Gli specifici aspetti relativi alla protezione dei dati personali del decreto legislativo 10 Marzo 2023, n. 24 di attuazione della Direttiva UE 2019/1937 sul whistleblowing.

Prof. Avv. Alessandro del Ninno
a.delninno@5lex.it
www.5lex.it

INDICE

---

§ 1. Introduzione: l'impianto della nuova disciplina riguardante la protezione delle persone che segnalano violazioni.

Il presente contributo intende svolgere talune considerazioni operative in merito agli specifici aspetti *data protection* implicati dalla applicazione del Decreto Legislativo 10 Marzo 2023, n. 24 (pubblicato nella G.U. – Serie Generale – n. 63 del 15 Marzo 2023) recante attuazione della c.d. Direttiva UE 2019/1937 sul *Whistleblowing* (*Direttiva 2019/1937 UE del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione*). Come è noto, il decreto legislativo italiano di attuazione – di seguito, per brevità, il "*Decreto*" e che si applica alla protezione delle persone che segnalano violazioni non solo della normativa unionale, ma anche – ovviamente – delle disposizioni della normativa nazionale - disciplina la *protezione delle persone* che segnalano violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato.

Che tipo di violazioni? Esse consistono in comportamenti, atti od omissioni che ledono l'interesse pubblico (inclusi gli interessi finanziari dell'Unione europea e gli interessi al funzionamento del mercato interno secondo le regole della concorrenza) o l'integrità dell'amministrazione pubblica o dell'ente privato, e si risolvono in illeciti amministrativi, contabili, ci-

vili o penali, in condotte illecite rilevanti ai sensi del decreto legislativo 8 giugno 2001, n. 231 (o in violazioni dei modelli di organizzazione e gestione ivi previsti) o che riguardano determinati settori (possono essere segnalate violazioni in vari settori, dagli appalti pubblici alla tutela dell'ambiente, fino alle stesse violazioni nel settore della "*tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi*").

Sono obbligati all'osservanza delle norme previste dal *Decreto* tutti gli enti del settore pubblico. Per i soggetti del settore privato sono tenuti quelli: (a) che hanno raggiunto, nell'ultimo anno, la media di almeno cinquanta lavoratori subordinati con contratti di lavoro a tempo indeterminato o determinato; (b) che nell'ultimo anno non hanno raggiunto tale media ma rientrano nell'ambito di applicazione di una serie di normative europee, specificate nell'Allegato al *Decreto* (alle parti I.B e II); (c) che nell'ultimo anno non hanno raggiunto tale media ma rientrano nell'ambito di applicazione del decreto legislativo 8 giugno 2001, n. 231, e adottano modelli di organizzazione e gestione ivi previsti.

Quanto alla decorrenza degli obblighi, il Decreto si applicherà a partire dal 15 Luglio 2023, salvo che per una parte dei soggetti privati. Per quelli che hanno impiegato, nell'ultimo anno, una media di lavoratori subordinati, con contratti di lavoro a tempo indeterminato o determinato, fino a duecentoquarantanove gli obblighi di istituzione di un canale di segnalazione interna si applicheranno a partire dal 17 Dicembre 2023.

* * * * *

Il *Decreto* garantisce la protezione non solo alle persone che *segnalano* violazioni (la c.d. "*persona segnalante*", la quale - oltre alla segnalazione mediante canale interno o esterno - può denunciare all'autorità giudiziaria o contabile o divulgare pubblicamente informazioni sulle violazioni di cui è venuta a conoscenza nell'ambito del proprio contesto lavorativo), ma anche alle persone *segnalate c*ome autori delle violazioni, alle persone comunque menzionate (c.d. "*persone coinvolte*") – come *terzi* - nelle segnalazioni; alle persone terze che prendono comunque parte al processo [si pensi ai cosiddetti "*facilitatori*", che l'articolo 2, comma 1, lettera (h) del *Decreto* definisce come "*la persona fisica che assiste una persona segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata*") e alle persone a vario titolo collegate al segnalante (come ad esempio le persone legate al segnalante da uno stabile legame affettivo o i suoi parenti fino al quarto grado oppure i colleghi con i quali il segnalante ha un rapporto abituale e corrente). Sono protetti (anche se non propriamente "*persone*", anche "*gli enti di proprietà della persona segnalante*", cfr. art. 3, comma 5, lettera d del *Decreto*).

Quanto alle persone che *segnalano* violazioni è opportuno ricordare che laddove segnalino un illecito di cui loro stesse si sono macchiate, saranno comunque sanzionate, non esistendo una sorta di "salvacondotto", in questi casi, per chi denuncia. La Suprema Corte di Cassazione, nell'ordinanza 9148 del 31 Marzo 2023, ha difatti chiarito che: "*l'applicazione al dipendente di una sanzione per comportamenti illeciti suoi propri resta dunque al di fuori della copertura fornita dalla norma, che non esime da responsabilità chi commetta un illecito di-*

sciplinare per il solo fatto di denunciare la commissione del medesimo fatto o di fatti analoghi ad opera di altri dipendenti".

Perché i soggetti sopra menzionati devono godere di una speciale protezione? Nella gran parte dei casi, quei soggetti sono lavoratori del contesto pubblico o privato e dunque sono per definizione *soggetti deboli* o *vulnerabili,* stante lo squilibrio di forza contrattuale con il datore di lavoro (o la dipendenza economica dal medesimo).Tra l'altro, la condizione di *vulnerabilità* del lavoratore è persino accentuata nel sistema delle segnalazioni di violazione: si pensi alla specifica definizione del "*contesto lavorativo*" rilevante ai sensi del *Decreto* in esame ("*le attività lavorative o professionali, presenti o passate, svolte nell'ambito dei rapporti di cui all'articolo 3, commi 3 o 4, attraverso le quali, indipendentemente dalla natura di tali attività, una persona acquisisce informazioni sulle violazioni e nel cui ambito potrebbe rischiare di subire ritorsioni in caso di segnalazione o di divulgazione pubblica o di denuncia all'autorità giudiziaria o contabile*") oppure alla definizione di "*ritorsione*" ("*qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica e che provoca o può provocare alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto*").

Per quanto riguarda gli altri soggetti diversi dai lavoratori dipendenti (la tutela è difatti riconosciuta anche a lavoratori autonomi, liberi professionisti, consulenti, appaltatori, azionisti, persino volontari e tirocinanti) la *ratio* della protezione non solo è quella di evitare la "*ritorsione*" (definita come "*qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica e che provoca o può provocare alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto*") ma anche quella di rafforzare le garanzie per chi denuncia (tanto che il *Decreto*, rispetto alle norme in materia già esistenti, amplia la platea dei destinatari delle tutele), onde evitare che i segnalanti siano scoraggiati dal segnalare temendo conseguenze e penalizzazioni. In tale prospettiva, il *Decreto* riconduce a un testo normativo unitario e integrato la disciplina normativa già esistente sul *whistleblowing* nel settore pubblico e privato (con le norme in materia del TU Enti Locali 165/2001 e del d.lgs. 231/2001 che vengono abrogate) introducendo nuovi obblighi, nuove forme di segnalazione (si pensi al canale esterno di segnalazione da istituirsi presso l'ANAC, Autorità Nazionale Anticorruzione), etc.

§ 2. Le ricadute organizzative e tecniche *data protection* connesse alla istituzione del canale di segnalazione interno delle violazioni ai sensi dell'articolo 4 del Decreto whistleblowing.

I primi aspetti operativi di tipo *data protection* della disciplina 2023 sul *whistleblowing* si incontrano all'articolo 4 del *Decreto*. Nel disciplinare l'attivazione del canale di segnalazione interno che tutti i soggetti pubblici e privati devono istituire (sentite le organizzazioni sindacali), è previsto che:

- la riservatezza dell'identità della persona segnalante;

- la riservatezza dell'identità della persona coinvolta;
- la riservatezza dell'identità della persona comunque menzionata nella segnalazione;
- la riservatezza del contenuto della segnalazione e della relativa documentazione.

siano adeguatamente tutelate mediante l'adozione (nei flussi di comunicazione tramite il canale di segnalazione interna) di "*strumenti di crittografia*". Viene cioè richiamata proprio una delle misure di sicurezza nel trattamento che l'articolo 32 del Regolamento Generale UE sulla protezione dei dati personali n. 679/2016 elenca come fondamentali nell'ambito dell'approccio *risk based* che permea la disciplina del GDPR. L'adozione della crittografia è adeguata a proteggere il carattere riservato del segnalante e della segnalazione, la quale – quando effettuata in forma scritta – può essere svolta, difatti, anche con "*modalità informatiche*".

Ovviamente, non è solo tale aspetto specifico di *security* che mette in diretta relazione la disciplina sulla protezione dei dati personali con quella sulla gestione delle segnalazioni delle violazioni: l'attivazione del canale di segnalazione interno – difatti – andrà "costruita" nel rispetto dei principi fondamentali del trattamento (cfr. art. 5 del Regolamento 679/2016) nonché in un'ottica di *privacy by design* (cfr. art. 25 Reg. 679/2016) ponendosi la normativa rilevante in materia di protezione dei dati personali quale vero e proprio presidio-presupposto dell'intero impianto normativo sul *whistleblowing*.

Altro aspetto che vede la *compliance data protection* quale presupposto di liceità della disciplina della segnalazione di violazioni emerge dalla lettura dell'articolo 4, comma 2, del *Decreto.* Tale norma prescrive che la gestione del canale di segnalazione interno venga affidata a una persona o a un ufficio interno autonomo dedicato e con personale specificamente formato per la gestione del canale oppure ad un soggetto esterno anch'esso autonomo e con personale specificamente formato. Tale disposizione va letta in combinato disposto con gli articoli 29 e 32, comma 4 del Regolamento 679/2016 sulle cosiddette "*persone autorizzate al trattamento dei dati personali*" e 2-*quaterdecies* del Codice della privacy (che prevede che specifici compiti e funzioni connessi al trattamento di dati personali – come appunto la gestione del canale interno di segnalazione, nel caso del *Decreto* – possano essere attribuiti a persone fisiche, espressamente designate e autorizzate, che operano sotto la autorità del titolare o del responsabile del trattamento). Dunque, l'accesso (ai dati del segnalante e della segnalazione) sarà lecito non solo se effettuato da personale "*specificatamente formato*" (evidentemente sugli aspetti procedurali, tecnici e di sicurezza del sistema di gestione delle segnalazioni interno attivato, come ad esempio quelli elencati all'articolo 5 del *Decreto* - ma – è conseguente – anche sugli specifici aspetti inerenti alla tutela e sicurezza dei dati oggetto di trattamento, in base alla normativa vigente), ma anche dotato di specifica autorizzazione *data protection* e con precise istruzioni che definiscano l'ambito del trattamento consentito alla luce delle due discipline normative (*whistleblowing* e *data protection*) sul punto convergenti. Sarà dunque necessario integrare – alla luce del *Decreto* – le istruzioni eventualmente già conferite alle *persone autorizzate* o ai *soggetti designati* ai sensi degli articoli 29, 32, comma 4 Reg. 679/2016 e 2-*quatrerdecies* del Codice della privacy (norme - tra l'altro – tutte nello specifico richiamate proprio dall'articolo 12 del *Decreto* in merito agli aspetti operativi dell'obbligo di riservatezza ivi disciplinato), ove a tali soggetti siano affidati incarichi di ge-

stione del canale di segnalazione interno ai sensi dell'art. 4, comma 2 del *Decreto*. Una sorta di linea-guida sul contenuto delle istruzioni può essere tratta dal l'elenco dei compiti affidati al gestore del canale ai sensi dell'articolo 5 del *Decreto*. Ed è anche necessario, prima dell'affidamento dell'incarico, verificare la "*specifica formazione*" aggiornata degli interessati. Gli aspetti organizzativi *data protection* segnalati con riferimento alle istruzioni e autorizzazioni da conferire a chi accede ai dati personali degli interessati per gestire il canale di segnalazione interno, valgono anche - per i soggetti pubblici – nel caso in cui tale gestione debba essere affidata al *responsabile della prevenzione della corruzione e della trasparenza*, di cui all'articolo 1, comma 7, della legge 6 novembre 2012, n. 190.

Appare poi il caso di precisare che laddove il soggetto pubblico o privato decidano di avvalersi di un "*soggetto esterno, anch'esso autonomo e con personale specificamente formato*" per la gestione del canale di segnalazione interno, il riferimento del legislatore al carattere di *autonomia* non qualifica tale ente esterno come *titolare del trattamento*: non appare difatti lasciata all'ente esterno alcuna facoltà decisionale autonoma in merito alle finalità e ai mezzi essenziali del trattamento (propria invero del soggetto appaltante, in caso) e dunque è probabile, anche alla luce dei criteri di cui alle *Linee Guida 7/2020 sul concetto di titolare e responsabile nel Regolamento 679/2016* del Comitato europeo per la protezione dei dati personali, che l'ente esterno vada qualificato *responsabile del trattamento* (con proprio margine di discrezionalità sulla scelta dei *mezzi non essenziali*, come ad esempio le misure di sicurezza nel trattamento) ai sensi dell'articolo 28 del Regolamento 679/2016. Sarà dunque il "*contratto o altro atto giuridico*" (e le istruzioni specifiche sul trattamento da allegarsi) la idonea sede documentale per la disciplina di tutti gli aspetti inerenti ai trattamenti di cui al *Decreto* in esame (es: adozione della crittografia per il canale di segnalazione; garanzie di formazione del personale dell'ente esterno, etc. oltre alle garanzie *data protection* specifiche previste all'articolo 28 Reg. 679/2016 – tra l'altro specificatamente richiamato dall'articolo 13, comma 6, del *Decreto* - come ad esempio le "*garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessato*").

Vi è infine anche il caso in cui la segnalazione possa essere ricevuta da un soggetto diverso da quello competente/affidatario della gestione del canale di comunicazione interna. In tali ipotesi, onde evitare trattamenti illeciti di dati personali, tale soggetto potrà lecitamente trattare i dati (senza accedere al contenuto della segnalazione, deve ritenersi) solo per il tempo necessario alla trasmissione della segnalazione erroneamente ricevuta al soggetto competente (dando contestuale notizia della trasmissione alla persona segnalante), che l'articolo 4, comma 6, del Decreto qualifica in "*sette giorni*". Anche questa ipotesi di trattamento provvisoriamente lecito dei dati deve essere inquadrata in un quadro di *compliance data protection*, nel senso che i soggetti pubblici o privati dovranno prevederla e disciplinarla nell'ambito delle istruzioni sul trattamento dei dati personali conferite alle persone autorizzate ai sensi delle già richiamate disposizioni di cui agli articoli 29 e 32, comma 4 del Regolamento 679/2016.

* * * * *

Una delle novità introdotte dal *Decreto* whistleblowing riguarda la possibilità di effettuare segnalazioni di violazione anche attraverso un *canale esterno* (cfr. art. 6) attivato dall'Autorità Nazionale Anticorruzione – ANAC (cfr. art. 7), tenuta alle identiche modalità di gestione del canale e agli stessi impegni alla riservatezza su segnalante, segnalati e segnalazione che abbiamo appena analizzato per il canale di segnalazione interno (in ogni caso, l'ANAC, sentito il Garante per la protezione dei dati personali, emanerà entro tre mesi dalla entrata in vigore del *Decreto* specifiche linee guida sulla gestione ed operatività del canale di segnalazione esterno, nel rispetto dei principi di tutela della riservatezza, cfr. art. 10 del *Decreto*).

La persona segnalante può presentare la segnalazione esterna solo al ricorrere di precise condizioni, come le seguenti:

1. al momento della sua presentazione non è prevista, nell'ambito del suo *contesto lavorativo*, l'attivazione obbligatoria del canale di segnalazione interna ovvero questo, anche se obbligatorio, non è attivo o, anche se attivato, non è conforme a quanto previsto dall'articolo 4;
2. la persona segnalante ha già effettuato una segnalazione interna e la stessa non ha avuto seguito;
3. la persona segnalante ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione possa determinare il rischio di ritorsione;
4. la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

§ 3. Obbligo di riservatezza ai sensi dell'articolo 12 del Decreto whistleblowing: aspetti organizzativi e il consenso dell'interessato.

L'articolo 12 del Decreto, rubricato "*Obbligo di riservatezza*", introduce le prescrizioni specifiche a tutela della riservatezza della identità della persona segnalante. La violazione di tali obblighi è punita con l'applicazione da parte dell'ANAC di una sanzione da 10 a 50 mila euro.

Intanto, una prima forma di protezione deriva dalla previsione di specifici limiti ai tempi di conservazione dei dati della segnalazione, essendo ovvio che più sono lunghi tali termini, maggiore può divenire il rischio di identificazione del segnalante. E in effetti, l'articolo 12, comma 1, del *Decreto*, nel prevedere che le segnalazioni non possono essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse, fissa un criterio generale che è una sorta di applicazione settoriale del principio fondamentale di *limitazione dei tempi di conservazione* di cui all'articolo 5, comma 1, lettera (e) del Regolamento 679/2016 ("*i dati personali possono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati*").

Certo, l'articolo 14 del D*ecreto* individua anche un termine *massimo* di conservazione ("*le segnalazioni, interne ed esterne, e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione*").

Ci si trova allora di fronte a due diversi termini di conservazione dei dati:

- da un lato, il termine di cui all'articolo 12 del *Decreto*, che non è un vero e proprio termine, quanto un criterio di individuazione dei limiti massimi di conservazione delle segnalazioni, rappresentato dalla necessità di espletare definitivamente tutte le esigenze connesse alla gestione e definitiva evasione della segnalazione ricevuta;
- dall'altro, il termine quinquennale specifico previsto all'articolo 14 del *Decreto* (compatibile anche con la durata media del termine prescrizionale dei principali illeciti suscettibili di verificarsi) che va tuttavia letto in subordine al primo, nel senso che tale norma riafferma in primo luogo che le segnalazioni, interne ed esterne, e la relativa documentazione sono conservate *per il tempo necessario al trattamento della segnalazione*, e la possibilità *("comunque")* del termine massimo di conservazione per cinque anni – una volta comunicato l'esito finale della procedura di segnalazione - va letta nel limite del "*rispetto degli obblighi di riservatezza di cui all'articolo 12*", e dunque la conservazione dei dati (successiva alla definizione della procedura di segnalazione) "*non oltre cinque anni"* potrà fondarsi, in coerenza con il principio di limitazione di cui all'articolo 5, comma 1, lettera (e) del Reg. 6790/20916 (non a caso richiamato nello specifico dall'articolo 14 del *Decreto*) solo ove i soggetti pubblici e privati abbiano in essere una specifica procedura di *data retention* che garantisca, tra l'altro:
    - la tutela della riservatezza della identità del segnalante (e anche delle altre persone), ad esempio conservando (nell'eventuale periodo quinquennale ammesso) dati anonimizzati o pseudonimizzati;
    - la speditezza delle procedure di gestione delle segnalazioni ricevute, onde chiarire agli interessati in maniera trasparente la prevedibile o presumibile durata della procedura di segnalazione, quanto alla sua gestione e comunicazione del definitivo esito;
    - chiare modalità di cancellazione dei dati una volta comunicato l'esito definitivo della procedura di segnalazione (salva la conservazione a termini di altre norme di legge dei documenti che li contengono);
    - la previsione di modalità operative di applicazione *by design* del *principio di limitazione dei tempi di conservazione dei dati personali*, anche ai sensi del paragrafo 3.7 delle *Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita* del Comitato europeo per la protezione dei dati personali.

* * * * *

Sempre in tema di obblighi di riservatezza, l'articolo 12, comma 2 del *Decreto* prescrive il principio generale che l'identità della persona segnalante e qualsiasi altra informazione da cui possa evincersi, direttamente o indirettamente, tale identità non possono essere rivelate, senza il *consenso espresso* della stessa persona segnalante, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni (che ovviamente non necessitano di alcun consenso) e che - come detto - devono essere espressamente autorizzate a trattare tali dati ai sensi degli articoli 29 e 32, comma 4, del Regolamento 679/2016 e dell'articolo 2-quaterdecies del Codice della privacy. Sulla natura di questo consenso, quando prestato dai lavoratori dipendenti segnalanti di soggetti pubblici o privati, può osservarsi che non sembrerebbero applicarsi in questo caso i principi generali in base ai quali i *soggetti vulnerabili* non possono prestare un consenso valido, in quanto la loro posizione di "debolezza" priverebbe il consenso delle caratteristiche di libertà e coartazione per le quali non potrebbe essere validamente reso. Ma in tale ipotesi, la decisione della persona segnalante di acconsentire espressamente e consapevolmente alla comunicazione della sua identità e degli altri dati riservati avviene su un piano di parità con la controparte interessata, che è la persona segnalata.

Vi sono alcuni casi in cui la norma costruisce come assoluto il divieto di comunicare l'identità della persona segnalante: è il caso, ad esempio, del procedimento disciplinare in cui la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa.

In altri casi, invece, il consenso espresso della persona segnalante alla rivelazione della sua identità è scriminante, come nelle ipotesi di contestazione disciplinare che sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa dell'incolpato. In tale specifico caso vi è un obbligo di trasparenza rafforzato, rappresentato dall'obbligo (da adempiersi a carico di chi non è chiaro, anche se provvederà probabilmente uno specifico soggetto autorizzato ai sensi dell'articolo 4, comma 2, del *Decreto*) di avvisare la persona segnalante "*mediante comunicazione scritta delle ragioni della rivelazione dei dati riservati*" alla luce della indispensabilità "*ai fini della difesa della persona coinvolta*".

§ 4. I principi generali del trattamento dei dati personali per finalità di gestione delle procedure di segnalazione delle violazioni di cui all'articolo 13 del Decreto whistleblowing.

L'articolo 13 del Decreto, rubricato in via generale "*Trattamento dei dati personali*", fissa i precisi rapporti tra disciplina *whistleblowing* e *data protection* complessivamente considerata, costituendo quest'ultima il presupposto di legittimità dei trattamenti nell'ambito delle procedure previste; la regola generale è appunto che ogni trattamento dei dati personali, compresa la comunicazione tra le autorità competenti, previsto dal *Decreto* deve essere effettuato in conformità al Regolamento 679/2016, al Codice della privacy, al decreto legislativo sul trattamento dei dati personali nell'ambito delle attività giudiziarie e di polizia (per le denunce) ai sensi del d.lgs. 51/2018 attuativo della direttiva UE 2016/680. Inoltre, la comunicazione di dati personali da parte delle istituzioni, degli organi o degli organismi dell'Unione europea

deve svolgersi nel quadro normativo di cui al Regolamento (UE) 2018/1725 sulla protezione dei dati personali in tale contesto.

L'articolo 13, comma 2, applica al contesto *whistleblowing* una serie di principi fondamentali del trattamento, e precisamente i principi pertinenza, esattezza, proporzionalità e non eccedenza dei dati. È difatti previsto che i dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente. Questo implica che nella corretta impostazione *data protection* delle politiche del trattamento connesse alla gestione delle procedure di segnalazione, le persone autorizzate (che – lo si ricordi – devono essere autorizzate e adeguatamente formate e informate) dovranno ricevere specifiche istruzioni e dovranno essere in grado di valutare quali dati siano utili/da conservare e inutili/da cancellare *immediatamente*, all'atto della ricezione della segnalazione. Una valutazione che - senza dubbio -assume particolare delicatezza e che non può essere affidata se non persone che sotto questo profilo forniscono adeguate garanzie (ancora maggiori se la gestione del canale di comunicazione delle segnalazioni è affidata a soggetto autonomo esterno e al personale di questo).

L'articolo 13, comma 3, raccorda per completezza ordinamentale, l'articolo 2-*undecies* del Codice della privacy con il *Decreto*. L'articolo 2-undecies (*Limitazioni ai diritti dell'interessato*) prevede che i diritti di cui agli articoli da 15 a 22 del Regolamento 679/2016 (accesso, rettifica, cancellazione, etc) non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo amministrativo al Garante ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto – tra l'altro – "*alla riservatezza dell'identità della persona che segnala violazioni di cui sia venuta a conoscenza in ragione del proprio rapporto di lavoro o delle funzioni svolte, ai sensi del decreto legislativo recante attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione, ovvero che segnala violazioni ai sensi degli articoli 52-bis e 52-ter del decreto legislativo 1° settembre 1993, n. 385, o degli articoli 4-undecies e 4-duodecies del decreto legislativo 24 febbraio 1998, n.* 58». [la nuova formulazione dell'articolo 2-*undecies*, comma 1, lettera (f) del Codice della privacy è stata appunto inserita proprio dall'articolo 24 del Decreto in esame].

In questi casi, dunque, al fine di salvaguardare la riservatezza dell'identità della persona che segnala violazioni, l'esercizio dei diritti potrà essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'interessato (e a meno che la comunicazione possa compromettere la finalità della limitazione) per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato.

In questa opera di raccordo tra limitazione dei diritti finalizzata a tutelare l'identità della persona segnalante e possibilità, a certe condizioni, di esercitarli, sembra mancare uno specifico coordinamento operativo tra Decreto whistleblowing e quanto previsto dall'articolo 2-undecies, comma 3, del Codice della privacy laddove prevede che nei casi di limitazione i diritti dell'interessato possono essere esercitati anche tramite il Garante con le modalità di cui

all'articolo 160 del Codice, dovendo tra l'altro il titolare del trattamento informare l'interessato (es: la persona segnalata) delle facoltà prevista dalla citata norma.

Una possibile criticità esegetica può derivare dalla previsione dell'articolo 13, comma 4 del *Decreto* che chiarisce la corretta individuazione dei "*soggetti di cui all'articolo 4*" quali titolari del trattamento dei dati personali relativi al ricevimento e alla gestione delle segnalazioni, tenuti a specifici obblighi di osservanza generale della normativa *data protection*, di trasparenza informativa, di impostazione *by design* dei sistemi di segnalazione, etc.

Chi sono "*soggetti di cui all'articolo 4*" del *Decreto?* La domanda è legittima, visto che tale norma menziona non solo "*i soggetti del settore pubblico e i soggetti del settore privato*" che attivano canali di segnalazione (ovvi titolari del trattamento) ma anche le persone *interne autonome e* dedicate alla gestione del canale di segnalazione, o i *soggetti esterni,* anch'essi autonomi. È possibile che i soggetti interni o esterni "autonomi" siano tali in quanto deputati a prendere decisioni sulle finalità e sui mezzi del trattamento, qualificandosi dunque come autonomi titolari, come poi codificato all'articolo 13 del *Decreto*? Si pensi - ad esempio - ai componenti dell'Organismo di Vigilanza da istituirsi ai sensi del d.lgs. 231/2001 la cui soggettività *data protection* il Garante per la protezione dei dati personali ebbe a chiarire in un parere del 2020, qualificando i componenti dell'OdV come persone autorizzate al trattamento e non l'OdV come autonomo titolare del trattamento. Chi scrive ritiene che la qualifica di titolari del trattamento riconosciuta dall'articolo 13 del Decreto "*soggetti di cui all'articolo 4*" non possa essere estesa a soggetti diversi dai *i soggetti del settore pubblico e i soggetti del settore privato*" che attivano canali di segnalazione. Ciò perché il Decreto prescrive chiaramente (cfr. art. 12, comma 2) che le "*persone competenti a ricevere o a dare seguito alle segnalazioni*" (quindi quei soggetti interni o esterni, uffici autonomi con personale dedicato e preparato) non possono che essere "*persone espressamente autorizzate ai sensi degli articoli 29 e 32, comma 4, del Regolamento 679/2016"* (o soggetti designati ai sensi dell'articolo 2-*quaterdecies* del Codice della privacy). E inoltre, come insegnano le *Linee Guida EDPB 7/2020 sui concetti di titolare e responsabile nel Regolamento 679/2016*, la titolarità autonoma del trattamento non può essere riconosciuta ad articolazione interne, ancorché autonome, di un'entità che nel suo complesso è il titolare del trattamento. Infine, le ipotesi di contitolarità del trattamento previste all'articolo 13, comma 5, del *Decreto* e l'obbligo di stipulare il noto accordo di riparto interno delle responsabilità tra contitolari ai sensi dell'articolo 26 del Regolamento 679/2016 sono disciplinate con chiaro ed esclusivo riferimento ai "*soggetti del settore pubblico e i soggetti del settore privato che condividono risorse per il ricevimento e la gestione delle segnalazioni*" e non vengono menzionati anche agli altri soggetti pure l'articolo 4 elenca. Se ne deve concludere, dunque, che la qualificazione della titolarità del trattamento effettuata all'articolo 13, comma 4 del *Decreto* sia sostanzialmente tautologica, essendo generale applicazione di principi già noti.

L'articolo 13, comma 6 del Decreto prescrive infine ai soggetti pubblici e privati di definire il proprio modello di ricevimento e gestione delle segnalazioni interne, individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, sulla base di una valutazione d'impatto sulla protezione dei dati.

§ 5. Conclusioni: i nuovi scenari conseguenti alle segnalazioni aventi ad oggetto le specifiche violazioni della normativa sulla protezione dei dati personali.

Concludendo la disamina specifica degli aspetti *data protection* del *Decreto whistleblowing*, appare opportuno formulare, in particolare, due considerazioni conclusive.

La prima: diviene ancora più rilevante la corretta impostazione della *compliance* delle politiche del trattamento presso titolari del trattamento pubblici e privati, poiché con la nuova disciplina introdotta dal *Decreto* la segnalazione potrà riguardare proprio le violazioni delle disposizioni nazionali e dell'Unione in materia di protezione dei dati personali (considerate tra le materie che rientrano nell'"*interesse pubblico*" - cfr. Allegato al Decreto, lettera J - leso da "*comportamenti, atti o omissioni*" in cui consistono le "*violazioni*" oggetto della segnalazione,).

E tale scenario è tanto più delicato se si considera che la segnalazione può avvenire con tutela della riservatezza della propria identità di segnalante, prima non garantita per eventuali segnalazioni di violazioni *data protection*, e può essere effettuata anche come segnalazione esterna all'ANAC (si pensi ai casi in cui una segnalazione interna su violazioni *data protection* non abbia sortito alcun effetto).

La seconda considerazione attiene alla previsione dell'articolo 20 del *Decreto* che prevede la non punibilità in nessuna sede civile o amministrativa per la rivelazione o diffusione di informazioni sulle violazioni relative alle disposizioni sulla protezione dei dati personali, anche nel caso in cui la persona che rivela o diffonde abbia acquisito i dati o avuto accesso alle informazioni e ai dati - poi rivelati o diffusi - in maniera non conforme (es: accesso ad email del terzo, ricezione di dati e informazioni per errore, senza essere il destinatario previsto, etc).

La non punibilità in sede civile e amministrativa si estende anche a ogni altra ipotesi di "*ulteriore*" responsabilità (dunque per profili civilistici o amministrativi non strettamente inerenti all'atto di rivelare o diffondere) mentre non si estende alla responsabilità penale, ed è comunque legata alle seguenti condizioni:

- al momento della rivelazione o diffusione, devono esservi fondati motivi per ritenere che la rivelazione o diffusione delle stesse informazioni sia necessaria per svelare la violazione;
- l'acquisizione delle informazioni e l'accesso ai dati poi rivelati o diffusi non devono costituire reato (si pensi all'articolo 167 del Codice della privacy e al reato di *trattamento illecito dei dati personali*, contraddistinto da dolo di profitto o di danno);
- al momento della segnalazione o della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica, la persona segnalante o denunciante aveva fondato motivo di ritenere che le informazioni sulle violazioni segnalate, divulgate pubblicamente o denunciate fossero vere e rientrassero nell'ambito oggettivo del Decreto;
- la persona segnalante ha previamente effettuato una segnalazione interna ed esterna, ma non ha ricevuto riscontro nei termini;

- la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;
- la persona segnalante ha fondato motivo di ritenere che la segnalazione esterna possa comportare il rischio di ritorsioni o possa non avere efficace seguito in ragione delle specifiche circostanze del caso concreto.

Va anche notato che la persona può anche diffondere i dati e le informazioni, mediante lo specifico atto di "*divulgare pubblicamente*" (cfr. art. 20, comma 1, del *Decreto*) che l'articolo 2, comma 1, lettera (f) del medesimo *Decreto* qualifica come il "*rendere di pubblico dominio informazioni sulle violazioni tramite la stampa o mezzi elettronici o comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone*". Una definizione che ricorda molto da vicino quella contenuta all'articolo 2-*ter*, coma 4 del Codice della privacy, relativa a una delle operazioni di trattamento più delicate, rappresentato dalla "*diffusione*" dei dati personali ("*il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione*").

In ogni caso, la responsabilità penale e ogni altra responsabilità, anche di natura civile o amministrativa, non è esclusa per i comportamenti, gli atti o le omissioni non collegati alla segnalazione, alla denuncia all'autorità giudiziaria o contabile o alla divulgazione pubblica o che non sono strettamente necessari a rivelare la violazione.