NOTA INFORMATIVA N.16/2022

LA PROTEZIONE DEI DATI PERSONALI

1. Premessa

A una prima lettura, le figure di reato ex artt. 167, 167-bis e 167-ter del d.lgs. n. 196/2003 (cd. «codice della privacy»), possono lasciare spaesato il cultore del diritto penale. Difatti, non solo appare evidente che il legislatore ha descritto larga parte dei corrispondenti fatti tipici impiegando la tanto deprecata «tecnica del rinvio», che notoriamente degrada la pena a strumento meramente sanzionatorio di un precetto aliunde descritto, ma, forte è a tutta prima l'impressione che siffatte figure criminose siano destinate ad ambientarsi in contesti applicativi molto specialistici, tendenzialmente lontani, quindi, dall'ordinaria esperienza di vita del comune cittadino. E in effetti, volendo naturalmente esemplificare, risulta che:

a) le fattispecie contenute nei commi 1, 2 e 3 dell'art. 167 puniscono chiunque, in violazione di specifiche disposizione del «codice» o del GDPR, operi ovvero proceda al trattamento di dati personali o al trasferimento di questi verso un paese terzo o un'organizzazione internazionale, e ciò al fine di trarne un profitto o arrecare un danno, e cagionando infine alla vittima un nocumento;

b) a sua volta, le fattispecie dell'art. 167-bis, commi 1 e 2, sottopongono a pena chiunque comunichi o diffonda un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala in violazione di specifiche disposizioni del «codice», ovvero, ove richiesto, senza il consenso del titolare, e ciò al fine di trarre un profitto o di arrecare un danno;

c) la fattispecie dell'art. 167-ter, infine, sanziona penalmente chiunque acquisisca con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, e ciò al fine di trarre un profitto o di arrecare un danno.

Come è agevole constatare, dunque, le figure di reato in questione fanno riferimento, per esempio, a un non meglio precisato trattamento dei dati personali che sia stato operato in contrasto con precipue disposizioni amministrative, a un trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale, alla diffusione ovvero alla acquisizione fraudolenta di un archivio automatizzato, o di una sua parte sostanziale, a un trattamento su larga scala di dati personali, e via dicendo: espressioni, tutte queste, che in effetti possono apparire, se non proprio esoteriche, quanto meno lontane dalla comune esperienza. Ma tutt'altra impressione si riporterebbe, probabilmente, là dove si avesse cura di approfondire il concetto (normativo) di dato personale e di trattamento dello stesso di gettare uno sguardo ai repertori di giurisprudenza. Invero, così facendo,

In primo luogo si scoprirebbe che l'oggetto materiale delle fattispecie criminose qui in rilievo è costituito, genericamente, da una qualsiasi informazione riguardante una persona fisica identificata o identificabile (art. 4, comma 1, n. 1, GDPR), che venga poi sottoposta a qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione» (art. 4, comma 1, n. 2, GDPR).

In secondo luogo, ci si accorgerebbe di come le figure di reato che qui rilevano possono sanzionare anche fatti tutt'altro che eccezionali nella vita quotidiana.

2. La signoria sui propri dati personali come diritto fondamentale della persona

La prima domanda che occorre farsi nell'approcciare tali fattispecie è quella di interrogarsi sulla ragione della loro esistenza, e quindi chiedersi quali siano le esigenze di tutela alle quali esse intendono offrire risposta. Nessuno può oggi seriamente dubitare di come le tecnologie informatiche, una volta applicate ai flussi di informazioni, abbiano determinato una enorme trasformazione, rispetto anche al recente passato, degli effetti derivanti dalla raccolta dei dati relativi alla persona. Difatti, la capacità degli elaboratori elettronici di conservare informazioni in quantità illimitata su tutti gli aspetti della vita quotidiana di ogni individuo e di aggregare e confrontare i dati ha creato un nuovo potere di dominio sociale sull'individuo, il che rende possibile un controllo costante e più penetrante dei comportamenti degli utenti e una ricognizione sempre aggiornata delle loro inclinazioni, abitudini, interessi, preferenze, rendendo così i dati personali una nuova e sempre più preziosa merce.
Non può quindi stupire se, raccogliendo un senso di angoscia senz'altro diffuso negli individui a fronte della possibilità che la loro sfera privata venga distrutta dalla circolazione incontrollata di siffatti dati, l'art. 1 del «codice della privacy», in origine, e l'art. 1, par. 2, del GDPR, oggi, abbiano avvertito il bisogno di proclamare l'esistenza di un vero e proprio diritto alla protezione dei dati personali, quale situazione soggettiva inscrivibile tra i diritti e le libertà fondamentali delle persone fisiche. Del resto, il «Considerando» n. 1 dello stesso GDPR ha cura di ricordare come la necessità della salvaguardia dei dati personali fosse già stata sancita sia dall'art. 8, par. 1, della Carta dei diritti fondamentali dell'Unione europea, sia dall'art. 16, par. 1, del Trattato sul funzionamento dell'Unione europea («TFUE»), pur riconoscendo al successivo par. 4 come tale diritto non debba intendersi come prerogativa assoluta, ma contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità (v. l'art. 23 e il «Considerando» n. 153 del GDPR), come per esempio la libertà di espressione o informazione, così recependo un canone da tempo elaborato anche dalla nostra Corte costituzionale, secondo cui nessun diritto può dirsi tiranno degli altri.
Da parte propria, la dottrina di settore, preso atto dell'esistenza normativa di tale diritto alla protezione dei dati personali, si è sforzata di meglio definirne i contenuti e di collocarlo in modo appropriato entro la scala assiologica dei beni giuridici tutelati dall'ordinamento. In tale prospettiva, si è detto che tale posizione soggettiva consiste precipuamente nel diritto del soggetto cui i dati si riferiscono di esercitare un controllo, anche attivo, su detti dati, che si estende dall'accesso alla verifica, la cui pratica estensione dipende chiaramente da quella del concetto di «dato personale», invero come visto assai ampia. Così definito, il diritto de quo andrebbe idealmente a collocarsi nell'alveo di quei diritti della personalità che, nel nostro ordinamento, e in difetto di più specifiche disposizioni costituzionali, viene comunemente fondato sulla "clausola aperta" dell'art. 2 della Carta; nondimeno, esso andrebbe distinto da alcuni altri diritti per così dire "limitrofi", con i quali, tuttavia, esso può qualche volta di fatto coincidere. In particolare, il diritto alla tutela dei dati personali andrebbe concettualmente distinto, tra gli altri:

- dal c.d. «diritto alla riservatezza», consistente nella facoltà di escludere altri dalla conoscenza di vicende strettamente personali, il quale, a differenza di quello alla tutela dei dati personali, ha contenuto eminentemente «negativo», sostanziandosi nella pretesa di non fare sapere ad altri informazioni relative esclusivamente alla vita privata, e risulta quindi violabile soltanto da condotte di comunicazione e diffusione di dati personali;
- dal c.d. «diritto all'identità personale», consistente nel diritto a non vedere travisata la propria personalità individuale, e cioè la pretesa a essere rappresentati, nella vita di relazione, nella propria, vera identità, come essa è conosciuta nella realtà sociale;
- dal c.d. «diritto all'immagine», che consiste nella pretesa di un soggetto di vietare a terzi l'utilizzo abusivo della propria immagine, da intendersi come rappresentazione, in qualsiasi forma riconoscibile, delle proprie sembianze.

A prescindere da tali distinzioni, che naturalmente incidono sui mezzi di tutela che il soggetto offeso può utilmente invocare di fronte all'Autorità, sotto il versante squisitamente punitivo può in ogni caso

affermarsi che, almeno secondo le più diffuse teorie costituzionalmente orientate del bene giuridico, la collocazione assiologica del diritto alla protezione dei dati personali tra quelli della personalità umana riconosciuti dell'art. 2 Cost. parrebbe già di per sé idonea a legittimare l'esistenza quanto meno della c.d. meritevolezza di pena, e quindi a giustificare l'allestimento di un cordone penalistico da porre a protezione dell'integrità di siffatta posizione soggettiva. E ciò anche prescindendo dalle indicazioni in materia rinvenibili nella normativa comunitaria d'origine, la quale, per vero, appare ambigua. In effetti, almeno inizialmente i decisori europei avevano addirittura lasciato liberi gli Stati di predisporre generiche «sanzioni» da applicare in risposta alla violazione del diritto in questione, come risultava dall'art. 24 della primigenia Direttiva 95/46/CE, attuata in Italia dalla legge 31 dicembre 1996, n. 675, antesignana dell'attuale «codice della privacy», ovvero dall'art. 15, par. 2, della Direttiva 2002/58/CE in materia di protezione dei dati personali nell'ambito di comunicazioni elettroniche, mentre, da parte propria, l'attuale GDPR si è limitato a specificare che i singoli legislatori nazionali «dovrebbero poter stabilire» sanzioni che adesso, però, vengono esplicitamente qualificate come «penali» (v. «Considerando» nn. 149 e 152), salvo naturalmente il rispetto del consueto obbligo di far sì che esse risultino «effettive, proporzionate e dissuasive» (art. 84, par. 1, GDPR).

3. La protezione dei dati personali tra law in books e law in action

Premessa, quindi, la astratta legittimazione del legislatore interno alla predisposizione di una risposta penale avverso le violazioni del diritto qui in rilievo, si tratta ora di puntualizzare i "modi" della stessa, ovverosia le tecniche di tutela impiegate dal legislatore, le quali sembrano volere selezionare specifiche forme di aggressione al bene giuridico. In particolare, balza agli occhi la previsione entro le figure criminose qui in rilievo del dolo specifico di «profitto» o di «danno», nonché del «nocumento», i quali a volte ricorrono in modo congiunto, come nel caso delle fattispecie contemplate dall'art. 167, altre volte no, avendo il legislatore richiesto esclusivamente l'orientamento finalistico del dolo, come nel caso delle incriminazioni recate dagli artt. 167-bis e 167-ter.
Per la verità, che una tale connotazione oggettiva e soggettiva delle fattispecie in rilievo non debba meravigliare soverchiamente l'interprete, non costituendo neanche un'assoluta novità, parrebbe suggerito sia dal dato storico che da una politica criminale che auspicabilmente si voglia rispettosa del *favor libertatis*. A tale riguardo, difatti, è opportuno anzitutto ricordare come l'immediato precedente normativo delle odierne incriminazioni in materia di trattamento illecito di dati personali, ossia il disposto dell'art. 35, commi 1 e 2, della richiamata legge n. 675/1996, contemplava la medesima necessità che l'agente agisse «al fine di trarre per sé o per altri profitto, o di recare ad altri un danno», mentre il comma 3 dello stesso art. 35 contemplava il verificarsi di un «nocumento», sebbene non come elemento costitutivo di fattispecie ma come circostanza aggravante. Se, con il conforto della dottrina e della giurisprudenza prevalenti, si volesse qualificare il «nocumento» richiamato dall'odierno art. 167 in termini di elemento costitutivo del reato e non di condizione obiettiva di punibilità, sottraendolo quindi alla rigida regola ascrittiva dell'art. 44 c.p.; se poi si volesse prendere atto di come la previsione di un tal evento di danno non possa che riflettersi positivamente sulla pregnanza offensiva della stessa figura criminosa, che non potrebbe più a ragione inscriversi entro il novero delle fattispecie di pericolo astratto, notoriamente oggetto di diffusi sospetti di incostituzionalità; se, infine, si volesse riconoscere che la caratterizzazione dell'elemento soggettivo nei termini appena descritti risulta storicamente radicata nella disciplina penale di settore, oltre che evidentemente tesa a restringere l'alveo applicativo della sanzione criminale, non resterebbe che plaudere incondizionatamente alla svolta garantista intrapresa dal moderno legislatore in materia di tutela penale del trattamento dei dati personali. Le forme di quest'ultima, infatti, dovrebbe ora apparire assai più razionali e selettive che in passato, puntualizzate su forme di offesa congrue e realmente lesive rispetto al bene giuridico protetto, così da raggiungere in modo più soddisfacente quel delicato equilibrio tra *right to information e right to privacy* sul quale, come noto, la disciplina penale e non del trattamento dei dati personali si fonda.
Tuttavia, anche a ritenere fondati i rilievi interpretativi e storico-normativi appena richiamati, non sembra che la realtà si sia a essi perfettamente adeguata.

Anzitutto, è la dimensione applicativa del diritto a suggerire una certa cautela nel giudicare la reale portata selettiva dei richiamati riferimenti al dolo specifico e all'evento di danno che la legge contempla. A tale proposito, occorre infatti ricordare come nella prassi i concetti di «profitto», di «danno» e di «nocumento» siano ben lungi dall'essere scolpiti nel marmo, e che, specialmente, se una loro interpretazione può dirsi prevalente, l'impressione è che essa non sia capace di selezionare finalità soggettive e/o risultati dannosi così caratterizzati da risultare tanto più ristretti rispetto a quelli che, secondo *l'id quod plerunque accidit*, appaiono già impliciti nelle condotte illecite richiamate dalle fattispecie penali qui in rilievo.
Per convincersene, basterà ricordare come:

- il «profitto» sia stato correntemente inteso come una qualsiasi soddisfazione o godimento che l'agente si ripromette di ritrarre, anche non immediatamente dalla propria azione;
- il «danno» sia stato rinvenuto in un qualsiasi pregiudizio giuridicamente rilevante per il soggetto passivo;
- infine, il «nocumento» sia stato identificato in ogni pregiudizio giuridicamente rilevante di qualsiasi natura, patrimoniale o non patrimoniale, subito dal soggetto cui si riferiscono i dati protetti oppure da terzi quale conseguenza dell'illecito trattamento, ovvero in effetti pregiudizievoli sotto il profilo morale, e ciò, peraltro, con il rischio di produrre una bizzarra e cortocircuitante convergenza con l'oggetto del richiamato dolo specifico di «danno».

Non può allora stupire il fatto che la più autorevole giurisprudenza ben raramente abbia negato la ricorrenza dei reati *de qui bus* per la mancanza di tali elementi costitutivi. A quanto risulta, ciò sembra essere accaduto soltanto in una ipotesi di c.d. «spamming», avendo ritenuto la Corte di cassazione che il nocumento non può certo esaurirsi nel semplice fastidio di dover cancellare di volta in volta le e-mail indesiderate, ovvero in un caso ove un individuo aveva erroneamente fatto pubblicare su una rivista hard il numero telefonico di un soggetto a lui sconosciuto in luogo del proprio, avendo i giudici di legittimità rilevato che, in seno alla fattispecie dell'art. 167, la strutturale intenzionalità finalistica della condotta tipica rende incompatibile la forma del dolo eventuale, che postula l'accettazione solo in via ipotetica, seppure avverabile, del conseguimento di un risultato.
Inoltre, non si deve trascurare l'influenza sull'interprete di un possibile condizionamento legato a un certo modo tradizionale di "sottintendere" le forme di tutela di certi beni giuridici. Non è, infatti, da escludere che nella pratica applicazione di tali disposizioni incriminatrici giochino pure un ruolo le matrici codicistiche alle quali le fattispecie degli artt. 167, 167-bis e 167-ter sembrano potersi in qualche modo ricondurre. La circostanza, non certo casuale, che tutte e tre le fattispecie in questione esordiscano con la clausola «Salvo che il fatto costituisca più grave reato» fornisce invero l'indizio forse più chiaro della loro contiguità a figure criminose più tradizionali, riconducibili alla tutela di interessi fondamentali della persona che possono dirsi "affini" a quello della signoria sui propri dati personali.
In effetti, la dottrina:

- da un canto, non ha mancato di rilevare come, vuoi appunto per la somiglianza dei beni tutelati, vuoi per le modalità aggressive tipizzate, le fattispecie in discorso ben possano interferire con l'applicazione di alcune figure di reato che il Codice penale ha posto a tutela della inviolabilità dei «segreti», come per esempio quelle degli artt. 326 e 616 s.;
- dall'altro, ha poi evidenziato la necessità di mantenere una certa «simmetria» tra le fattispecie qui in rilievo e quelle incriminazioni codicistiche che di fatto salvaguardano il più ampio bene della «privacy», sebbene da aggressioni realizzate con modalità diverse da quelle del trattamento dei dati personali, come per esempio sembrano fare i delitti degli artt. 615-bis e, appunto, 616 s. c.p.

Da qui, la possibile tendenza a una sorta di "obliterazione interpretativa di fatto" di quegli elementi costitutivi del reato avvertiti come tipologicamente estranei alle forme classiche di tutela penale dei diritti fondamentali della persona, le quali in effetti tendenzialmente prescindono dalle inclinazioni

finalistiche della volontà del reo o dalla presenza di eventi dannosi ulteriori rispetto a quello insito nella violazione dello stesso diritto salvaguardato.

4. Le violazioni del «codice della privacy» penalmente rilevanti e il rapporto con l'illecito amministrativo a seguito del d.lgs. n. 101 del 2018

In effetti, la reale pregnanza del presidio penale posto a salvaguardia del corretto trattamento dei dati personali deve essere misurata alla luce sia *dell'ubi consistam* delle condotte criminose, ovverosia, in questo caso, del contenuto delle disposizioni del «codice della privacy» la cui violazione risulta penalmente repressa, sia del riparto tra le aree di intervento del reato e dell'illecito punitivo amministrativo, che sin dalla legge n. 675/1996 ha concorso alla strategia di tutela dei dati personali. Ebbene, proprio questi ambiti sono stati oggetto di due recenti interventi legislativi:

- il primo, di contenuto assai ampio e incisivo, è quello operato dal noto GDPR e dal d.lgs. 10 agosto 2018, n. 101, che ha dettato le disposizioni per il necessario adeguamento del diritto interno al regolamento in questione;
- il secondo, di portata assai più circoscritta, è rinvenibile nel d.l. 8 ottobre 2021, n. 139, convertito con modificazioni dalla l. n. 205/2021, che ha inciso indirettamente sulle fattispecie criminose qui in rilievo agendo su alcune delle disposizioni del «codice della privacy» da esse richiamate.

Volendo qui limitare l'attenzione ai soli interventi normativi che hanno inciso sull'addenda penalistica del «codice della privacy» sembra che almeno tre siano state le direttrici fondamentali lungo le quali i regolatori si sono mossi.
In primo luogo, il riferimento è alle sostanziali modifiche che, sulla scorta della mutata normativa comunitaria, il legislatore ha introdotto nella tradizionale fattispecie del «Trattamento illecito di dati» recata dall'art. 167, che è stato riscritto. La prospettiva nella quale ci si è qui mossi è stata quella di una espansione applicativa dell'illecito amministrativo, alla quale ha fatto eco, se non una apprezzabile riduzione quantitativa, senz'altro una "specializzazione qualitativa" dell'area del penalmente rilevante. Una tale opzione di tutela è stata di fatto imposta dai par. 4, 5 e 6 dell'art. 83 GDPR, i quali hanno considerato alla stregua di illecito amministrativo la violazione di una lunga teoria di disposizioni del medesimo GDPR, parte delle quali, trasfuse nel «codice», erano per l'appunto richiamate dalla fattispecie incriminatrice dell'art. 167.
Ne è perciò risultato:

- da un canto, una sostanziosa dilatazione del campo applicativo dell'art. 166, il quale, sotto la rubrica «Criteri di applicazione delle sanzioni amministrative pecuniarie e procedimento per l'adozione dei provvedimenti correttivi e sanzionatori», nei primi due commi in realtà stila una estesa lista di articoli del «codice» la cui violazione viene ora espressamente repressa con la sanzione amministrativa pecuniaria, peraltro definita nei propri limiti edittali dal diretto rinvio al predetto art. 83 GDPR;
- dall'altra, come si anticipava, una "settorializzazione" della tutela penale recata dalla fattispecie dell'art. 167, la quale, salvo quanto già detto a proposito del dolo specifico e del nocumento, rispetto al passato presuppone la violazione di più settoriali disposizioni del «codice».

In particolare, e volendo qui naturalmente solo richiamare per sommi casi una disciplina amministrativa sottostante assai più complessa e articolata, la pena risulta ora sanzionare:

- propriamente, il trattamento di categorie particolari di dati personali (v. artt. 9 e 10 GDPR) che risulti necessario «per motivi di interesse pubblico rilevante», che attenga a «dati genetici, biometrici e relativi alla salute» ovvero a «dati relativi a condanne penali e reati», il quale violi le precipue disposizioni che sovraintendono alle sue modalità di svolgimento (v. artt. 2-sexies, 2-septies e 2-octies);

- le operazioni compiute in violazione delle specifiche disposizioni previste per i dati «relativi al traffico riguardanti contraenti e utenti trattati dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico» (v. art. 123), o per i «dati relativi all'ubicazione diversi dai dati relativi al traffico, riferiti agli utenti o ai contraenti di reti pubbliche di comunicazione o di servizi di comunicazione elettronica accessibili al pubblico» (v. art. 126);
- la violazione del provvedimento (amministrativo!) del Garante per la protezione dei dati personali che abbia previamente definito le «modalità di inserimento e di successivo utilizzo dei dati personali relativi ai contraenti negli elenchi cartacei o elettronici a disposizione del pubblico» e individuato le relative «idonee modalità per la manifestazione del consenso all'inclusione negli elenchi e, rispettivamente, all'utilizzo dei dati per finalità di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale [...]» (v. art. 129);
- la violazione di una capillare serie di prescrizioni atte a disciplinare le cc.dd. «Comunicazioni indesiderate», ovverosia quelle inoltrate mediante l'utilizzo di «sistemi automatizzati di chiamata o di comunicazione di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale svolgimento», anche ove implicanti l'uso di «posta elettronica, telefax, messaggi del tipo MMS (Multimedia Messaging Service) o Sms (Short Message Service) o di altro tipo» (v. art. 130).

In secondo luogo, e in evidente continuità con l'opzione di tutela appena richiamata, il legislatore ha inteso regolare il rapporto applicativo tra la potenziata sanzione amministrativa e quella penale, probabilmente memore delle annose questioni di legittimità costituzionale e convenzionale e dei disorientamenti giurisprudenziali originati dall'introduzione del sistema del c.d. «doppio binario» sanzionatorio amministrativo/penale per meglio fronteggiare, per esempio, il fenomeno degli «abusi di mercato» in ambito finanziario. In questa prospettiva, e pur con alcune riserve legate alla non proprio cristallina formulazione della norma, è da salutare con favore il disposto dell'ultimo comma dell'art. 167, richiamato anche dagli artt. 167-bis e 167- ter, il quale, presupposta l'avvenuta riscossione di una somma di denaro comminata, per il medesimo fatto, a titolo di sanzione amministrativa pecuniaria, prevede una non meglio specificata «diminuzione» della successiva pena pecuniaria eventualmente irrogata al medesimo autore.
In terzo e ultimo luogo, il legislatore ha provveduto a estendere l'area di intervento della pena a condotte tradizionalmente estranee al «trattamento illecito» dei dati personali, che costituisce la figura di reato senz'altro più rappresentativa di questo ambito di materia. Il riferimento, in particolare, è alle nuove previsioni di reato di cui agli artt. 167-bis e 167-ter, che sanzionano, come già ricordato, la comunicazione, la diffusione (con il consenso o meno, a seconda che esso sia o no richiesto dalla legge) e la acquisizione fraudolenta, anche parziale, di un archivio, automatizzato o meno, che contenga dati personali e che sia soggetto a un c.d. «trattamento su larga scala». La pena edittale qui significativamente più rigorosa di quella prevista dall'art. 167 rende ragione delle maggiori e diverse potenzialità offensive di tali fatti rispetto a quelle del più tradizionale «trattamento illecito» di dati personali, le quali possono apprezzarsi sotto due diversi profili.
Principalmente, sotto quello dell'oggetto materiale delle condotte criminose, se è vero, anzitutto, che i dati personali che qui rilevano si presentano in modo aggregato, poiché raccolti appunto in un «archivio», e che, giusto quanto si ricava dal «Considerando» n. 91 del GDPR, essi risultano oggetto di pratiche 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».
Inoltre, sotto quello della lesività insita nell'u*bi consistam* delle condotte o nella loro modalità di commissione. Al riguardo, infatti, appare evidente che la «comunicazione» e la «diffusione» di siffatti dati, che l'art. 2-ter, comma 4, distingue in ragione del tradizionale criterio della determinatezza (-determinabilità) o indeterminatezza dei soggetti destinatari della loro conoscenza, amplifica l'offesa, così come la modalità «fraudolenta» di acquisizione degli stessi presenta chiaramente in sé un disvalore intrinseco meritevole di maggiore stigma rispetto a una qualsiasi altra operazione "irregolare", in quanto

irrispettosa di prescrizioni procedimentali formalizzate, che fosse stata eventualmente intrapresa sui medesimi dati personali.

5. Conclusioni

Se il ricordato ampliamento dell'area di prensione dell'illecito amministrativo sembra corrispondere agli auspici da tempo formulate dalla dottrina di settore, che in esso ha visto, qui, uno strumento di tutela particolarmente efficace e spedito, non sembra, invece, che gli ultimi interventi novellatori abbiano inciso significativamente sulla qualità della disciplina penale di settore. Il mantenimento della «tecnica del rinvio» nella formulazione dell'art. 167, e sebbene in minore misura anche in quella dell'art. 167-bis, sembra infatti qui perpetuare, se non addirittura esasperare, antichi vizi. In particolare, il riferimento non è tanto alle tensioni che, così operando, il legislatore determina in rapporto al principio di determinatezza, forse troppo spesso sopravvalutate e comunque pressoché inevitabili in materie, come questa, dall'alto contenuto tecnico, quanto alla violazione di un duplice e ulteriore profilo di garanzia. E invero, da un canto, e nonostante i contorsionismi teorici che possono farsi nell'individuare ciò che debba esattamente intendersi per «precetto» penale, è difficile non vedere il vulnus al principio della riserva di legge che si crea ogniqualvolta la pena venga utilizzata per sanzionare la violazione di un provvedimento emesso da una Autorità amministrativa come indubbiamente è il Garante per la protezione dei dati personali. Ma ancor di più, d'altro canto, ciò che appare fortemente compromessa nel richiamo, entro il precetto sanzionatorio, di una serie ampia e assai internamente articolata di prescrizioni tecniche, a volte anche molto minute, è la stessa capacità della fattispecie incriminatrice di selezionare gli aspetti più pregnanti della disciplina extra-penale la cui inosservanza possa ritenersi davvero significativa, e quindi tale da richiedere ragionevolmente la reazione sanzionatoria più rigorosa, almeno sulla carta, della quale il legislatore dispone; e ciò tanto più là dove, come detto, si giudichino i riferimenti al dolo specifico e al nocumento di per sé stessi non pienamente idonei, ove non ulteriormente connotati, ad ammantare di un significativo e aggiuntivo disvalore la fattispecie. In difetto, non resta che affidarsi alla ponderazione del giudice nel muoversi entro la forbice sanzionatoria edittale o nel ricorrere, quando possibile, a quegli strumenti che oggi inverano processualmente l'antico adagio per cui de minimis non *curat Praetor*.
Forse non è peregrino sostenere la possibilità che il presidio dell'articolata disciplina amministrativa del trattamento dei dati personali sia devoluto al più agile strumento dell'illecito punitivo amministrativo, magari non soltanto di natura pecuniaria, lasciando al diritto penale la stigmatizzazione di quelle più aggressive condotte di «indiscrezione» e di «rivelazione» che, in ambiti limitrofi, sono ben conosciute. In questa prospettiva, però, occorre riconoscere che l'utilità pratica di fattispecie come quelle recate dagli artt. 167-bis e 167-ter dipende dalla loro capacità di connotarsi specificamente quanto ai fatti da reprimere, dato che è verosimile che condotte come quelle di «comunicazione» o di «diffusione» illecita di dati personali vadano a pregiudicare, nella più parte dei casi, ulteriori diritti fondamentali della persona, aprendo così all'applicazione di altre e diverse figure di reato.

10 marzo 2022

A cura di Avv. Bruna Capparelli