Diritto e Giustizia
IL QUOTIDIANO DI INFORMAZIONE GIURIDICA

Reati e sanzioni penali nel nuovo Codice della privacy coordinato al GDPR: commentario specifico dei singoli reati privacy. L'articolo 167-bis e il (nuovo) reato di comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala

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

Indice

§ 1. Analisi e commento dell'articolo 167-bis del Codice della privacy: il (nuovo) reato di comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala

Rispetto alla previgente versione del Codice della privacy, la fattispecie di reato di *comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala* è di nuova introduzione. Il primo comma dell'art 167-*bis* dispone che 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.

In questo primo caso, la illiceità del trattamento e la rilevanza penale della condotta delittuosa sono legate alla violazione:

(1) della base giuridica prevista per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri;
(2) della disciplina prevista per il lecito trattamento di particolari categorie di dati personali necessario per motivi di interesse pubblico rilevante;
(3) dei principi applicabili al trattamento dei dati relativi a condanne penale e reati.

Il secondo comma dell'articolo 167-*bis* prevede la identica condotta delittuosa come già descritta al primo comma (e la stessa pena da uno a sei anni di reclusione), salvo che la violazione cui sono legate la illiceità del trattamento e la rilevanza penale della condotta delittuosa è rappresentata dalle ipotesi in cui la "comunicazione" o "diffusione" di un "*archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala*" avvengano senza chiedere – ove obbligatorio come base giuridica del trattamento – il preventivo consenso dell'interessato per le specifiche operazioni di comunicazione o diffusione.

Una considerazione introduttiva sui primi due commi dell'articolo 167-*bis* del Codice della privacy 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 – l'applicazione della disciplina del reato in concreto più grave. 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.

Una seconda considerazione va effettuata sul soggetto autore del reato: 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).

Con riferimento alla persona offesa, il reato in esame può interessare (si pensi al dolo di danno) tanto le persone fisiche cui si riferiscono i dati personali trattati su larga scala e contenuti nell'archivio automatizzato oggetto di illecita comunicazione o diffusione, quanto i gestori e/o i titolari dell'archivio in questione: anzi, spesso saranno entrambi e simultaneamente a subire le conseguenze dannose delle condotte delittuose (si pensi agli effetti della comunicazione o diffusione illecita del database dell'Agenzia delle Entrate contenente le dichiarazioni dei redditi dei cittadini persone fisiche o al database aziendale di una multinazionale che contiene i dati sulle retribuzioni dei lavoratori in tutte le sedi mondiali). Si potrebbe anche argomentare che una comunità o la collettività in generale possano subire il danno menzionato dalla norma (che di fatti non parla di "interessato" o di "altri"): si pensi alla comunicazione o diffusione illecite di grandi archivi elettronici pubblici.

Appare inoltre opportuno segnalare tre considerazioni rilevanti nella prospettiva della configurabilità del reato in esame.

La prima considerazione è che per integrare le fattispecie delittuose previste dall'art. 167-*bis* del Codice della privacy è necessario che l'archivio oggetto di illecita comunicazione o diffusione sia "*automatizzato*": in altri termini, non appare rientrare nella ipotesi di reato la comunicazione o diffusione di archivi cartacei o non automatizzati o di parti sostanziali di essi. La difficoltà interpretativa risiede nel fatto che il Legislatore non fornisce una definizione di "archivio automatizzato" (mentre, come più oltre si dirà, il Regolamento 679/2016 contiene la definizione di "archivio").

La seconda considerazione rilevante nella prospettiva della configurabilità del reato in esame è che si tratti di un archivio automatizzato che contiene "dati personali" oggetto di trattamento su larga scala: dunque esclusivamente informazioni riguardanti persone fisiche identificate o identificabili. In altri termini, non appare rientrare nella ipotesi di reato la comunicazione o diffusione di archivi automatizzati (o parti sostanziali di essi) che contengono ad esempio informazioni (pur trattate su larga scala) che non costituiscono dati personali (es: archivi di informazioni puramente aziendali, oppure archivi di "*contraenti*" persone giuridiche ai sensi dell'art. 121, comma 1-*bis*, lettera (f) del Codice della privacy, oppure archivi che contengono "*dati non personali*", così come definiti all'art. 3 della proposta di Regolamento europeo sulla libera circolazione di dati non personali, e cioè "*i dati diversi dai dati personali ai sensi dell'articolo 4, paragrafo 1, del regolamento (UE) 2016/679*", etc).

La terza considerazione rilevante nella prospettiva della configurabilità del reato in esame è che si tratti di un archivio automatizzato ove il trattamento dei dati delle persone fisiche avvenga su "larga scala": in caso contrario, la comunicazione o la diffusione di un

archivio automatizzato di dimensioni limitate contenente dati di persone fisiche trattati non su larga scala, non integrerebbe lo specifico reato di cui all'art. 167-*bis*, salvo verificare se non vi siano profili di illiceità penale in base ad altre disposizioni di legge. Non parrebbe nel caso neanche applicabile l'articolo 167 e il reato di trattamento illecito di dati, stante la specificità delle condotte ivi punite.

Infine, anche per quanto appena sopra specificato, va rilevato come il reato di cui all'art. 167-*bis* del Codice privacy abbia un campo di applicazione limitato (anche perché il Legislatore ha riformulato l'ipotesi di reato in senso più restrittivo persino rispetto al più generico reato di "*comunicazione e diffusione illecita di dati personali riferibili a un rilevante numero di persone*" originariamente previsto nello schema di decreto). E' difatti integrata la fattispecie solo qualora la diffusione o comunicazione avvenga in violazione di specifiche e limitate disposizioni del Codice della privacy per lo più applicabili a soggetti che trattano dati professionalmente o per obbligo di legge nell'ambito di archivi di notevoli dimensioni.

§ 2. Elementi oggettivi del reato: le condotte punibili ai sensi dell'art. 167-bis del Codice della privacy. Le definizioni di "archivio", "comunicazione", "diffusione" e di "trattamento su larga scala"

Le condotte punibili sono rappresentate – in entrambe le ipotesi di cui al primo e al secondo comma dell'art. 167-bis – dall'avere il soggetto agente autore del reato proceduto alla "comunicazione" oppure alla "diffusione" di un "archivio" automatizzato o parte sostanziale di esso contenente dati personali oggetto di trattamento su "*larga scala*".

La definizione di "*archivio*" cui fare necessariamente riferimento è quella contenuta all'articolo 4, n. 6) del Regolamento Generale UE 679/2016 ("GDPR"): "*qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico*". Tale definizione - anche se include sia gli archivi "automatizzati" che quelli cartacei e "manuali" - evidenzia tuttavia al tempo stesso i fondamentali elementi costitutivi senza i quali un "*archivio*" non può dirsi tale ed esistente, e cioè: (1) la presenza di un insieme strutturato di dati personali secondo criteri specifici; e (2) la possibilità di accedere a tale insieme secondo criteri di consultazione e di accesso (pre)determinati. Ciò è confermato anche dal alcuni Considerando del GDPR: ad esempio, il Considerando n. 15 ricorda che non rientrano nell'ambito di applicazione del regolamento "*i fascicoli o le serie di fascicoli non strutturati secondo criteri specifici*" (si ricordi anche, ai sensi dell'articolo 2 GDPR sull'ambito di applicazione materiale, che il trattamento manuale o cartaceo è soggetto al GDPR non in quanto tale, ma solo se il trattamento non automatizzato riguarda "*dati personali contenuti in un archivio o destinati a figurarvi*").

Se dunque un archivio è una raccolta sistematica e organizzata di atti, dati e documenti, strutturata in base a specifici criteri ed accessibile o consultabile secondo criteri predeterminati, è ovvio che un "*archivio automatizzato*" (di cui non esiste una specifica

definizione, né nel Codice della privacy né all'interno del GDPR, che cita gli "*archivi automatizzati*" una sola volta, al Considerando n. 67 in tema di diritto alla limitazione del trattamento) sarà tale in quanto i suoi creatori abbiano affidato a soluzioni automatiche e tecnologiche esattamente la *strutturazione* delle informazioni e i *criteri* di accesso ai dati e di consultazione delle informazioni strutturate. In assenza di una specifica definizione normativa di "*archivio automatizzato*", può venire in soccorso – per comprendere cosa esso sia – la definizione di "banca dati"(elettronica) contenuta all'articolo 2, n. 9 della Legge sul diritto d'autore n. 633/1941: "*raccolta di dati o di altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici*". Di talchè, ad esempio, non sarebbe un "archivio" automatizzato rilevante ai fini del reato di cui all'art. 167-*bis* del Codice della privacy una cartella elettronica salvata su un PC contenente *files* non strutturati né indicizzati, oppure una chiavetta USB che – come un "contenitore" - conserva informazioni non strutturate (documenti Office, file audio, video, immagini), etc. E ciò anche se fossimo in presenza di trattamento su larga scala di dati relativi a persone fisiche (d'altra parte, anche la mera "*conservazione*" è una operazione di "*trattamento*" rilevante ai sensi dell'art. 4, n. 2 del GDPR).

Chiarito che oggetto della condotta di reato è un "archivio" automatizzato con le specifiche caratteristiche sopra evidenziate, con riferimento alle precise condotte illecite, queste consistono nella "comunicazione" o nella diffusione" di tale "archivio" automatizzato (o di una parte sostanziale di esso). Il che ci porta immediatamente ad una criticità interpretativa: il reato consiste nella "comunicazione" o nella diffusione" di un archivio automatizzato (o di una parte sostanziale di esso) in quanto tale, e non anche dei dati personali che da esso siano stati eventualmente estratti e successivamente comunicati o diffusi. A meno di non propendere per una sorta di sciatteria linguistico-redazionale del Legislatore (si comunicano o diffondono "dati" più che "archivi"), deve ritenersi che con il riferimento specifico ad un "archivio" si sia voluta punire sul piano penale la illecita comunicazione o diffusione di insiemi strutturati di dati personali (ad esempio illecitamente copiati) che all'atto della comunicazione o diffusione continuano ad essere sia strutturati che accessibili e consultabili secondo criteri specifici (continuando ad essere – dunque – un "archivio"). Al contrario, deve ritenersi che se il soggetto agente estrae da un archivio anche una considerevole mole di dati e informazioni riferite a persone fisiche, ma all'atto della comunicazione o diffusione tali dati hanno perso la loro strutturazione come insieme o la loro consultabilità secondo criteri specifici, allora non sarà più contestabile lo specifico reato di cui all'art. 167-*bis* del Codice della privacy, poiché non si avrà più un "archivio", salvo ovviamente verificare l'applicabilità di altre ipotesi di reato previste dall'ordinamento. E ciò anche se la rubrica dell'articolo 167-bis è "*Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala*": la norma incriminatrice, difatti, specifica che l'oggetto della condotta può essere solo un "*archivio automatizzato o una parte sostanziale di esso*". D'altra parte, la stessa attività di *estrazione* dei dati da un archivio trova una precisa definizione giuridica nell'ordinamento: può farsi difatti riferimento all'art. 102-*bis*, comma 1 della legge sul diritto d'autore n. 633/1941, qui richiamato analogicamente, a mente del quale l'*estrazione* è "*il trasferimento permanente o temporaneo della totalità o di una parte*

sostanziale del contenuto di una banca di dati su un altro supporto con qualsiasi mezzo o in qualsivoglia forma". Si distingue difatti il "contenuto (dati) dal contenente (banca dati-archivio). Dunque nella ipotesi di estrazione di dati da un archivio automatizzato ai fini della successiva comunicazione o diffusione non si avrebbe ad oggetto della condotta un "archivio", ma il contenuto (eventualmente anche non strutturato) di esso, cioè i dati, e dunque non dovrebbe ritenersi integrata la specifica fattispecie di reato di cui all'art. 167-*bis* del Codice della privacy, anche per il divieto di applicazione analogica *in malam partem* nel diritto penale.

Quanto alla condotta di "*comunicazione*" o "*diffusione*", tali operazioni specifiche di trattamento sono definite dall'art. 2-*ter*, comma 4, del Codice della privacy che riprende le identiche e previgenti definizioni già incluse nel Codice (mentre corrispondenti definizioni sono del tutto assenti nel GDPR). Si intende per:

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.

Dunque si avrà una tecnicamente una "comunicazione" ogni qual volta si ottiene l'effetto di "*dare conoscenza*" dei dati personali ad uno o più soggetti "*determinati*" (cioè il destinatario deve essere individuato o individuabile con precisione) ed esterni al contesto e alle informazioni e dati oggetto della comunicazione (difatti non è considerata tecnicamente una "comunicazione" la messa a disposizione e la conoscenza proprio ad opera dei soggetti elencati che logicamente si presume già conoscano i dati). Inoltre, la definizione è talmente ampia da includere qualsiasi modalità di azione o trattamento ("*qualunque forma*") con cui si mette in condizione il destinatario - esterno e determinato - di avere effettiva conoscenza dei dati comunicati. L'elenco di modalità pratiche con cui si dà conoscenza dei dati (messa a disposizione dei dati, consultazione, interconnessione) è meramente esemplificativo e non tassativo.

L'ufficio risorse umane di un'azienda che comunica i dati personali di un proprio lavoratore ai familiari di questi, compie una "comunicazione", così come un Istituto scolastico che mette a disposizione dei genitori degli studenti i loro dati personali mediante consultazione tramite *app* del registro elettronico.

Va inoltre evidenziato che nonostante l'idea di *comunicazione* possa - *prima facie* - fare concettualmente riferimento ad una idea di trasferimento proattivo dell'oggetto della comunicazione da chi comunica a chi riceve, in realtà, per aversi tecnicamente una "comunicazione", non è affatto necessario che vi sia anche un trasferimento dei dati o delle

informazioni: la norma evidenzia difatti che è fondamentale il "*dare conoscenza*" dei dati, anche se ciò avviene "*mediante la loro messa a disposizione, consultazione o mediante interconnessione*". Di conseguenza, si avrà tecnicamente una "comunicazione" di dati se – ad esempio – si forniscono a un destinatario esterno le credenziali di autenticazione per accedere ad un archivio elettronico, oppure se una azienda parte di un Gruppo costituisce un proprio archivio aziendale aperto alla consultazione condivisa da parte delle altre società della Holding, che possono semplicemente accedervi.

Con riferimento alla definizione dello specifico trattamento rappresentato dalla *diffusione*, valgono le identiche considerazioni appena sopra svolte sul trattamento rappresentato dalla *comunicazione*: l'unica differenza è rappresentata dai destinatari, che in caso di diffusione non sono né determinati, né individuabili: è il caso, ad esempio, della pubblicazione su Internet di dati (accessibili globalmente da una sconfinata platea di potenziali destinatari) o della affissione in bacheche (aziendali scolastiche, condominiali, etc) di documenti contenenti dati personali (e come tali accessibili da indeterminati soggetti che passino di fronte alle bacheche).

Quanto alla definizione di "*trattamento su larga scala*", essa non si rinviene né nel Codice della privacy, né nel GDPR, nonostante in quest'ultimo – al Considerando numero 91 – vi sia una sorta di definizione: "*trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati*". E' in ogni caso nelle *Linee Guida WP 243 sui Responsabili della Protezione dei dati personali* che è possibile rinvenire approfonditi chiarimenti interpretativi dei Garanti UE su cosa debba intendersi per *trattamento dei dati personali su larga scala*. Anche se in realtà i Garanti UE riconoscono che è impossibile precisare la quantità di dati oggetto di trattamento o il numero di interessati in modo da coprire tutte le eventualità, ciò non significa che sia impossibile individuare alcuni standard utili a specificare in termini più specifici e/o quantitativi cosa debba intendersi per "larga scala" con riguardo ad alcune tipologie di trattamento magiormente comuni, tenendo conto, in particolare, dei seguenti fattori:

1. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
2. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
3. la durata, ovvero la persistenza, dell'attività di trattamento;
4. la portata geografica dell'attività di trattamento.

Alcuni esempi di trattamento su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
- trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);
- trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di fast food;

- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;
- trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;
- trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

Alcuni esempi di trattamento non su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;
- trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

Si può dunque in conclusione affermare che integrano il reato di cui all'art. 167-*bis* del Codice della privacy le attività - al fine di trarre profitto per sé o per altri ovvero al fine di arrecare un danno - di illecita messa a disposizione in qualunque forma e modo di destinatari esterni determinati ("comunicazione") o non individuabili ("diffusione") di un archivio automatizzato (o di una parte sostanziale di esso) inteso come insieme strutturato di una notevole quantità di dati personali (per numero di interessati, volume e tipologia di dati, durata e riferimento geografico del trattamento a livello regionale, nazionale o sovranazionale) accessibili secondo criteri determinati.

E' infine interessante notare che l'articolo 167-*bis* del Codice della privacy non fa alcuna menzione – come il precedente articolo 167 in caso di reato di trattamento illecito di dati – dell'effetto delle sopra citate condotte di "*arrecare nocumento all'interessato*". Tra gli elementi costitutivi del reato di comunicazione o diffusione illecita di dati personali di dati vi sono solo il dolo e il fine di profitto (per sé o per altri) o di danno, ma non anche il "nocumento" arrecato all'interessato (che la Cassazione ha qualificato come elemento costitutivo del reato di illecito trattamento di dati). Dunque sarà integrata la fattispecie delittuosa di cui all'art. 167-*bis* del Codice della privacy anche se la illecite attività di comunicazione o diffusione di un archivio automatizzato non determinino un "nocumento" da intendersi, 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).

§ 3. Le condotte punibili menzionate dal primo comma dell'art. 167-bis del Codice della privacy

Il primo comma dell'art. 167-*bis* del Codice della privacy punisce con la reclusione da uno a sei anni, salvo che il fatto costituisca più grave reato, chiunque comunica o diffonde al fine di trarre profitto per sè 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*.

Il primo comma attribuisce la illiceità del trattamento e la rilevanza penale della condotta delittuosa alla violazione degli articoli 2-*ter*, 2-*sexies* e 2-*octies*.

L'articolo 2-*ter* del Codice della privacy, rubricato *Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri* specifica quanto previsto dall'articolo 6, comma 3, del GDPR che prescrive che laddove la base giuridica su cui si fonda il trattamento sia rappresentata dalla necessità di adempiere ad un obbligo legale al quale è soggetto il titolare del trattamento o dalla necessità di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, allora, in tali casi, è lo Stato Membro cui è soggetto il titolare del trattamento a stabilire la specifica base giuridica del trattamento nei casi menzionati.

Quindi l'articolo 2-*ter* del Codice della privacy dispone che la base giuridica del trattamento in tali casi è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento, le uniche fonti che dunque possono specificare l'obbligo legale o il compito di interesse pubblico o connesso all'esercizio di pubblici poteri cui il titolare del trattamento deve adempiere.

La stessa norma – al comma 3 – prescrive chiaramente che la diffusione e la comunicazione di dati personali trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti (sia pubblici che privati, non operando la norma nessun a distinzione) che intendono trattarli per altre finalità sono ammesse unicamente se previste da una norma di legge o, nei casi previsti dalla legge, di regolamento. In tutti gli altri casi di comunicazione e diffusione dei dati non specificatamente prevista da una legge o da un regolamento, si integrerà la fattispecie di cui all'art. 167-*bis* del Codice? Ad avviso di chi scrive, la risposta è negativa: la violazione si verificherà solo se la comunicazione o diffusione hanno ad oggetto dati che possano costituire un "archivio automatizzato" (o una parte sostanziale di esso) e se il trattamento è su larga scala. Nei casi diversi, ci si dovrebbe attenere strettamente ai confini ed ai limiti fissati dal Legislatore (con tecnica redazionale che crea non poche difficoltà interpretative e applicative) nella norma incriminatrice e dunque non troverebbe applicazione l'articolo 167-*bis* del Codice.

L'articolo 2-*ter*, comma 2 del Codice della privacy (che contiene anche le definizioni giuridiche di "*comunicazione*" e "*diffusione*") dispone poi che la comunicazione fra titolari che effettuano trattamenti di dati personali comuni (dunque non di particolare natura o relativi a condanne penali e reati, ai sensi degli articoli 9 e 10 del GDPR) per l'esecuzione di un

compito di interesse pubblico o connesso all'esercizio di pubblici poteri è ammessa se prevista se prevista da una norma di legge o, nei casi previsti dalla legge, di regolamento. In mancanza di tale norma, la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di quarantacinque giorni dalla relativa comunicazione al Garante, senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati. La norma disciplina la comunicazione di dati personali comuni tra soggetti pubblici (es: tra pubbliche amministrazioni), prevedendo come base giuridica del trattamento rappresentato dalla comunicazione dei dati ordinari o la norma di legge (o di regolamento, se previsto) oppure – in assenza di tale norma (e ciò appare in palese conflitto con il primo comma dell'art. 2-*ter* che individua in via generale come base giuridica "*esclusivamente*" la norma di legge o di regolamento…) - sia il perseguimento delle finalità istituzionali che lo svolgimento di compiti di interesse pubblico da parte del Titolare (evidentemente pubblico), che comunque potrà effettuare la comunicazione solo se avrà richiesto l'autorizzazione al Garante e l'Autorità – con meccanismo di silenzio-assenso – non abbia risposto nei successivi 45 giorni decorrenti dalla richiesta di autorizzazione.

Ancora una volta, deve ritenersi che la violazione di questa specifica disposizione di cui al comma 2 non determini automaticamente la commissione del reato ex art. 167-*bis* del Codice. Anzi, è una fattispecie diversa che può assumere rilevanza nell'ottica incriminatrice solo se – ancora una volta - la comunicazione o diffusione abbiano ad oggetto dati che possano costituire un "archivio automatizzato" (o una parte sostanziale di esso) e se il trattamento sia su larga scala. In un'ottica diversa, non troverebbe applicazione l'articolo 167-*bis* ove un soggetto pubblico abbia comunicato ad un altro soggetto pubblico dati (non su larga scala e non strutturati) senza richiedere l'autorizzazione al Garante in caso di assenza di una norma di legge o senza attendere il termine dei 45 giorni previsto per la risposta eventuale del Garante. Ed ovviamente, non vi sarebbe il reato specifico se la comunicazione o la diffusione non hanno ad oggetto un vero e proprio "archivio" automatizzato strutturato.

Il primo comma dell'art. 167-*bis* del Codice della privacy collega poi la illiceità del trattamento e la rilevanza penale della condotta delittuosa alla violazione dell'articolo 2-*sexies*. Tale articolo, rubricato *Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante* specifica quanto previsto dall'articolo 9, comma 2, del GDPR che prescrive che si possa derogare al divieto (che è regola generale fissata all'art. 9, primo comma) di trattamento dei dati di particolare natura (cioè i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona) laddove – tra gli altri casi elencati - *" 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"*.

Prescrive dunque la norma nazionale che i relativi trattamenti dei dati di particolare natura necessari per motivi di interesse pubblico sono ammessi qualora siano 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, nonchè' le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Anche in tale caso dobbiamo riferirci a titolari del trattamento pubblici, i quali dovranno individuare – prima di procedere al trattamento dei dati di particolare natura sopra elencati – le specifiche norme di legge o eventualmente di regolamento che specifichino esattamente: (1) i tipi di dati che possono essere trattati (es: quelli sindacali ma non anche quelli sanitari), le operazioni di trattamento eseguibili (es: sola conservazione dei dati con divieto di comunicazione); (3) il motivo di interesse pubblico rilevante (es: stabilire se una certa categoria di cittadini che versa in condizioni sanitarie particolari abbia o meno il diritto di accedere ad agevolazioni fiscali), nonché (4) le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. Se esistessero tali normative così specifiche, significherebbe avere un Legislatore dalla elevata e sopraffina tecnica redazionale delle norme dell'ordinamento, che dovrebbero essere scritte (quando in realtà non lo sono affatto) con logica, dettaglio della fattispecie, precisione, etc….

Il Codice della privacy individua a monte e in via generale solo il terzo elemento, e cioè *il rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri:* difatti l'articolo 2-*sexies*, comma 2, elenca una lunghissima lista di materie e settori dove a monte è individuato *ex lege* il motivo di rilevante interesse pubblico.

Ma per quanto riguarda gli altri elementi, *quid* ove non esista una norma di legge o di regolamento? Il soggetto pubblico non potrà procedere al trattamento dei dati di particolare natura? Effettivamente, con l'abrogazione dell'articolo 20, comma 2 del Codice (che prevedeva in questi casi che fossero gli stessi soggetti pubblici ad emanare e rendere pubblico un proprio *Regolamento sul trattamento dei dati sensibili e giudizia*ri che identificasse, in assenza di una norma di legge o di regolamento specifiche, i tipi di dati che trattati, le operazioni di trattamento eseguibili e le misure appropriate di tutela), l'attuale formulazione dell'art. 2-sexies appare in tal senso preclusiva. Tuttavia, per lo meno per quanto riguarda i dati genetici, i dati biometrici e i dati relativi alla salute (in base alla specifica previsione dell'articolo 9, comma 4 del GDPR) potranno essere le regole deontologiche del Garante – che saranno emanate ai sensi dell'art. 2-*quater*, primo comma, del Codice della privacy – a colmare le lacune (e l'assenza dei Regolamenti dei soggetti pubblici, ora non più previsti) e a prevedere gli elementi in base ai quali consentire anche ai soggetti pubblici il trattamento dei dati di particolare natura. Inoltre, sempre per quanto riguarda il trattamento dei dati genetici, biometrici e relativi alla salute, non va dimenticato che l'ultimo comma dell'articolo 2-*sexies* prescrive che "*il trattamento avviene comunque nel rispetto di quanto previsto dall'articolo 2-septies*": dunque anche nel pieno rispetto dei

singoli e specifici Provvedimenti di garanzia che in base a tale norma il Garante dovrà emanare (in aggiunta alle regole deontologiche) con cadenza biennale.

Anche nelle ipotesi di cui all'articolo 2-*sexies* è comunque difficile effettuare un immediato raccordo con le ipotesi incriminatrici dell'art. 167-*bis* del Codice della privacy: dovremmo in ogni case ipotizzare violazioni (abbastanza teoriche) da parte di soggetti pubblici o funzionari dello Stato i quali comunicano o diffondono archivi automatizzati (o parti rilevanti di essi) ove si svolgono trattamenti di dati personali su larga scala, e in violazione (o anche in semplice assenza) di specifiche norme di legge o di regolamento che prevedano la comunicazione o la diffusione o in violazione di future regole deontologiche o dei provvedimenti di garanzia del Garante.

Infine, il primo comma dell'art. 167-*bis* del Codice della privacy collega la illiceità del trattamento e la rilevanza penale della condotta delittuosa alla violazione dell'articolo 2-*octies*. Tale articolo, rubricato *Principi relativi al trattamento di dati relativi a condanne penali e reati* prescrive che il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza 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. In mancanza delle disposizioni di legge o di regolamento, i trattamenti dei dati e le garanzie per i diritti e le libertà degli interessati sono individuati con decreto del Ministro della giustizia (che sarà emanato entro diciotto mesi decorrenti dalla data del 19 Settembre 2018). Tuttavia il comma 3 dell'articolo in esame contiene una sorta di elenco di trattamenti di dati relativi a condanne penali e a reati che rinvia a specifiche disposizioni settoriali che li autorizzano, anche se il successivo comma 4 rinvia sempre al Decreto del Ministro della Giustizia l'individuazione delle specifiche misure di garanzia per i diritti e le libertà degli interessati, se non previste da quelle disposizioni.

L'articolo 2-*octies* si applica solo ai soggetti privati (in ciò va letto il riferimento al *trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza* che non avviene sotto il controllo dell'autorità pubblica) ed è speculare all'articolo 2-sexies. Tanto è vero che il comma 5 prevede che quando il trattamento dei dati relativi a condanne penali e a reati o a connesse misure di sicurezza avviene invece sotto il controllo dell'autorità pubblica, si applicheranno le disposizioni previste dall'articolo 2-*sexies* (per i soggetti pubblici).

Dal punto di vista della configurabilità del reato ex articolo 167-*bis* del Codice, è ovvio che il riferimento alla violazione dell'articolo 2-*octies* (che si applica anche ai privati) rende meno teorica la possibilità del reato (rispetto alla attività di soli soggetti pubblici): si pensi ad una azienda attiva nel settore dell'autonoleggio che tratti su larga scala in un proprio archivio automatizzato (autorizzato per propri fini antifrode) i dati personali di clienti denunciati per frode o appropriazione indebita o furto di veicoli. Se, ad esempio, tale azienda mettesse in condivisione con altre aziende del settore l'archivio o parte sostanziale di esso in assenza di specifiche previsioni di legge, o in contrasto con quanto previsto dal (futuro) decreto

del Ministro della Giustizia, ecco che sarebbe configurabile il reato di comunicazione illecita ex art. 167-*bis*.

§ 4. Le condotte punibili menzionate dal secondo comma dell'art. 167-bis del Codice della privacy

Il secondo comma dell'articolo 167-*bis* del Codice della privacy prevede che salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sè o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, è punito con la reclusione da uno a sei anni, quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione.

E' evidente che tale comma sia speculare al primo: mentre nella disposizione del primo comma il reato è legato alla violazione delle specifiche norme ivi richiamate che costituiscono ai sensi del GDPR le basi giuridiche del trattamento svolto da soggetti pubblici, nella disposizione di cui al secondo comma, il reato è legato alla violazione della specifica base giuridica del trattamento rappresentata dal consenso dell'interessato, che fonda principalmente trattamenti di dati effettuati da titolari privati.

Ed in tale prospettiva viene immediatamente in considerazione la costituzione di grandi database clienti da parte di aziende o di archivi strutturati (es: mailing list, recapiti, indirizzari, profili, etc) ove è svolto su larga scala il trattamento di dati personali che possono essere messi in vendita da società specializzate e utilizzati da aziende acquirenti a scopi di marketing. O, ancora, vengono in considerazione specifici archivi strutturati che profilano persone fisiche (es: database sulla affidabilità, sistemi di *scoring*, etc). In tale prospettiva va ricordato che il trattamento dei dati personali degli interessati a scopi di marketing o di profilazione (come anche ricordano le *Linee Guida dei Garanti UE WP 251 sulla profilazione e sulle decisioni automatizzate*) e al di là di quanto anche previsto dal Considerando n. 47 del GDPR (che pure apre scenari di trattamenti marketing basati sulla diversa base giuridica dell'interesse legittimo del titolare del trattamento) va nella quasi totalità dei casi fondato su specifici e granulari consensi informati. Anzi, il titolare del trattamento dovrà procedere ad acquisire un consenso specifico per ciascuna distinta finalità quali ad esempio: marketing, profilazione, comunicazione a terzi dei dati.

Nella costituzione di archivi elettronici poi oggetto di comunicazione a terzi devono essere documentabili tutti gli specifici consensi, ivi incluso quello distinto alla comunicazione dei dati a terzi, per non incorrere appunto nel reato di comunicazione illecita ai sensi dell'art. 167-*bis*, comma secondo, del Codice.

In assenza della possibilità di documentare tali consensi (con particolare riferimento al consenso specifico alla comunicazione dei dati a terzi), configureranno il reato in esame – ad esempio – le seguenti ipotesi di comunicazione (in assenza di consenso) di archivi automatizzati:

1. vendita da parte di una società specializzata ad aziende acquirenti di un archivio elettronico strutturato contenente un elevato volume di *records* (larga scala) di

potenziali clienti persone fisiche che l'azienda acquirente intende utilizzare a scopi di marketing;

2. costituzione da parte di una società di un gruppo multinazionale di un archivio elettronico strutturato contenente un elevato volume di *records* (larga scala) di profili dei propri clienti (strutturati in base alle abitudini di consumo rispetto ai prodotti e servizi specifici offerti da tale azienda) che venga messo in condivisione con tutte le altre società del medesimo gruppo comunque interessate a scopi di proprie strategie commerciali a visionare i profili.

Si può anche affermare che il reato di comunicazione o diffusione illecita di un archivio automatizzato contenente dati personali oggetto di trattamento su larga scala in assenza del consenso dell'interessato quando detto consenso è necessario sia l'unica ipotesi in cui tale reato può concorrere con quello ex art. 167 di trattamento illecito: si pensi alla violazione dell'obbligo di consenso preventivo dell'interessato (*opt-in)* ai sensi dell'art. 130, primo e secondo comma del Codice (ipotesi di trattamento illecito sanzionata penalmente dall'art. 167, prima comma).

§ 5. Il comma 3 dell'art. 167-bis del Codice della privacy: i rapporti tra Autorità Garante e Autorità Giudiziaria e le conseguenze degli accertamenti in sede amministrativa e delle indagine penali

Il comma 3 dell'articolo 167-*bis* del Codice della privacy richiama l'applicabilità delle medesime norme procedurali di cui all'articolo 167, commi 4, 5 e 6.

Il pubblico ministero, quando ha notizia del reato di comunicazione o diffusione illecita di archivi automatizzati, 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-*bis* come presupposto del reato di comunicazione o diffusione illecita di archivi contenenti dati personali trattati su larga scala è sanzionabile anche in sede amministrativa.

In particolare, è 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;
- 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 quello del Garante, il 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 delle disposizioni che precedono – assenti nelle precedenti versioni del Codice della privacy – 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.

Infine, anche al caso di comunicazione o diffusione illecita di dati personali oggetto di trattamento su larga scala troverà la regola in base alla quale quando per lo stesso fatto è stata applicata a norma del Codice o del GDPR a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita.

Tale norma è mutuata 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.