Nuovo schema di decreto Gdpr, che cambia: soggetti designati, poteri del Garante, sanzioni

Il nuovo testo dello schema di decreto legislativo delegato che dovrà adeguare l'ordinamento italiano al GDPR stravolge il testo precedentemente circolato e regola ampiamente tutti gli ambiti in cui il legislatore nazionale avrebbe potuto intervenire sulla base del Regolamento. Ne facciamo una sintetica ricostruzione.

La Commissione speciale della Camera dei deputati ha iniziato da poco le sessioni per arrivare all'ormai famoso (fantomatico) decreto Gdpr. Per la precisione, dovranno adesso emettere il parere sullo schema di decreto legislativo delegato che dovrà adeguare l'ordinamento italiano al Regolamento (UE) n. 679/2016, meglio noto come **GDPR.**

È necessario ricordare che l'articolo 13 della legge n. 163 del 2017, delegava il Governo ad adottare, entro sei mesi dalla data di entrata in vigore della medesima legge (21 novembre 2017), e dunque entro il 21 maggio 2018, uno o più decreti legislativi per armonizzare il sistema italiano alla nuova disciplina europea.

Ai sensi dell'articolo 31, comma 3, della legge n. 234 del 2012 il termine di scadenza della delega, in assenza dei due pareri delle Commissioni dei rispettivi rami parlamentari, è prorogato di novanta giorni, e, quindi, sino al 21 agosto 2018.

Com'è noto nel mese di marzo era stato reso pubblico **un primo schema di decreto legislativo che prevedeva l'abrogazione dell'attuale Codice Privacy** (d.l.vo n. 196/2003). Tale testo ha ricevuto molti contrastanti pareri dai commentatori, soprattutto per la tecnica normativa e l'assenza di previsioni sanzionatorie in ambito penale. Dopo un periodo di "oblio" in cui non si sono più avute informazioni dello schema di decreto, nel mese di maggio, e quindi in tempi strettissimi rispetto alla data di piena efficacia del Regolamento europeo, è avvenuta la trasmissione alle Commissioni parlamentari.

Il nuovo testo, su cui il Garante per la protezione dei dati personali ha espresso il proprio parere positivo condizionato, si differenzia dal precedente innanzitutto per la tecnica

normativa adottata. Anziché abrogare interamente l'attuale d.l.vo n. 196/2003 vengono sostituiti in blocco alcuni Titoli e capi dello stesso, e, con una minuziosa opera di cesellamento, modificate in maniera specifica articoli, commi e parole. **Il risultato è quello di un puzzle di non immediata lettura, che però regola ampiamente tutti gli ambiti in cui il legislatore nazionale avrebbe potuto intervenire sulla base del Regolamento**, e che cerchiamo di ricostruire in maniera sintetica.

Il testo dello schema si apre con l'art. 1, che dichiara **l'applicabilità generale del GDPR al trattamento dei dati personali.** La previsione, seppur potrebbe sembrare pleonastica, in realtà pone un principio di rilevante importanza, perché riconduce alla disciplina del Regolamento la generalità dei trattamenti effettuati nel nostro Paese. La normativa europea, infatti, ha un preciso ambito di applicazione materiale delimitato dai Trattati, e, pertanto, non è applicabile per quelle attività estranee al diritto dell'Unione Europea. In tale ottica **non sarebbero assoggettabili al GDPR i trattamenti effettuati per attività la difesa, la sicurezza nazionale, la sicurezza interna e l'ordine pubblico**, quelli effettuati dagli Stati membri nell'esercizio di attività relative alla **politica estera e di sicurezza comune** dell'Unione nonché nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE ossia le politiche relative ai **controlli alle frontiere, all'asilo e all'immigrazione**.

Cosa cambia rispetto al Codice Privacy

In tale ambito lo schema riporta una serie dettagliata di regole contenuta ora nel Titolo 1-bis. La principale **novità rispetto all'attuale Codice Privacy è che il trattamento collegato ad un interesse pubblico non viene più inquadrato dal punto di vista soggettivo, ossia con riferimento all'appartenenza dei Titolari alla categoria di soggetti pubblici**, bensì da quello oggettivo con riferimento alla finalità del trattamento, che può appunto essere considerata diretta a soddisfare un interesse pubblico anche qualora il trattamento sia effettuato da un soggetto privato.

Viene previsto che la base giuridica per tali tipologie di trattamenti sia esclusivamente una norma di legge o di regolamento e disciplinata la comunicazione (che non riguardi le particolari categorie di dati di cui all'art. 9 del GDPR o i dati giudiziari), riconfermando la distinzione tra i due trattamenti di comunicazione e diffusione, presente nella nostra normativa nazionale sin dalla l. n. 675/1996.

Una specifica disciplina, più restrittiva, viene introdotta per il trattamento delle particolari categorie di dati di cui all'art. 9 GDPR, il cui trattamento è consentito qualora necessario per il perseguimento di un interesse pubblico rilevante.

Cosa rientra nell'interesse pubblico rilevante

Lo schema contiene anche un elenco di ciò che è considerato rientrante nell'interesse pubblico rilevante, includendo una serie di finalità che spaziano dall'accesso ai documenti amministrativi, ad attività sanzionatorie, allo svolgimento di compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario.

In tale elenco è interessante notare che sono ricomprese le attività legate all'instaurazione, gestione ed estinzione di rapporti di lavoro per soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri.

Rischio discriminazione

La norma, qualora invariata, è destinata a creare un'evidente discriminazione tra i soggetti privati che effettuano tali trattamenti e rientrano nella categoria di coloro che svolgono compiti di interesse pubblico – autorizzati in via generale da tale previsione – ed i privatiche invece non rientrano in tale categoria, pur trattandosi, alla fine, di trattamenti necessari alla gestione dei rapporti di lavoro.

Regole deontologiche, misure di garanzia e provvedimenti generali

Lo schema di decreto prevede due strumenti che il Garante può utilizzare negli ambiti sopra descritti dei trattamenti per lo svolgimento di compiti di interesse pubblico e delle particolari categorie di dati. L'art. 2 quater disciplina infatti la promozione di "regole deontologiche" il cui rispetto, in seguito all'approvazione e pubblicazione, diviene condizione essenziale per la liceità e la correttezza del trattamento. Si tratterebbe di **uno strumento diverso dai Codici di condotta** di cui all'art. 40 GDPR, volto probabilmente a salvaguardare l'esistenza dei codici già adottati (i quali però dovrebbero essere aggiornati alle previsioni del GDPR). In considerazione di tale "sovrapposizione", e dato che il Regolamento prevede un apposito parere del **Comitato Europeo per la protezione dei dati** qualora il codice si riferisca ad attività di trattamento in vari Stati membri, l'utilizzo dello strumento delle "regole deontologiche" si potrebbe trovare ad essere esposto al rischio di violazione delle previsioni regolamentari, qualora vada ad incidere su trattamenti che riguardano il trattamento in vari Stati membri (si pensi a regole deontologiche in materia di dati relativi alla salute trattati da una multinazionale, ove vi siano Codici di condotta a livello europeo che già ne disciplinino il trattamento).

Oltre alle regole deontologiche, ed esclusivamente **qualora si tratti di dati genetici, biometrici e relativi alla salute**, il legislatore italiano intenderebbe anche esercitare l'opzione consentita dall'art. 9, 4° comma GDPR di far e**manare apposite misure di garanzia da parte del Garante.**

Si tratterebbe di un provvedimento simile a quelli già adottati nel vigore del **Codice Privacy**, con cui sono state indicate particolari misure di sicurezza o accorgimenti che i Titolari devono osservare nel trattare tali particolari categorie di dati. **La modularità della nuova norma, che stabilisce la possibilità di emanare tale tipologia di provvedimento per ogni singola diversa finalità di trattamento, ricorda evidentemente lo schema delle autorizzazioni generali**.

Infine, come ulteriore provvedimento del Garante, l'art. 2. *quaterdecies*prevede che per trattamenti nell'esecuzione di un compito di interesse pubblico che può presentare rischi particolarmente elevati, di cui all'art. 35 GDPR, ossia per quei trattamenti per i quali sarebbe necessaria una valutazione di impatto, **il Garante può adottare d'ufficio provvedimenti a carattere generale prescrivendo misure ed accorgimenti a garanzia dell'interessato**.

Avremo quindi vari tipi di provvedimenti: le regole deontologiche, la cui formazione coinvolge determinati soggetti; le misure di garanzia per specifiche tipologie di dati (genetici, biometrici e relativi alla salute), nonché provvedimenti generali per trattamenti che sarebbero soggetti a valutazione di impatto. Per tali ultimi, non potendo sicuramente il provvedimento generale del Garante sopprimere l'obbligo di effettuare la valutazione di impatto sarà quindi necessario lo svolgimento della stessa e l'adozione comunque degli accorgimenti e garanzie previste in tali tipologie di provvedimenti.

I casi di restrizione dei diritti dell'interessato

La restrizione dei diritti dell'interessato regolati dal GDPR è prevista in contemperamento a particolari interessi, quali le finalità **antiriciclaggio,**il sostegno alle **vittime di richieste estorsive**, l'attività delle **Commissioni parlamentari di inchiesta, la politica monetaria e valutaria, nonché il controllo del sistema dei pagamenti**, e degli intermediari creditizi e finanziari, nonché per lo svolgimento delle indagini difensive.

In tali ipotesi l'interessato non può esercitare direttamente i propri diritti, ma è stabilito che possano essere esercitate tramite il Garante, con una particolare procedura regolata all'art. 160.

Analoghe limitazioni, con pari meccanismi di tutela, sono previste per i trattamenti effettuati per **ragioni di giustizia**.

Garanzie e cautele per i diritti e le libertà fondamentali

La costrizione dei diritti dell'interessato deriva dall'applicazione dell'art. 23 del GDPR che la prevede purché vi siano particolari **garanzie e cautele per i diritti e le libertà fondamentali degli interessati**.

Ciò non sembra essere attuato con la previsione dell'art. 75 dello schema, il cui secondo comma contiene invece una totale disapplicazione dei diritti dell'interessato al trattamento di dati personali effettuato per finalità di tutela della salute e incolumità fisica dell'interessato o di terzi o della collettività. In particolare, al contrario di quanto appena previsto, non sono stabiliti dei criteri per tale limitazione o meccanismi alternativi di esercizio di detti diritti. Si tratta, in sostanza, di **una vera e propria "cancellazione" dei diritti dell'interessato**, che però sembra contraria alle previsioni di cui all'art. 23, che ne consente sì la limitazione ma non la completa soppressione.

I soggetti designati

L'art. 2 – *terdecies* dello schema sembra voler porre un chiarimento relativamente alla discussione, tutta italiana, se la figura del Responsabile del trattamento, prevista dal GDPR, sia applicabile anche ai cosiddetti responsabili interni, ossia a quei soggetti appartenenti all'organizzazione a cui sono affidati specifici compiti in merito al trattamento dei dati personali. **La norma, quindi, introduce il concetto di soggetti designati, che sembrerebbe diverso da quello dei soggetti "istruiti"** al trattamento di cui all'art. 29 GDPR. I designati, infatti, sono coloro a cui vengono attribuiti specifici compiti e funzioni –

e quindi non sono solo “istruiti” – internamente all’assetto organizzativo del titolare o del responsabile e relativamente al trattamento dei dati personali, che non saranno più inquadrati come responsabili interni ma solamente come soggetti designati.

Il secondo comma, invece, fa riferimento ai soggetti che sono autorizzati al trattamento di dati personali sotto la diretta autorità del titolare o responsabile. **La norma sembra però richiedere un *quid*aggiuntivo rispetto al GDPR, che prevede solo la necessaria istruzion**e – e non autorizzazione – di coloro che effettuano il trattamento. Trattandosi però di un atto che sicuramente è contenuto nel primo – se istruisco qualcuno ad effettuare un trattamento è implicito che lo devo aver autorizzato allo stesso – non sembra aggiungere nulla rispetto alla previsione regolamentare.

Disposizioni in settori specifici

Lo schema contiene poi una serie di disposizioni tese a regolare settori specifici. Si tratta da una parte della disciplina dei trattamenti di particolari categorie di dati in determinati ambiti (accesso ai documenti amministrativi, ambito sanitario) e dall’altra della regolamentazione di particolari trattamenti, come quello inerente ai **dati degli studenti, dei professionisti iscritti in albi, per archiviazione nel pubblico interesse, di ricerca storica, a fini statistici e ricerca scientifica,** compresa quella medica e biomedica, nonché, infine, per i trattamenti nell’ambito del rapporto di lavoro con il rinvio all’adozione di regole deontologiche e la disciplina dei *curricula* spontanei.

Servizi di comunicazione elettronica

Lo schema di decreto legislativo interviene anche sul Titolo X dell’attuale Codice Privacy. Si tratta di quell’insieme di norme che sono state introdotte nel nostro ordinamento in attuazione della direttiva n. 58/2002. Ebbene, il GDPR, all’art. 95, espressamente prevede che il Regolamento non avrebbe imposto obblighi supplementari rispetto a tale ambito di trattamenti, facendo salva quindi l’applicazione della normativa prevista nella direttiva n. 58/2002 in attesa di una riformulazione completa della materia con il **Regolamento e-Privacy**, attualmente ancora in sede di esame presso le istituzioni europee.

Il legislatore italiano, quindi, nell’ambito delle comunicazioni elettroniche non potrebbe inserire degli ulteriori obblighi giustificandoli dall’entrata in efficacia del GDPR, ma dovrebbe limitarsi ad adeguare tale normativa per ciò che è strettamente necessario in relazione alle nuove definizioni contenute nel Regolamento europeo.

Lo schema in esame alla Commissione parlamentare, però, non si limita a ciò.

Una norma pleonastica

Il nuovo art. 132 *ter* introduce una sorta di **rafforzamento in materia di sicurezza per i fornitori di servizi di comunicazione elettronica accessibili al pubblico**. Sinceramente la norma appare del tutto pleonastica, richiamando espressamente l’art. 32 GDPR e riproduttiva della norma regolamentare ed in quanto tale vietata come più volte chiarito dalla Corte di Giustizia europea.

Il successivo art. 132-quater, invece, aggiunge **un obbligo di informativa verso gli utenti non previsto dal Regolamento, e quindi in netto contrasto con l'art. 95 dello stesso** sopra richiamato, imponendo al fornitore di servizi di comunicazione elettronica accessibile al pubblico di dare informazione agli abbonati ed agli utenti di un particolare rischio di violazione di sicurezza della rete. Si tratta, in tutta evidenza, di un onere aggiuntivo che non trova alcun fondamento nella necessità di adeguare l'ordinamento interno al GDPR e che, forse, sarebbe stato più corretto inserire nello schema di decreto legislativo di recepimento della Direttiva n. 2016/1148 (cd. Direttiva NIS) data la stretta correlazione tra sicurezza delle reti e infrastruttura di cyber sicurezza nazionale.

I trattamenti effettuati in ambito di giornalismo

Alcune modifiche sono previste anche per **i trattamenti effettuati in ambito di giornalismo**. Innanzitutto, viene ampliata la portata delle norme prevedendone l'applicabilità quando il trattamento è effettuato ai fini della pubblicazione di saggi o altre opere anche in via non temporanea.

Inoltre, viene autorizzato il trattamento delle particolari categorie di dati di cui all'art. 9 GDPR, anche senza il consenso dell'interessato, ma nel rispetto delle regole deontologiche da adottarsi entro sei mesi dalla proposta del Garante, stabilendo un periodo di "transitorio, in cui il Garante in cooperazione con l'ordine dei giornalisti prescriverà misure di garanzia a tutela degli interessati.

Infine, ai trattamenti in ambito giornalistico non si applicano le misure di garanzia ed i provvedimenti generali di cui all'art. 2- *quaterdecies*.

Procedure e poteri del Garante

Lo schema modifica in parte le procedure di tutela per l'interessato. **Il reclamo innanzi al Garante può essere proposto se non sia già pendente un procedimento innanzi all'autorità giudiziaria** per il medesimo oggetto e le stesse parti, così come la proposizione del reclamo renderebbe improponibile la medesima domanda in sede giudiziaria.

Il reclamo può essere sottoscritto dall'interessato o da un'associazione rappresentativa. Pur se non menzionato espressamente, data l'alternatività tra tutela innanzi al Garante e tutela giudiziaria, deve ritenersi che il reclamo possa essere presentato anche con il patrocinio di un avvocato difensore.

I tempi di decisioni del reclamo sono fissati in nove mesi, ma il Garante può nelle more emanare i provvedimenti di cui all'art. 58 GDPR (correttivi e di indagine).

Diversa dal reclamo è la segnalazione che può essere proposta da chiunque e sulla base della quale il Garante d'ufficio i suddetti provvedimenti di cui all'art. 58.

Dal punto di vista della competenza dell'autorità giudiziaria è stabilito che nelle materie regolate dal GDPR la stessa sia assegnata alla magistratura ordinaria.

Nei poteri del Garante, elencati nel nuovo art. 154, rientra anche quello di denunciare i fatti configurabili come reati perseguibili di ufficio, oltre a quelli già previsti in via generale dal GDPR e dalle altre normative richiamate nella disposizione.

Il Garante, inoltre, ha anche facoltà di esercizio dell'azione in giudizio nei confronti dei titolari o dei responsabili del trattamento nel caso di violazione della normativa. Tale facoltà si eserciterebbe con il patrocinio dell'Avvocatura dello Stato o, in caso di conflitto di interesse, con propri funzionari od avvocati del libero foro.

I poteri di accertamento dell'Autorità

I poteri di accertamento dell'Autorità vengono ampliati, dato che la richiesta di esibizione oggi viene estesa anche al contenuto di banche dati, con possibilità di accesso alle stese, agli archivi e facoltà di ispezionare e verificare i luoghi in cui è effettuato il trattamento o comunque effettuare rilevazioni utili al controllo del rispetto della disciplina.

Gli accertamenti, inoltre, possono anche riguardare reti di comunicazioni accessibili al pubblico potendo procedersi all'acquisizione di dati ed informazioni online.

Infine, per i trattamenti aventi riguardo esigenze di sicurezza nazionale gli accertamenti devono essere svolti da un componente designato del Garante, senza possibilità di delega.

Una disciplina sanzionatoria articolata

E' noto che una delle critiche che era stata mossa al precedente schema di decreto legislativo era quella di non aver previsto alcuna sanzione penale, così "scriminando" la generale fattispecie di trattamento illecito dei dati.

Nel nuovo schema in esame, invece, trova posto un'articolata disciplina sanzionatoria, in realtà di non immediata comprensione, che regola sia l'applicazione delle sanzioni amministrative sia le fattispecie di reato per il Gdpr.

Il GDPR dal canto suo, già contiene un'articolata previsione delle sanzioni amministrative pecuniari, fissate solo nel massimo, applicabili alla violazione delle previsioni del regolamento. L'art. 83, paragrafo 4 GDPR, stabilisce le fattispecie la cui violazione comporta **la sanzione amministrativa pecuniaria fino a 10.000.000 di Euro**, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, mentre l'art. 83, paragrafo 5, prevede le ipotesi in cui la sanzione può arrivare fino a 20.000.000 di Euro o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

La medesima impostazione si ritrova nell'art. 166 come sostituito dallo schema di decreto legislativo.

Le fattispecie di sanzione “modesta”

Nell’ambito della sanzione più “modesta” rientrano le ipotesi di **violazione dell’obbligo di redigere un’informativa con linguaggio semplificato per i minori** (raccomandazione contenuta nel 58 Considerando ma poi non trasposta all’interno della parte normativa del GDPR, e ripresa invece al comma 2, art. 2- *quinquies* del Regolamento), la **violazione dei provvedimenti generali del Garante**, la violazione degli artt. 92 e 93, comma 1, del Codice Privacy (relativi alle cartelle cliniche ed ai certificati di assistenza al parto, norme in realtà non modificate dallo schema), nonché **la violazione di una serie di norme relativi ai servizi di comunicazione elettronica**, e quindi, teoricamente, esclusi dall’applicazione del GDPR, intesa quale imposizione di oneri aggiuntivi, quali la violazione dell’art. 123, 4° comma, sull’informativa inerenti ai dati di traffico, l’art. 124 sulla fatturazione dettagliata agli abbonati, l’art. 128 sul trasferimento di chiamata, l’art. 129 sugli elenchi, nonché il nuovo art. 132-*ter* sulle misure di sicurezza per tali soggetti.

I casi che prevedono sanzioni pesanti

Il 2° comma dell’art. 166 applica invece la più grave sanzione di cui all’art. 83, 5 paragrafo GDPR ad una serie molto ampia di fattispecie, tra cui la violazione dell’art. 2-ter, inerente alla base giuridica per il trattamento effettuato in esecuzione di un compito di interesse pubblico o connesso a pubblici poteri, 2 *quinquies* comma 1, che disciplina il consenso del minore (che, in verità, nel GDPR è sanzionato con la sanzione più lieve, potendo quindi risultare tale previsione contraria alla norma regolamentare), 2 *sexies*, per **il trattamento di particolare categorie di dati per motivi di interesse pubblico rilevante**, 2 *septies*, 7° comma, in caso di **violazione del divieto di diffusione dei dati genetici, biometrici o relativi alla salute**, 2-octies, in caso di **inosservanza delle previsioni per i dati giudiziari,** 2-*duodecies*, inerente la disciplina dei dati relativi a persone decedute, 53, per i dati identificati degli interessati nell’informatica giuridica, 75, 78, 79, 80, 82, 92 relativi agli adempimenti per i dati trattati in ambito sanitario, 93, commi 2 e 3, sempre in relazione ai certificati di assistenza al parto, 96, per **i trattamenti relativi agli studenti**, 99 e 100, 101 per il trattamenti per scopi di **archiviazione e ricerca storica,** 105 per i trattamenti a fini statistici e ricerca scientifica, 110, per i trattamenti di ricerca medica, biomedica ed epidemiologica, 111, 111 *bis* e 116, per i trattamenti nell’ambito di lavoro, 120 sulle assicurazioni, 122, nonché per quasi tutte le previsioni relative ai servizi di comunicazione elettronica, in caso di violazione degli artt. 123, 124, 125, 126, 130, 132, 132, 132 *bis*, 132 *quater*, 152 (che in verità riguarda la ripartizione di competenze tra nei giudizi) e la violazione delle misure di garanzia, delle regole deontologiche e delle modalità tecniche previste negli artt. 2 *septies* e 2 *quater*.

A questo elenco si aggiungono, sempre con applicazione della **sanzione massima, la violazione delle disposizioni relative al registro delle opposizioni.**

Orbene, tralasciando qualche evidente refuso del testo, come la sanzionabilità dell’art. 152 ed il pericolo in alcuni casi di duplicazione della sanzione già prevista nel Regolamento, oltretutto con una disciplina diversa da quella stabilita in sede Europea, viene da chiedersi se effettivamente ci sia una proporzionalità tra le condotte e le sanzioni nelle varie ipotesi. Equiparare la violazione del divieto di diffusione di dati genetici allo *spam*, entrambi sanzionabili con un massimo di 20.000.000 di Euro potrebbe violare un basilare principio di proporzionalità e gradualità della sanzione, a prescindere qui dal discorso della

legittimità del prevedere una sanzione in una materia per la quale il Regolamento prevede non vengano stabiliti oneri aggiuntivi, tenuto conto proprio dei diritti e delle libertà fondamentali degli interessi che entrano in gioco nelle due differenti ipotesi.

L'inserimento delle sanzioni penali suscita alcune perplessità

Il 1° comma, sanziona con la reclusione da sei mesi ad un anno e sei mesi chiunque contravviene alle disposizioni di cui agli art. 123, 126 e 130 o in violazione del provvedimento di cui all'art. 129, arrecando nocumento all'interessato. Si tratta, anche in questo caso, della violazione delle disposizioni relative ai servizi di comunicazione elettronica, che, come più volte si è detto, per le quali il GDPR non dovrebbe imporre obblighi aggiuntivi ai titolari. Nello specifico si tratta delle **disposizioni relative alla raccolta di informazioni sull'interessato tramite installazione di dei cookie, o alla disciplina delle comunicazioni indesiderate** (già però sanzionata nel precedente art.166 con la sanzione pecuniaria).

E' poi prevista la reclusione da uno a tre anni per il trattamento delle categorie di dati particolari di cui all'art. 9 GDPR o dei dati giudiziari in violazione di quanto previsto dalla norma che definisce i motivi di interesse pubblico rilevante o dalle specifiche disposizioni di cui all'art. 2 *octies.* Alla stessa pena soggiace chi per trarre profitto arreca nocumento all'interessato trasferendo i dati verso un paese terzo al di fuori dei casi consentiti dal Regolamento (condotta già espressamente sanzionata dallo stesso GDPR all'art. 83, 5° comma).

Inoltre, viene prevista una norma di chiusura, abbastanza incerta nella formulazione, secondo la quale quando per lo stesso fatto sia stata già applicata una sanzione amministrativa pecuniaria, e la medesima sia stata riscossa la pena deve essere diminuita, non specificando però a quanto ammonterebbe tale diminuzione, né come calcolare la stessa.

Tre specifiche fattispecie di reato

Infine, vengono inserite tre specifiche fattispecie di reato:

- la comunicazione e diffusione illecita di dati personali riferita ad un numero rilevante di persone, concetto però che sembra eccessivamente astratto per poter adeguatamente garantire la certezza della fattispecie di reato;
- l'acquisizione fraudolenta di dati personali, sempre riferito ad un "numero rilevante di persone",
- la falsità nelle dichiarazioni al Garante e l'interruzione dei compiti o l'esercizio dell'esercizio dei poteri del Garante.

La disciplina transitoria

Da ultimo un breve cenno alla disciplina transitoria stabilita nello schema di decreto.

Innanzitutto è previsto che **i Codici di deontologia e buona condotta già approvati conservino la loro validità sino alla definizione della procedura di approvazione**, e purchè entro sei mesi vengano sottoposti nuovi Codici di condotta ai sensi dell'art. 40 GDPR.

Per le autorizzazioni generali emanate, e relative alle previsioni di cui all'art. 6, par. 1, commi c) ed e) ed all'art. 9 par. 4 ed al capo IX del GDPR, il Garante dovrebbe individuare, entro 90 giorni dalla pubblicazione del decreto legislativo in esame, le prescrizioni di dette autorizzazioni che risultano compatibili con il GDPR, provvedendo nel caso all'aggiornamento. Quelle incompatibili o quelle per cui non sia stato adottato il provvedimento di adeguamento cesseranno di avere efficacia alla scadenza dei 90 giorni. Tutte le altre autorizzazioni generali cesseranno di avere effetto il novantesimo giorno successivo all'entrata in vigore del decreto.

Infine, i provvedimenti del Garante continueranno ad applicarsi successivamente alla data di entrata in vigore dello schema in quanto compatibili con il GDPR e con le disposizioni del decreto stesso.

Infine, la procedura di previa comunicazione dei trattamenti effettuati sulla base giuridica del legittimo interesse del Titolare, di cui agli art. 1022 e 1023, cesserà di avere efficacia generale, e sarà applicabile solamente all'ipotesi di dati del minore raccolti online.

Conclusioni

La disamina dello schema di adeguamento non può che far riflettere se, effettivamente, la scelta di stravolgere il testo precedentemente circolato sia da considerarsi migliore o meno. **Vi sono sicuramente alcune parti dell'articolato degni di nota, come l'applicabilità del GDPR a tutte le tipologie di trattamenti**, la definizione puntuali di quelli che sono i trattamenti necessari per l'esecuzione di un interesse pubblico, o che rispondo ad un interesse pubblico rilevante.

Altri tasselli, però, sembrano poter andare oltre a quanto richiesto per il semplice adeguamento della normativa italiana, come la modifica e l'introduzione di nuovi adempimenti nell'ambito dei servizi di comunicazione elettronica, o l'introduzione in maniera indistinta di un vasto numero di sanzioni, sia amministrative sia di carattere penale, senza alcuna gradazione delle stesse rispetto all'effettiva lesività della condotta.

Purtroppo, evidentemente anche a causa della difficile situazione politica che sta attraversando il nostro Paese, **il ritardo si è oramai consolidato**. Sarebbe però auspicabile che, a questo punto, si valuti l'ipotesi di adottare **un approccio *soft* all'applicazione** della regolamentazione europea, sfruttando questi ulteriori mesi di tempo per la scadenza della delega per apportare i necessari miglioramenti al testo esaminato.