da tre mesi a due anni chiunque, essendovi tenuto, non osserva determinati provvedimenti del Garante.

Un discorso a parte merita la norma di cui all'art. **171** D. Lgs. n. 196/2003: "**La violazione delle disposizioni di cui all'articolo 113 e all'articolo 4, primo e secondo comma, della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della legge n. 300 del 1970**" (articolo così sostituito dall'art. 23, comma 2, D. Lgs. 14 settembre 2015, n. 151, a decorrere dal 24 settembre 2015, ai sensi di quanto disposto dall'art. 43, comma 1, del medesimo D. Lgs. n. 151/2015).

L'art. **113** (**raccolta di dati e pertinenza**) stabilisce che resta fermo quanto disposto dall'articolo **8** della legge 20 maggio 1970, n. 300 (**divieto di indagini sulle opinioni**): "è fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore".

Quanto poi all'art. 4 L. n. 300/1970, secondo il **vecchio testo** ("impianti audiovisivi"), "è vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori. Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le

modalità per l'uso di tali impianti. Per gli impianti e le apparecchiature esistenti, che rispondano alle caratteristiche di cui al secondo comma del presente articolo, in mancanza di accordo con le rappresentanze sindacali aziendali o con la commissione interna, l'Ispettorato del lavoro provvede entro un anno dall'entrata in vigore della presente legge, dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti. Contro i provvedimenti dell'Ispettorato del lavoro, di cui ai precedenti secondo e terzo comma, il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art. 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale".

Il **Jobs Act**, e precisamente l'art. 1, co. 7, **L. n. 183/2014** ha delegato il Governo ad adottare uno o più decreti legislativi, di cui uno recante un testo organico semplificato delle discipline delle tipologie contrattuali e dei rapporti di lavoro, nel rispetto di alcuni princìpi e criteri direttivi, in coerenza con la regolazione dell'Unione europea e le convenzioni internazionali: "*f)* revisione della disciplina dei controlli a distanza sugli impianti e sugli strumenti di lavoro, tenendo conto dell'evoluzione tecnologica e contemperando le esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore".

Il nuovo articolo 4 è così formulato: "***Impianti audiovisivi e altri strumenti di controllo.*** - Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero del lavoro e delle politiche sociali.

"**La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.**

"Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196" (articolo così sostituito dall'art. 23, comma 1, D. Lgs. 14 settembre 2015, n. 151, a decorrere dal 24 settembre 2015, ai sensi di quanto disposto dall'art. 43, comma 1, del medesimo D. Lgs. n. 151/2015).

In sostanza, la citata disposizione adegua la normativa contenuta nell'art. 4 – risalente al 1970 – alle innovazioni tecnologiche nel frattempo intervenute.

La norma non "liberalizza", dunque, i controlli ma si limita a fare chiarezza circa il concetto di "strumenti di controllo a distanza" ed i limiti di utilizzabilità dei dati raccolti attraverso questi strumenti, in linea con le indicazioni che il **Garante della *Privacy*** ha fornito negli ultimi anni e, in particolare, con le linee guida del 2007 sull'utilizzo della posta elettronica e di Internet.

Come già la norma originaria, anche questa nuova disposizione prevede che gli strumenti di controllo a distanza, dai quali derivi anche la possibilità di controllo dei lavoratori, possono essere installati:

- esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale;
- ed esclusivamente previo accordo sindacale o, in assenza, previa autorizzazione della Direzione Territoriale del Lavoro o del Ministero.

La modifica all'articolo 4 chiarisce, poi, che non possono essere considerati "strumenti di controllo a distanza" gli strumenti che vengono assegnati al lavoratore "per rendere la prestazione lavorativa" (una volta si sarebbero chiamati gli "attrezzi di lavoro"), come pc, tablet e cellulari.

In tal modo, viene fugato ogni dubbio circa la necessità del previo accordo sindacale anche per la consegna di tali strumenti.

L'espressione "per rendere la prestazione lavorativa" comporta che l'accordo o l'autorizzazione non servono se, e nella misura in cui, lo strumento viene considerato quale mezzo che "serve" al lavoratore per adempiere la prestazione: ciò significa che, nel

momento in cui tale strumento viene modificato (ad esempio, con l'aggiunta di appositi *software* di localizzazione o filtraggio) per controllare il lavoratore, si fuoriesce dall'ambito della disposizione: in tal caso, infatti, da strumento che "serve" al lavoratore per rendere la prestazione il pc, il tablet o il cellulare divengono strumenti che servono al datore per controllarne la prestazione. Con la conseguenza che queste "modifiche" possono avvenire solo alle condizioni ricordate sopra: la ricorrenza di particolari esigenze, l'accordo sindacale o l'autorizzazione.

Perciò, non si autorizza nessun controllo a distanza; piuttosto, si chiariscono solo le modalità per l'utilizzo degli strumenti tecnologici impiegati per la prestazione lavorativa ed i limiti di utilizzabilità dei dati raccolti con questi strumenti.

Il nuovo articolo 4, peraltro, rafforza e tutela ancor meglio rispetto al passato la posizione del lavoratore, imponendo:

- che al lavoratore venga data adeguata informazione circa l'esistenza e le modalità d'uso delle apparecchiature di controllo (anche quelle, dunque, installate con l'accordo sindacale o l'autorizzazione della DTL o del Ministero);
- e, per quanto più specificamente riguarda gli strumenti di lavoro, che venga data al lavoratore adeguata informazione circa le modalità di effettuazione dei controlli, che, comunque, non potranno mai avvenire in contrasto con quanto previsto dal Codice *Privacy*. Qualora il lavoratore non sia adeguatamente informato dell'esistenza e delle modalità d'uso delle apparecchiature di controllo e delle modalità di effettuazione dei controlli, dal nuovo articolo 4 discende che i dati raccolti non sono utilizzabili a nessun fine, nemmeno a fini disciplinari.

A proposito di **impianti audiovisivi**, la giurisprudenza ha recentemente affermato che la creazione, da parte di preposto aziendale e per conto del datore di lavoro, di un falso profilo *Facebook*, al fine di effettuare un controllo sull'attività del lavoratore, già in precedenza allontanatosi dalla postazione lavorativa per parlare al cellulare, **esula dal divieto di cui all'art. 4**, trattandosi di **controllo difensivo**, volto alla tutela dei beni aziendali, insuscettibile di violare gli obblighi di buona fede e correttezza in quanto mera modalità di accertamento dell'illecito comportamento del dipendente (Cass. civ. n. 10955/2015).

Circa, infine, le **sanzioni** di cui all'art. **38** L. n. 300/1970, richiamate dall'art. 171 D. Lgs. n. 196/2003, esse sono l'**ammenda** e l'**arresto** da 15 giorni ad un anno.

Nei casi più gravi le pene dell'arresto e dell'ammenda sono applicate congiuntamente. Quando, per le condizioni economiche del reo, l'ammenda può presumersi inefficace anche se applicata nel massimo, il giudice ha facoltà di aumentarla fino al quintuplo. Nei casi più gravi, l'Autorità Giudiziaria ordina la pubblicazione della sentenza penale di condanna nei modi stabiliti dall'art. 36 c.p.