Diritto e Giustizia
IL QUOTIDIANO DI INFORMAZIONE GIURIDICA

Reati e sanzioni penali privacy nel nuovo Codice della privacy coordinato al GDPR: commentario specifico dei singoli reati privacy. L'articolo 167 e il reato di trattamento illecito di dati

Di Alessandro del Ninno, Professore e Avvocato
Studio Legale Tonucci & Partners

Indice

§ 1. Analisi e commento dell'articolo 167 del Codice della privacy: il reato di trattamento illecito di dati

Il nuovo articolo 167 del Codice della privacy conferma – con talune modifiche di coordinamento – il previgente reato di trattamento illecito di dati personali. Il primo comma prevede l'ipotesi ordinaria di reato (mentre i commi 2 e 3 prevedono ulteriori ipotesi aggravate di reato), disponendo che salvo che il fatto costituisca più grave reato (che dunque assorbirà quello di trattamento illecito dei dati, applicandosi la disciplina del reato assorbente più grave), chiunque, al fine di trarre per sè 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 (i minimi e i massimi edittali della pena sono gli stessi della precedente versione dell'articolo 167, anche se è stata cancellata l'ipotesi di trattamento illecito costituito da comunicazione o diffusione dei dati, prima punita con la reclusione da sei a 24 mesi).

Una considerazione introduttiva sul primo comma può essere svolta con riferimento alla cosiddetta clausola di sussidiarietà espressa "*salvo che il fatto costituisca più grave reato*" che appunto comporta – nella analisi comparativa della gravità tra reati in astratto concorrenti (es: il reato di diffamazione aggravata e il reato di trattamento illecito di dati personali) – l'applicazione della disciplina del reato in concreto più grave. Possiamo appunto riprendere l'esempio di due reati in astratto concorrenti: la diffamazione aggravata on line e la diffusione di dati personali illecita (spesso è attraverso la diffusione di dati e informazioni sulla persona offesa che si determina l'effetto diffamatorio). La Corte di Cassazione ha di recente chiarito (cfr. sentenza 26.9.2017, n. 44390) i criteri con i quali svolgere il giudizio di gravità che determina l'assorbimento del reato di minore gravità in quello di maggiore gravità. Ha precisato la Suprema Corte che seppure un risalente orientamento ha in passato ritenuto che la maggior gravità del reato deve stabilirsi in relazione alla pena edittale detentiva, in particolare avendo riguardo alla pena massima in astratto comminata, oppure - in caso di pari gravità della massima - alla pena minima, tuttavia la valutazione va invece e necessariamente svolta avendo riguardo alla pena in concreto irrogabile, e quindi tenendo anche conto delle circostanze in concreto ritenute e dell'esito dell'eventuale bilanciamento tra esse. Nel caso di specie (in cui un soggetto aveva pubblicato *on line* articoli diffamatori, ricevendone la condanna sia per diffamazione aggravata che per trattamento illecito di dati personali), alla luce delle pene concretamente inflitte, la Corte conclude che il reato di illecito trattamento di dati personali sia assorbito da quello di diffamazione aggravata (infatti, nel caso in esame, per effetto del diniego delle circostanze attenuanti generiche, la diffamazione aggravata è risultata più grave - perchè punita con la pena della reclusione da sei mesi a tre anni o della multa non inferiore ad Euro 516,00 - rispetto al reato di cui all'art. 167, come contestato nella specie (punibile – nella previgente versione dell'art. 167 - con la reclusione pari nel massimo a due anni).

Una seconda considerazione va effettuata sul soggetto autore del reato. Come nella precedente versione del primo comma dell'articolo 167, è autore del reato "*chiunque*" ponga in essere le condotte punibili: dal titolare del trattamento al responsabile del trattamento; dalle persone autorizzate al trattamento ai "*soggetti designati*" ora previsti dall'art. 2-*quaterdecies* del Codice della privacy (cioè le persone fisiche espressamente designate dal titolare o dal responsabile del trattamento, che operano sotto la loro autorità ed a cui vengono attribuiti specifici compiti e funzioni connessi al trattamento di dati personali).

Si modifica invece la persona offesa dal reato: mentre nella precedente versione dell'articolo 167 integrava il reato – oltre al dolo di profitto – anche, e in alternativa, il "*recare ad altri un danno*" (quindi anche a terzi diversi dalla persona fisica cui i dati personali illecitamente trattati si riferivano), nella attuale versione il Legislatore ha specificato in tutte le ipotesi di trattamento illecito che il dolo di danno come elemento soggettivo del reato può riguardare esclusivamente l'interessato (cioè la sola persona fisica cui si riferiscono i dati personali).

§ 2. Elementi oggettivi del reato di trattamento illecito di dati: le condotte punibili al primo comma dell'art. 167 del Codice della privacy

Con riferimento alle condotte punibili, il reato di trattamento illecito di dati personali menzionato al primo comma del nuovo articolo 167 è integrato dalla violazione degli articoli 123, 126, 130 o del provvedimento previsto dall'articolo 129 del Codice della privacy.

Sono cioè punite le condotte:

- che violano la disciplina sui dati relativi al traffico [art. 123; ai sensi del nuovo articolo 121, comma 1- *bis*, lettera (h) del Codice – che riprende le definizioni prima inserite all'articolo 4 - sono «*dati relativi al traffico*» qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione; si pensi ai servizi telefonici e/o telematici voce e dati e al relativo traffico];
- che violano l'articolo 126 [che reca la disciplina sul trattamento dei «*dati relativi all'ubicazione*», cioè ai sensi del nuovo articolo 121, comma 1- *bis*, lettera (i) ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico; si pensi ad *app*, funzioni o servizi di geolocalizzazione e georeferenziazione e ai servizi VAS, a valore aggiunto, pure disciplinati];
- quelle che violano il provvedimento del Garante ai sensi dell'art. 129 del Codice circa le modalità di inserimento e di successivo utilizzo dei dati personali relativi ai *contraenti* [ai sensi del nuovo articolo 121, comma 1- *bis*, lettera (f) è un «*contraente*», qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate] negli elenchi cartacei o elettronici a disposizione del pubblico;
- quelle che violano la disciplina del rilevante articolo 130 del Codice sulle comunicazioni indesiderate (che disciplina il telemarketing in senso lato e si applica anche al trattamento di dati di persone giuridiche in quanto tali, vista la definizione di "contraente" sopra riportata, i cui dati sono tutelati dalla disposizione).

Tuttavia, con la novella dell'articolo 167 la configurabilità delle condotte punibili ha una portata più ampia rispetto alla previgente versione, nel senso che segue. Mentre difatti nella previgente versione del primo comma per aversi punibilità si doveva "*procedere al trattamento di dati personali in violazione di quanto disposto dagli articoli… 123, 126 e 130 ovvero in applicazione dell'articolo 129*", ora è sufficiente che l'autore del reato semplicemente agisca "*operando in violazione di quanto disposto dagli articoli… 123, 126 e 130 o dal provvedimento di cui all'articolo 129*" e cioè sarà punibile anche se non procede ad alcun trattamento di dati. Facciamo alcuni esempi pratici partendo proprio dalla disciplina delle norme di cui agli articoli 123, 126 e 130.

In quali casi potrà dirsi integrato il reato ex art. 167, primo comma, anche se non si procede ad alcun trattamento di dati ma si *opera in violazione* delle prescrizioni contenute negli articoli 123, 126, 129 o 130? Ad esempio nei seguenti casi:

- il fornitore del servizio non informa ai sensi dell'art. 13 o 14 del GDPR il contraente o l'utente sulla natura dei dati relativi al traffico che sono sottoposti a trattamento e sulla durata del medesimo trattamento ai fini di fatturazione o di commercializzazione (in questo caso il fornitore opererebbe in violazione dell'art. 123, comma 4 del Codice, commettendo il reato per la semplice omissione informativa);
- il fornitore del servizio non informa il contraente o l'utente - prima di richiedergli il consenso - sulla natura dei dati relativi alla ubicazione, sugli scopi e sulla durata del trattamento, nonché sull'eventualità che i dati siano trasmessi ad un terzo per la prestazione di un servizio a valore aggiunto (in questo caso il fornitore opererebbe in violazione dell'art. 126, comma 2 del Codice, commettendo il reato per la semplice omissione informativa);
- il fornitore non fornisce un idoneo recapito presso il quale l'interessato possa esercitare i diritti di cui agli articoli da 15 a 22 del GDPR (in questo caso il fornitore opererebbe in violazione dell'art. 130, comma 5 del Codice, commettendo il reato per la semplice omissione informativa).

Come appena visto, in tutti i casi pratici sopra citati il reato sarebbe integrato in assenza di qualsivoglia trattamento specifico, per semplice condotta omissiva dell'aver operato l'autore del reato in violazione delle norme menzionate. Con la conseguenza – cui il Legislatore non ha evidentemente pensato – che il reato non potrebbe definirsi di "*trattamento illecito di dati personali*", visto che vengono semmai incriminate e punite condotte che con il trattamento non hanno nulla a che fare…

§ 2.1 Segue – Gli altri elementi costitutivi del reato di trattamento illecito di dati: inquadramento dei concetti di "danno" e "nocumento"

Tra gli elementi costitutivi del reato di trattamento illecito di dati vi sono sia il dolo e il fine di profitto (per sé o per altri) o di danno che il "nocumento" arrecato all'interessato. Con riferimento al profitto quale oggetto del dolo specifico richiesto dalla norma incriminatrice, esso può concretarsi in qualsiasi soddisfazione o godimento (anche di natura non economica) che l'agente si ripromette di acquisire, anche non immediatamente, dalla propria azione (per esempio, Cass. 07/03/2013, n. 28280 ha ravvisato 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).

Per quanto attiene agli altri elementi costitutivi del reato, poi, la norma cita insieme sia il "danno" che il "nocumento". Va dunque chiarito che cosa sia il "nocumento", che rapporto c'è tra nocumento e danno e se il nocumento sia un elemento costitutivo del reato o una semplice condizione di punibilità. Il delitto di trattamento illecito dei dati personali rientra nella categoria dei reati di danno. Per ritenere integrato il reato è necessario che dalla realizzazione della condotta criminosa derivi un nocumento per la vittima, da intendersi però, a differenza del danno, come qualsiasi effetto pregiudizievole che possa scaturire dall'arbitrario ed illecito comportamento dell'autore dell'azione delittuosa. In altri termini, il "nocumento" è una categoria ben più ampia del "danno", includendo il primo qualsiasi pregiudizio giuridicamente rilevante, di qualsiasi natura, patrimoniale e non (anche di natura morale). Non sono punibili, invece, le condotte che non abbiano determinato alcuna conseguenza (né in termini di nocumento, né di danno).

Cassazione pen. 23/11/2016, n. 15221 ha chiarito che il nocumento per la persona alla quale i dati illecitamente trattati si riferiscono (ora solo l'interessato, non un terzo) costituisce - per la sua omogeneità rispetto all'interesse leso, e la sua diretta derivazione causale dalla condotta tipica - un elemento costitutivo del reato, e non una condizione oggettiva di punibilità; ne consegue che esso deve essere previsto e voluto o comunque accettato dall'agente come conseguenza della propria azione, indipendentemente dal fatto che costituisca o si identifichi con il fine dell'azione stessa.

§ 3. Considerazioni conclusive sul primo comma dell'art. 167: possibili criticità applicative

A conclusione dell'esame del primo comma dell'articolo 167, possono formularsi due considerazioni finali.

La prima è che il Legislatore ha scelto di non riprodurre nella novella le circostanze aggravanti prima contenute al medesimo comma 1 e rappresentate da particolari modalità del trattamento illecito, e cioè dalla "*comunicazione*" o dalla "*diffusione*" illecita dei dati (prima punita con la reclusione da sei a ventiquattro mesi).

Come è noto, il GDPR non contiene - tra le definizioni dell'articolo 4, n. 2) - quelle specifiche di "*comunicazione*" e "*diffusione*" (modalità incluse però nella definizione generale e negli esempi di operazioni di trattamento).

Il nuovo Codice della privacy, invece, mantiene le già note definizioni specifiche riprendendo e aggiornando all'articolo 2-*ter*, comma 4, le definizioni di:

a) "*comunicazione*", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-*quaterdecies*, al trattamento dei dati personali sotto l''autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;

b) "*diffusione*", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Le definizioni di "comunicazione" e "diffusione" costituiscono però il presupposto di un nuovo e specifico reato (oggetto di successivo approfondimento): quello di *comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala*.

La seconda considerazione è relativa a possibili contrasti interpretativi che la formulazione della norma potrebbe determinare. Ora, come è stato già messo in evidenza, il primo comma dell'art. 167 limita al solo interessato la individuazione della persona offesa dal reato. E come è noto, se dobbiamo stare alla formale definizione di "*interessato*", questi è la sola "*persona fisica identificata o identificabile*"[cfr. articolo 4, n. 1) GDPR]. Dunque l'elemento costitutivo del reato sarà costituito dal dolo di danno alla sola persona fisica interessata e dal nocumento arrecato alla sola persona fisica interessata. Non dovrebbe integrare alcuna ipotesi di reato di illecito trattamento – se è vera l'interpretazione formale che precede – se l'autore operando in violazione delle norme citate arreca danno o nocumento a persone giuridiche *contraenti* i cui dati siano oggetto di illecito trattamento; queste difatti non rientrano nella definizione di "interessato",

applicabile alla sola persona fisica. Per uscire dall'*impasse* interpretativo, si dovrebbe ammettere che il Legislatore ha utilizzato il termine "interessato"in senso non tecnico (non facente cioè riferimento formale alla definizione di "interessato" di cui all'art. 4, n. 1 del GSDPR) e dunque applicabile sia a persone fisiche che giuridiche interessate (nel senso di coinvolte) dalla commissione del reato.

§ 4. Il reato aggravato di trattamento illecito di dati: le condotte punibili al secondo comma dell'art. 167 del Codice della privacy

Il secondo comma dell'articolo 167 punisce con la reclusione da uno a tre anni (anche in tale caso il Legislatore ha scelto di riprodurre gli stessi minimi e massimi edittali previgenti) ipotesi di trattamento illecito aventi ad oggetto dati di maggiore delicatezza, e dunque più gravi. Stabilisce la norma che: "*salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sè 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 ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-quinquiesdecies arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni*".

Valgano le considerazioni già svolte sulla clausola di salvaguardia, sull'autore del reato ("*chiunque*"), sul dolo specifico di profitto o danno, sui concetti di "danno" e nocumento" e sul concetto di "interessato", considerazioni tutte applicabili anche all'esame del secondo comma dell'articolo 167 del Codice.

Interessante invece notare come la condotta criminosa - a seconda dei casi – sia duplice: "*procedere al trattamento*" (condotta non specificatamente menzionata al primo comma) od *operare in violazione di determinate norme* (prescindendo – come detto – da un trattamento effettivo).

In particolare si integrerà il reato più grave previsto dal secondo comma dell'art. 167 nel caso in cui l'autore *proceda al trattamento* di dati personali di particolare natura ai sensi dell'art. 9 del GDPR (cioè di dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, oppure di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, di dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona) oppure ove tale autore proceda al trattamento di dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza ai sensi dell'art. 10 GDPR in violazione delle specifiche prescrizioni menzionate, e cioè:

- se il trattamento dei dati di particolare natura ex articolo 9 GDPR avviene in violazione dell'art. 2-*sexies* del Codice privacy (rubricato *Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante)*; l'articolo 2-*sexies* prescrive che i trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del GDPR, necessari per motivi di interesse pubblico rilevante, sono ammessi solo se previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonche' le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. Apparirebbe dunque un reato riferito soprattutto a soggetti/ufficiali pubblici, ma in realtà la lettura coordinata dell'art. 167, comma 2 del

Codice con l'articolo 22, comma 9 del d.lgs. 101/2018 di coordinamento della normativa nazionale al GDPR ("*le disposizioni di legge o di regolamento che individuano il tipo di dati trattabili e le operazioni eseguibili al fine di autorizzare i trattamenti delle pubbliche amministrazioni per motivi di interesse pubblico rilevante trovano applicazione anche per i soggetti privati che trattano i dati per i medesimi motivi*") rende la commissione del reato possibile anche per i titolari del trattamento privati;

- se il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza ai sensi dell'art. 10 GDPR avviene in violazione dell'art. 2-*octies* del Codice privacy (rubricato *Principi relativi al trattamento di dati relativi a condanne penali e reati*); l'articolo 2-*octies* prescrive che il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, del GDPR e che non avviene sotto il controllo dell'autorità pubblica è consentito solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le libertà degli interessati oppure è consentito, in mancanza delle predette disposizioni di legge o di regolamento, in base ad un decreto del Ministro della Giustizia che dovrà essere adottato entro diciotto mesi decorrenti dal 19 Settembre 2018 (cfr. art. 22. Comma 12 del d.lgs. 101/2018) o – infine – è consentito in base a specifici presupposti direttamente individuati dal medesimo articolo, al comma 3, dalle lettere da (a) ad (m);
- se il trattamento dei genetici, biometrici e relativi alla salute avviene in violazione delle misure di garanzia che l'art. 2-*septies* del Codice privacy (rubricato *Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute*) rinvia alla futura adozione da parte del Garante privacy di specifici provvedimenti da adottarsi (a aggiornarsi con cadenza biennale; in particolare il Garante dovrà adottare un provvedimento per le misure di garanzia applicabili al trattamento dei dati genetici, un diverso provvedimento per i dati biometrici ed un terzo per i dati relativi alla salute). Va evidenziato che la violazione delle misure di garanzia contenute in tali futuri provvedimenti del Garante sarà penalmente rilevante anche in caso di violazione dell'art. 2-*sexies* (infatti, l'articolo 2-*sexies*, comma 3 prescrive espressamente che "*per i dati genetici, biometrici e relativi alla salute il trattamento avviene comunque nel rispetto di quanto previsto dall'articolo 2-septies*").

L'articolo 167 comma 2, prevede che sia integrato il reato (più grave) di trattamento illecito di dati anche quando – prescindendo da un trattamento – l'autore "*operi in violazione delle misure adottate ai sensi dell'articolo 2-quinquiesdecies*". Anche in questo caso il reato appare specificatamente riferito all'azione criminosa di soggetti/ufficiali pubblici (o comunque di soggetti anche diversi ma investiti del potere di dare esecuzione a un compito di pubblico interesse), dal momento che l'articolo 2-*quinquiesdecies* (rubricato *Trattamento che presenta rischi elevati per l'esecuzione di un compito di interesse pubblico*) si applica ai trattamenti svolti per l'esecuzione di un compito di interesse pubblico che possono presentare rischi elevati ai sensi dell'articolo 35 del GDPR e implica la violazione (da parte dell'autore che deve eseguire un compito di interesse pubblico) di provvedimenti a carattere generale eventualmente adottati in materia e d'ufficio dal Garante per prescrivere misure e accorgimenti a garanzia dell'interessato.

§ 4.1 Segue – Considerazioni conclusive sul secondo comma dell'art. 167 del Codice della privacy: l'applicabilità delle norme incriminatrici solo a partire dalla emanazione dei futuri provvedimenti oggetto di violazione

L'analisi conclusiva del comma 2 dell'articolo 167 del Codice della privacy non può prescindere da una fondamentale domanda: è corretto ritenere che la contestazione del reato – nelle articolazioni aggravate ivi previste - sarà in alcuni casi menzionati dalla norma possibile solo

quando saranno emanati i provvedimenti citati dalle varie norme (dal decreto del Ministero della Giustizia citato dall'art. 2-*octies*, ai provvedimenti che il Garante dovrà emanare ai sensi dell'art. 2-*septies*, etc) ed oggetto di eventuale violazione penalmente rilevante?

Oppure, dal momento che il d.lgs. 101/2018 (che non bisogna mai dimenticare di leggere e applicare insieme al Codice della privacy, almeno nel lungo periodo transitorio previsto) detta delle norme transitorie e di coordinamento, è possibile contestare violazioni penalmente rilevanti anche in assenza dei provvedimenti citati dal comma 2 dell'art. 167 del Codice?

Ad esempio, l'articolo 22, commi 11 e 12 del d.lgs. 101/2018 dettano le seguenti norme transitorie:

- *"11. le disposizioni del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, relative al trattamento di dati genetici, biometrici o relativi alla salute continuano a trovare applicazione, in quanto compatibili con il Regolamento (UE) 2016/679, sino all'adozione delle corrispondenti misure di garanzia di cui all'articolo 2-septies del citato codice, introdotto dall'articolo 2, comma 1, lett. e) del presente decreto";*
- *"12. Sino alla data di entrata in vigore del decreto del Ministro della giustizia di cui all'articolo 2-octies, commi 2 e 6, del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, da adottarsi entro diciotto mesi dalla data di entrata in vigore del presente decreto, il trattamento dei dati di cui all'articolo 10 del Regolamento (UE) 2016/679 è consentito quando e' effettuato in attuazione di protocolli di intesa per la prevenzione e il contrasto dei fenomeni di criminalità organizzata stipulati con il Ministero dell'interno o con le Prefetture - UTG, previo parere del Garante per la protezione dei dati personali, che specificano la tipologia dei dati trattati e delle operazioni eseguibili".*

A parere di chi scrive, il secondo comma dell'art. 167 sarà applicabile solo ai casi di violazione delle specifiche norme e misure ivi menzionate, e dunque solo a partire dalla emanazione ed applicabilità di decreti, provvedimenti del Garante e delle altre norme ivi citate e ad oggi non in vigore. Non essendo tra l'altro possibile alcuna interpretazione analogica (vietata dal diritto penale) né prescrivendo il d.lgs. 101/2018 in via transitoria alcuna misura penale applicabile prima della emanazione e completa entrata in vigore dei provvedimenti di cui agli articoli 2-*sexies, septies* ed *octies* come richiamati dall'articolo 167, comma 2 del Codice della privacy.

§ 5. Il reato aggravato di trattamento illecito di dati: le condotte punibili al terzo comma dell'art. 167 del Codice della privacy

Il comma 3 dell'articolo 167 punisce con la reclusione da uno a tre anni il trasferimento illecito dei dati personali verso Paesi terzi (extra UE) od organizzazioni internazionali in violazione delle specifiche condizioni di liceità del trasferimento poste agli articoli 45, 46 e 49 del GDPR. Prescrive la norma che "*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 sè 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*".

Valgano le considerazioni già svolte sulla clausola di salvaguardia, sull'autore del reato ("*chiunque*"), sul dolo specifico di profitto o danno, sui concetti di "danno" e nocumento" e sul concetto di "interessato", considerazioni tutte applicabili anche all'esame del terzo comma dell'articolo 167 del Codice.

Le condizioni di liceità del trasferimento di dati personali (ovviamente al di fuori della Unione Europea, visto che non si ha tecnicamente un "trasferimento" se i dati personali circolano all'interno della UE, considerata appunto dal GDPR come mercato e territorio unitario) fissate dagli articoli del GDPR richiamati dal terzo comma dell'art. 167 del Codice sono le seguenti.

In primo luogo, ai sensi dell'art. 45, il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale (definita dall'art. 4, n. 26 del GDPR come "*un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati*") è ammesso in base alla esistenza – per il Paese o l'organizzazione in questione – di una decisione di adeguatezza emanata dalla Commissione UE, la quale ha stabilito che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione dei dati adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche. Ad oggi, le decisioni di adeguatezza (anche in forza della clausola di ultrattività di cui all'art. 45, comma 9 del GDPR) riguardano i seguenti Stati: Andorra, Argentina, Australia – PNR, Canada, Faer Oer, Guernsey, Isola di Man, Israele, Jersey, Nuova Zelanda, Svizzera, Uruguay, USA PNR e Privacy Shield. Trasferire i dati in tali Stati è dunque consentito in base alle relative decisioni di adeguatezza.

In secondo luogo, ai sensi dell'art. 46 del GDPR, in mancanza di una decisione di adeguatezza per il Paese o l'organizzazione in questione, il titolare del trattamento o il responsabile del trattamento possono trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se hanno fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi. Il cosiddetto trasferimento in base a garanzie adeguate può alternativamente basarsi sui seguenti presupposti (e non sono necessarie autorizzazioni specifiche):

1. uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici;
2. le norme vincolanti d'impresa (*binding corporate rules*) in conformità dell'articolo 47;
3. le clausole tipo di protezione dei dati (nell'ambito dei cosiddetti *data transfer agreement*) adottate dalla Commissione UE;
4. le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione (queste clausole contrattuali tipo sono una novità introdotta dal GDPR);
5. un codice di condotta o un meccanismo di certificazione (anche queste sono novità introdotte dal GDPR).

In terzo luogo, ai sensi dell'art. 49 del GDPR, in mancanza di una decisione di adeguatezza o di garanzie adeguate è ammesso il trasferimento o un complesso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale soltanto se si verifica una delle seguenti condizioni:

a) l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate;

b) il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;

c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato;

d) il trasferimento sia necessario per importanti motivi di interesse pubblico;

e) il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;

f) il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

g) il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri.

Se poi non è possibile basare il trasferimento su nessuna delle condizioni stabilite agli articoli 45, 46, 47 o 49 del GDPR, lo stesso art. 49 fissa come condizioni ultimative le seguenti: il trasferimento verso un paese terzo o un'organizzazione internazionale è ammesso soltanto se non è ripetitivo, riguarda un numero limitato di interessati, è necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato, e qualora il titolare e del trattamento abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei dati personali. Il titolare del trattamento in questi casi è obbligato a informare del trasferimento l'autorità di controllo e nella informativa dovrà specificatamente informare l'interessato del trasferimento e degli interessi legittimi cogenti perseguiti.

§ 6. Considerazioni conclusive sul terzo comma dell'art. 167 del Codice della privacy

Dopo aver analizzato le condizioni di liceità del trasferimento internazionale dei dati personali possiamo svolgere alcune considerazioni in merito ai profili penalistici della norma incriminatrice di cui al terzo comma del'art. 167 del Codice della privacy.

In primo luogo, il Legislatore conferma – come nella previgente versione dell'articolo 167 – che la violazione delle norme sul trasferimento dei dati personali rappresenta ipotesi aggravata del reato di trattamento illecito dei dati, confermando altresì la previgente pena aggravata (da uno a tre anni).

In secondo luogo, è interessante notare come la condotta criminosa sia solo quella di "*procedere al trasferimento al di fuori dei casi consentiti dagli articoli 45, 46 e 49*" del GDPR. Non è punita – come nei commi precedenti – la condotta rappresentata dall'*operare in violazione* (prescindendo – come detto – da un trattamento effettivo) degli articoli 45, 46 e 49 del GDPR. Dunque la violazione di talune condizioni pure poste dagli articoli 45, 46 e 49 (ma che prescindono dall'effettivo trasferimento dei dati) non appare essere penalmente rilevante: ad esempio, non

costituirà reato la violazione dell'art. 49, comma 6, del GDPR ("*Il titolare del trattamento o il responsabile del trattamento attesta nel registro di cui all'articolo 30 la valutazione e le garanzie adeguate di cui al paragrafo 1, secondo comma, del presente articolo.*") oppure la mancata informativa sui rischi del trasferimento o sugli interessi legittimi e cogenti del titolare.

§ 7. Le novità procedurali introdotte dai commi 4, 5 e 6 dell'art. 167 del Codice della privacy: i rapporti tra Autorità Garante e Autorità Giudiziaria e le conseguenze degli accertamenti in sede amministrativa e delle indagine penali

Innovative sono le norme procedurali di cui ai commi 4, 5 e 6 dell'articolo 167 del Codice privacy.

In base al comma 4, il Pubblico ministero, quando ha notizia dei reati come articolati – nelle varie ipotesi, anche aggravate, di trattamento illecito - dai commi 1, 2 e 3, ne informa senza ritardo il Garante. Ciò al fine di consentire all'Autorità Garante di esercitare ai sensi dell'art. 166 del Codice il proprio potere di accertamento e sanzione sul piano amministrativo. Non va difatti dimenticato che la violazione delle medesime norme menzionate dall'articolo 167 come presupposto del reato di trattamento illecito è sanzionabile anche in sede amministrativa.

In particolare, è sanzionata fino a 10 milioni di Euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, la violazione:

- dell'articolo 2-*quinquiesdecies* relativo a trattamenti che presentano rischi elevati per l'esecuzione di un compito di interesse pubblico: la norma sanziona la violazione di eventuali provvedimenti di carattere generale adottati d'ufficio dal Garante per prescrivere misure e accorgimenti a garanzia dell'interessato che il titolare del trattamento in questi specifici casi è tenuto ad adottare;
- dell'articolo 123, comma 4 (sulla oscurazione delle ultime tre cifre dei numeri telefonici chiamati nella fatturazione al cliente);
- dell'articolo 129, comma 2 (sulla violazione del divieto di utilizzo – per l'abbonato che non ha dato il preventivo ed esplicito consenso - dei dati tratti dagli elenchi telefonici pubblici per finalità di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale).

E' invece sanzionata fino a 20 milioni di Euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, la violazione:

- dell'articolo 2-*sexies* sul trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante;
- dell'articolo 2-*septies*, comma 7, sull'utilizzo dei dati biometrici con riguardo alle procedure di accesso fisico e logico ai dati da parte dei soggetti autorizzati;
- dell'articolo 2-*ocities* recante i principi relativi al trattamento di dati relativi a condanne penali e reati;
- di quasi tutte le norme del Titolo X sulle Comunicazioni elettroniche (articoli da 121 a 134-*quater*), incluso l'articolo 130, che richiede a tali fini il consenso preventivo sia di persone fisiche che delle persone giuridiche "contraenti";
- delle future regole deontologiche che recheranno ulteriori misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute e per i trattamenti necessari per adempiere un obbligo legale al quale è soggetto il titolare del trattamento o per l'esecuzione di un

compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

* * * * *

Speculare all'obbligo informativo del pubblico ministero è il comma 5 dell'art. 167: 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.

La norma prescrive un obbligo (nuovo) più ampio rispetto all'ordinario obbligo ordinamentale di comunicare una possibile notizia di reato all'Autorità giudiziaria (come già avviene ora quando il Garante ritiene di trasmettere eventuali notizie di reato alla Procura della Repubblica): il Garante – entro il termine delle ordinarie attività ispettive e di accertamento in sede amministrativa di eventuali violazioni al Codice (*rectius*: al GDPR e al Codice, visto che il Legislatore pare esserselo dimenticato) – trasmette (a) tutta la documentazione raccolta e (b) una relazione di accompagnamento su possibili profili penalmente rilevanti, la cui valutazione è demandata al Pubblico Ministero.

L'esame congiunto dei commi 4 e 5 dell'art. 167 - recanti norme prima non previste nella previgente versione dell'articolo – appare rafforzare in senso sostanziale le azioni sanzionatorie in sede sia amministrativa che penale (e la probabilità di comminazione delle relative pene e sanzioni) rispetto a quanto avvenuto fino ad oggi.

* * * * *

Il comma 6 dell'art. 167 del Codice della privacy prevede che quando per lo stesso fatto è stata applicata a norma del 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.

Tale comma 6 è mutuato dall'art. 187-*terdecies* del d.lgs. 58/1998 sugli abusi di mercato: ove vi sia una convergenza sul medesimo fatto di sanzioni pecuniarie (amministrative o disposte dall'autorità giudiziaria quale conseguenza del reato), la pena pecuniaria penale è diminuita (per l'imputato o per la persona giuridica) se il Garante ha già comminato e riscosso per il medesimo fatto la diversa sanzione amministrativa pecuniaria prevista dal Codice o dal GDPR.

Va ricordato, infine, che i meccanismi appena sopra esaminati di cui ai commi 4, 5 e 6 dell'art. 167 del Codice si applicano non solo allo specifico reato di trattamento illecito di dati, ma anche – in forza di quanto previsto agli articoli 167-*bis* e 167-*ter* – ai reati di *comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala* e di *acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala*.