Dicembre 2019

La nuova direttiva europea in materia di *whistleblowing*

Antonio Carino, Partner, Giampiero Falasca, Partner, DLA Piper

1. Premessa

Il 26 novembre scorso è stata pubblicata in Gazzetta Ufficiale la Direttiva (UE) 2019/1937 "*riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione*"[1] (di seguito la "Direttiva") il cui scopo è quello di stabilire norme minime comuni volte a garantire un elevato livello di protezione delle persone che segnalano violazioni del diritto dell'Unione in specifici settori.

La Direttiva – adottata al termine di un lungo processo decisionale promosso da ONG, sindacati e organizzazioni internazionali – risponde all'esigenza di fornire ai segnalanti (o *whistleblowers*) una tutela uniforme in tutti gli Stati membri e armonizzata tra i vari settori, introducendo regole comuni che impongano l'adozione di canali di segnalazione efficaci, riservati e sicuri e, al tempo stesso, garantiscano una protezione efficace degli informatori da possibili ritorsioni.

2. Il *whistleblowing* nel panorama normativo italiano

La materia del *whistleblowing* è attualmente disciplinata in Italia dalla Legge 30 novembre 2017, n. 179, cui si sono affiancate varie norme di settore.[2] La L. 179/2017 si compone di tre articoli: il primo, dedicato alla tutela del dipendente pubblico che segnala

[1] Gli Stati membri hanno tempo, rispettivamente, fino al 17 dicembre 2021 per recepire le disposizioni necessarie per conformarsi al nuovo testo legislativo e – per quanto riguarda gli enti privati con più di 50 e meno di 250 dipendenti – fino al 17 dicembre 2023 per adeguarsi alle disposizioni legislative, regolamentari e amministrative necessarie per conformarsi all'obbligo di stabilire un canale di segnalazione interno.

[2] Si vedano i seguenti testi legislativi:

- il D.Lgs. 12 maggio 2015, n. 72 che ha introdotto nel Testo Unico Bancario l'obbligo per le banche di adottare due canali di segnalazione delle violazioni, uno interno e uno esterno;
- il D.Lgs. 25 maggio 2017, n. 90 che ha introdotto nel decreto antiriciclaggio una disciplina *ad hoc* per le segnalazioni, stabilendo delle garanzie di tutela per il segnalante e prevedendo un apposito canale di comunicazione;
- il D.Lgs. 3 agosto 2017, n. 129 che, relativamente al settore della *market abuse*, ha introdotto nel Testo Unico della Finanza due norme inerenti, rispettivamente, il c.d. *whistleblowing* interno e *whistleblowing* esterno;
- il D.Lgs. 21 maggio 2018, n. 68 che ha disciplinato l'istituto nel settore assicurativo.

illeciti; il secondo, dedicato alla tutela del dipendente o del collaboratore che segnala illeciti nel settore privato, ha introdotto nell'art. 6 del D.Lgs. 2 giugno 2001, n. 231 (di seguito "Decreto") un apparato di misure dedicate al *whistleblower* nel settore privato e, infine, il terzo relativo all'obbligo di segreto d'ufficio, professionale, scientifico o aziendale.

Con riferimento al settore privato, la L. 179/2017 ha disposto che i Modelli di organizzazione e di gestione (di seguito "Modelli") adottati per prevenire la commissione dei reati prevedano uno o più canali che consentano ai soggetti di cui all'art. 5, comma 1, lett. a) e b) del Decreto, c.d. apicali e sottoposti, di presentare segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del Decreto e fondate su elementi di fatto precisi e concordanti, o violazioni dei Modelli di cui il segnalante sia venuto a conoscenza in ragione delle funzioni svolte; tutto ciò garantendo la riservatezza dell'identità del *whistleblower* nelle attività di gestione della segnalazione.

La circostanza che la disciplina del *whistleblowing* sia stata inserita nell'ambito del Decreto implica che i destinatari della stessa siano solo gli enti a cui si applica la normativa sulla responsabilità amministrativa degli enti. Inoltre, stante la funzione dei Modelli come esimente per la responsabilità della società e la conseguente non obbligatorietà della loro adozione, le tutele previste dalla L. 179/2017 potranno trovare applicazione solo se la società di segnalazione ha adottato un Modello e, di conseguenza, un sistema di segnalazioni. Quanto ai soggetti tutelati, la norma fa espresso riferimento all'art. 5 del Decreto, che identifica un ambito sostanzialmente circoscritto al personale dell'ente, con l'eccezione dei soggetti dotati di poteri di rappresentanza, dei collaboratori e di coloro che anche di fatto svolgono il controllo dell'ente.

Quanto ai requisiti di operatività di tali sistemi, la L. 179/2017 impone l'adozione di canali di segnalazione che garantiscano la riservatezza dell'identità del segnalante e almeno uno dei quali consenta di effettuare segnalazioni con modalità informatiche. Oltre al divieto di atti di ritorsione o discriminatori nei confronti del *whistleblower*, per motivi collegati, direttamente o indirettamente, alla segnalazione, i Modelli devono stabilire adeguate sanzioni nei confronti di chi violi le misure di tutela del segnalante e di chi effettui (con dolo o colpa grave) segnalazioni che si rivelino infondate.

3. La nuova Direttiva

3.1. L'ambito di applicazione

Il *whistleblower* è definito come la persona fisica che segnala o divulga informazioni sulle violazioni acquisite nell'ambito delle sue attività professionali, a prescindere dalla natura di tali attività o del fatto che il rapporto di lavoro sia nel frattempo terminano o non ancora iniziato (per esempio nel caso in cui le informazioni siano acquisite durante il processo di selezione o in fase di trattativa precontrattuale).

Nello specifico, rientrano tra i segnalanti tutelati dalla Direttiva le persone aventi la qualifica di "lavoratori" ai sensi dell'art. 45 TFUE, ossia le persone che nel settore privato come in quello pubblico forniscono, per un certo periodo di tempo, a favore di terzi e sotto la direzione di questi, determinate prestazioni verso il corrispettivo di una retribuzione. La protezione deve, quindi, essere concessa anche ai lavoratori con contratti atipici, quali quello a tempo parziale e a tempo determinato, nonché a chi ha un contratto o un rapporto di lavoro con un'agenzia interinale, ai tirocinanti e ai volontari. Le medesime tutele dovrebbero, altresì, essere applicate a lavoratori autonomi, consulenti, subappaltatori e fornitori esposti a ritorsioni quali la risoluzione o l'annullamento del contratto di servizi, della licenza o del permesso, il boicottaggio o l'inserimento in liste nere. Sono, infine, tutelati gli azionisti e le persone negli organi direttivi che potrebbero subire ritorsioni in termini finanziari o danni alla reputazione.

La Direttiva introduce una protezione dalle misure ritorsive non solo dirette, ma anche indirette ed estende le medesime tutele anche ai c.d. "facilitatori", ossia a coloro che assistono i segnalanti nel processo di segnalazione, nonché a terzi eventualmente connessi ai *whistleblowers*, quali colleghi o parenti. La ritorsione indiretta comprende, inoltre, le misure che possono essere intraprese contro il soggetto giuridico di cui il segnalante sia proprietario, per cui lavori o a cui sia altrimenti connesso, quali l'annullamento della fornitura di servizi o il boicottaggio.

Le tutele previste dal nuovo testo legislativo trovano applicazione in tutti i casi in cui vengano segnalate violazioni del diritto dell'Unione, definite come atti od omissioni illecite ovvero che vanificano l'oggetto e le finalità di norme dell'Unione relative agli specifici settori individuati nell'allegato alla Direttiva, relativi a settori quali gli appalti pubblici, la prevenzione del riciclaggio e del finanziamento del terrorismo, la sicurezza dei prodotti, la tutela dell'ambiente e la salute pubblica.

Le tutele previste dalla Direttiva sono concesse nel caso in cui siano segnalate violazioni già commesse o non ancora commesse (ma che molto verosimilmente potrebbero esserlo), atti od omissioni che il segnalante abbia fondati motivi di ritenere violazioni, nonché tentativi di nascondere violazioni. Sono, tuttavia, stabiliti alcuni specifici requisiti per poter accedere alle tutele. Innanzitutto, il segnalante deve avere ragionevoli motivi, alla luce delle circostanze e delle informazioni di cui dispone al momento della segnalazione, per ritenere che i fatti che segnala siano veri. Tale requisito, garantendo che chi fornisce deliberatamente informazioni errate o fuorvianti sia escluso dalla protezione e che, al contrario, possa beneficiare delle tutele chi effettua una segnalazione imprecisa in buona fede, si pone come una garanzia essenziale contro le segnalazioni dolose, futili o infondate. Inoltre, è necessario che il segnalante abbia fondati motivi per ritenere che le informazioni segnalate rientrino nell'ambito di applicazione della Direttiva stessa.

3.2 I canali di segnalazione

Uno dei punti più controversi della proposta inizialmente presentata dalla Commissione Europea era la previsione di un processo trifasico: per poter godere delle tutele previste

dalla Direttiva, i segnalanti dovevano, in primo luogo, utilizzare i canali interni; se questi non funzionavano o non avevano possibilità di successo, dovevano rivolgersi alle autorità esterne e, solo come ultima possibilità, potevano rendere le informazioni di dominio pubblico. In fase di approvazione, il meccanismo, tuttavia, è stato modificato e ai *whistleblowers* è ora riconosciuta la facoltà di scegliere il canale che ritengono più appropriato, anche se la divulgazione al pubblico è ancora soggetta ad alcune condizioni.

La Direttiva impone l'obbligo di istituire canali di segnalazione interni a tutte le imprese con almeno 50 lavoratori, indipendentemente dalla natura delle loro attività, in funzione del loro obbligo di riscuotere l'IVA, nonché a tutti i soggetti giuridici del settore pubblico, compresi quelli di proprietà o sotto il controllo degli stessi. L'esenzione delle piccole e medie imprese da tale obbligo non si applica, tuttavia, ai soggetti che operano nel settore dei servizi finanziari esposti a rischio di riciclaggio e finanziamento del terrorismo che, pertanto, dovranno istituire canali di segnalazione interni indipendentemente dalle loro dimensioni. Inoltre, a seguito di un'opportuna valutazione del rischio, è riconosciuta agli Stati membri la facoltà di esigere che anche società con un numero di dipendenti inferiore istituiscano canali di segnalazione interna in casi specifici, per esempio a causa dei notevoli rischi che possono derivare dalle loro attività.

Quanto alle modalità di implementazione di tali canali, la Direttiva impone una serie di requisiti che gli enti devono rispettare, riconoscendo, al tempo stesso, che spetti comunque a ciascun soggetto definire il tipo di canale da istituire. Nello specifico le procedure per le segnalazioni devono prevedere che i canali per ricevere le segnalazioni siano progettati, realizzati e gestiti in modo sicuro e tale da garantire la riservatezza dell'identità del segnalante, nonché di eventuali terzi citati nella segnalazione. Al *whistleblower* deve essere consentito di segnalare per iscritto e di trasmettere le segnalazioni per posta, mediante cassetta per i reclami o piattaforma online o di segnalare oralmente mediante linea telefonica gratuita o altro sistema di messaggistica vocale, o entrambi. Inoltre, su richiesta del segnalante, deve essere possibile effettuare segnalazioni mediante incontri di persona con i soggetti incaricati. La Direttiva impone, altresì, ai soggetti l'obbligo di rispettare determinate tempistiche: entro sette giorni il segnalante deve ricevere una avviso circa il ricevimento della segnalazione stessa e le procedure devono prevedere un termine ragionevole (non superiore a tre mesi) per dare un riscontro alla segnalazione.

I canali di segnalazione possono essere gestiti internamente da una persona o da un servizio designato a tal fine o essere messi a disposizione esternamente da terzi, purché offrano adeguate garanzie di indipendenza, riservatezza, protezione dei dati e segretezza. È, inoltre, necessario che sia designata una persona o un servizio imparziale competente per dare seguito alle segnalazioni, che potrebbe essere la stessa persona o lo stesso servizio che riceve le segnalazioni e che manterrà la comunicazione con il segnalante.

La Direttiva riconosce che uno dei fattori col maggior effettuo dissuasivo su potenziali segnalanti è la mancanza di informazioni circa l'opportunità di presentare una

segnalazione, le modalità e i tempi della stessa. Pertanto, è fatto obbligo ai soggetti che hanno predisposto le procedure di fornire informazioni sulle stesse nonché sulle procedure per la segnalazione esterna alle autorità competenti.

Infine, è necessario conservare la documentazione relativa a tutte le segnalazioni, nonché assicurare che ogni segnalazione sia consultabile e che le informazioni ricevute possano, se del caso, essere utilizzate come elementi di prova. Pertanto, nel caso di segnalazione telefonica o nei casi in cui il segnalante abbia richiesto un incontro di persona, deve potersi procedere a registrare la conversazione su un supporto durevole che consenta l'accesso alle informazioni o a trascrivere in modo completo e accurato la conversazione.

Quanto alle segnalazioni esterne, i *whistleblowers* possono segnalare violazioni alle autorità identificate dagli Stati membri, nonché a quelle competenti a livello europeo. Tali enti devono, pertanto, implementare canali di segnalazioni indipendenti e autonomi e incaricare appositi dipendenti a ricevere e dare seguito alle segnalazioni. Infine, la Direttiva riconosce la possibilità di effettuare divulgazioni pubbliche in alcuni specifici casi. In particolare, in tali circostanze, i segnalanti beneficiano delle protezioni previste a condizione che: (i) abbiano prima segnalato internamente ed esternamente o direttamente esternamente, ma non sia stata intrapresa un'azione appropriata in risposta alla segnalazione entro il termine di tre mesi previsto dalla Direttiva oppure (ii) abbiano fondati motivi di ritenere che possa esservi un pericolo imminente o palese per il pubblico interesse o le prospettive che la violazione sia affrontata efficacemente siano scarse.

3.3 Tutele

Il timore di ritorsioni è ritenuto da sempre il fattore che maggiormente influisce sulla scelta di segnalare o meno una violazione. La Direttiva vieta qualsiasi forma di ritorsione, diretta o indiretta, attuata, incoraggiata o tollerata da parte dei datori di lavoro, dei clienti, dei destinatari dei servizi e delle persone che lavorano per l'organizzazione o per conto di quest'ultima, compresi i colleghi del segnalante e i dirigenti della stessa organizzazione o di altre organizzazioni con le quali il segnalante sia in contatto nell'ambito della sua attività professionale. Nel recepire il nuovo testo di legge, pertanto, gli Stati membri dovranno adottare le misure necessarie per vietare qualsiasi forma di ritorsione, comprese le minacce e i tentativi di ritorsione quale, per esempio, il licenziamento, la retrocessione o la mancata promozione, l'imposizione di misure disciplinari, la discriminazione, l'inserimento in liste nere, la conclusione anticipata di contratti per beni o servizi, l'annullamento di licenze o permessi, i danni, anche alla reputazione della persona, in particolare sui social media o la sottoposizione ad accertamenti psichiatrici o medici.

La Direttiva prevede, altresì, la predisposizione di numerose altre misure di sostegno a favore dei *whistleblowers*, incluso l'accesso a titolo gratuito a informazioni circa le procedure e i mezzi di ricorso disponibili in materia di protezione dalle ritorsioni, l'assistenza da parte delle autorità competenti dinnanzi a qualsiasi autorità e misure di assistenza finanziaria e sostegno, anche psicologico, nell'ambito dei procedimenti giudiziari.

Dal momento che è possibile che per giustificare la ritorsione siano addotti motivi diversi dalla segnalazione e può essere difficile per il segnalante dimostrare il nesso tra la segnalazione e la ritorsione, la Direttiva prevede che, una volta che il *whistleblower* abbia dimostrato di aver effettuato una segnalazione a norma della Direttiva e di aver subito un danno, l'onere della prova sia spostato sulla persona che ha compiuto l'azione ritorsiva che è, pertanto, tenuta a dimostrare che a misura adottata non era in alcun modo connessa alla segnalazione. Inoltre, non è possibile far valere nei confronti del segnalante obblighi giuridici o contrattuali degli individui come le clausole di lealtà dei contratti o gli accordi di riservatezza o non divulgazione per impedire di effettuare una segnalazione, negare la protezione o penalizzare le persone segnalanti per aver effettuato la segnalazione.

Nei procedimenti giudiziari, compresi quelli per diffamazione, violazione del diritto d'autore o degli obblighi di segretezza, divulgazione di segreti commerciali nonché azioni di risarcimento, è esclusa la responsabilità del segnalante per effetto di segnalazioni o divulgazioni pubbliche ed è riconosciuta al segnalante la possibilità di chiedere il non luogo a procedere purché avesse fondati motivi di ritenere che la segnalazione fosse necessaria per rivelare una violazione. Inoltre, è prevista l'immunità dalla responsabilità laddove i segnalanti abbiano acquisito od ottenuto accesso in modo lecito alle informazioni segnalate o ai documenti contenenti tali informazioni. Ciò si applica, per esempio, quando viene rivelato il contenuto di documenti cui hanno lecitamente accesso o ne vengono fatte fotocopie anche in violazione di clausole contrattuali o di altro tipo. L'immunità si applica, altresì, nei casi in cui dall'acquisizione delle informazioni possa discendere un tema di responsabilità, come nel caso in cui abbia acquisito le informazioni accedendo ai messaggi di posta elettronica di un collega o a luoghi a cui solitamente non ha accesso. Permane, tuttavia, la responsabilità penale nel caso in cui sia stato commesso un reato quale accesso abusivo o pirateria informatica.

A tutela del sistema di protezione dei segnalanti previsto dalla Direttiva, gli Stati membri sono chiamati a prevedere sanzioni – di natura civile, penale o amministrativa – effettive, proporzionate e dissuasive per scoraggiare le persone fisiche o giuridiche dall'ostacolare le segnalazioni, attuare atti di ritorsione, intentare procedimenti vessatori contro i segnalanti o violare gli obblighi di riservatezza circa la loro identità.

Principali differenze	
Legge 179/2017 (art. 6 D.Lgs. 231/2001)	**Direttiva (UE) 2019/1937**
La normativa italiana si applica, nel settore privato, solo agli enti che hanno adottato il Modello di organizzazione e gestione.	La Direttiva riguarda tutte le imprese con almeno 50 dipendenti, a prescindere dall'adozione del Modello di organizzazione e gestione, nonché ai soggetti operanti nei servizi finanziari e a rischio riciclaggio/finanziamento del terrorismo, indipendentemente dalle

	dimensioni. In base a un appropriato *risk assessment*, gli Stati membri possono decidere di applicare la Direttiva anche a soggetti con meno di 50 dipendenti.
La tutela del segnalante prevista dalla normativa si applica a tutti i casi di condotte illecite rilevanti ai fini dei reati presupposto *ex* D.Lgs. 231/2001 e violazioni del Modello di organizzazione e gestione.	La Direttiva considera tutte le violazioni relative ad alcuni specifici settori del diritto dell'Unione, tra i quali rientrano appalti, servizi finanziari, sicurezza dei prodotti e dei trasporti, tutela dell'ambiente e dei consumatori.
Quanto alla categoria dei segnalanti, sono tutelati i destinatari del Modello di organizzazione e gestione, quindi dipendenti, amministratori e terze parti.	Tra gli altri, sono tutelati gli azionisti delle società, i liberi dipendenti, i soggetti che assistono i *whistleblower*, gli ex dipendenti e coloro che hanno conosciuto gli illeciti in fase di selezione o negoziazione precontrattuale.
Agli enti è richiesto di adottare uno o più canali (dei quali ameno uno in forma informatica) che consentano le segnalazioni garantendo la riservatezza dell'identità del segnalante.	Gli enti dovranno: a) individuare un soggetto – interno o esterno – per la gestione e l'analisi delle segnalazioni nonché un soggetto che si occupi di seguire le indagini e mantenere la comunicazione con il segnalante; b) consentire al *whistleblower* di effettuare segnalazioni scritte, orali (incluso via telefono e messaggio vocale) o di persona; c) comunicare la ricezione della segnalazione entro 7 giorni; d) prendere in carico le segnalazioni e mantenere il whistleblower informato entro un tempo ragionevole (non oltre 3 mesi); e) conservare traccia e archiviare le segnalazioni e i relativi follow up;

	f) fornire informazioni chiare e dettagliate sulle procedure di segnalazione interna.
E' sancito il divieto di atti di ritorsione o discriminatori nei confronti del whistleblower, per motivi collegati, direttamente o indirettamente, alla segnalazione. Inoltre, sono nulli il licenziamento ritorsivo o discriminatorio del segnalante, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei suoi confronti.	E' vietata qualsiasi forma di ritorsione, comprese le minacce e i tentativi di ritorsione quale, per esempio, il licenziamento, l'imposizione di misure disciplinari, l'inserimento in liste nere, l'annullamento di licenze o permessi, i danni, anche alla reputazione della persona, in particolare sui social media o la sottoposizione ad accertamenti psichiatrici o medici. Sono, altresì, vietate le ritorsioni indiretti che possono essere intraprese contro il soggetto giuridico di cui il segnalante sia proprietario, per cui lavori o a cui sia altrimenti connesso in un contesto lavorativo.

4. Modalità di implementazione dei canali di segnalazione

Da quanto riportato, appare evidente che la nuova Direttiva avrà un notevole impatto sulle società che rientrano nel suo ambito di applicazione. In particolare, tali soggetti possono considerare i seguenti aspetti di particolare rilevanza:

- nell'implementare i canali di segnalazione in conformità ai requisiti previsti dalla Direttiva e la relativa procedura per dare seguito alle segnalazioni, è opportuno testare il sistema e verificare che funzioni in modo adeguato entro i tempi prescritti, al fine di evitare possibili sanzioni;

- è necessario assicurare che i dati personali del *whistleblower* e di terze parti nominate nella segnalazione siano mantenuti confidenziali e trattati in modo conforme a quanto previsto dal GDPR. Tutti i dati e le informazioni relativi alla segnalazione devono essere conservati diligentemente in modo da poterle fornire alle autorità competenti se necessario;

- la scelta del soggetto o della funzione più competente a ricevere o dare seguito alle segnalazioni dipende dalla struttura del soggetto stesso, purché sia assicurata l'indipendenza e l'assenza di conflitto di interessi. Nei soggetti più piccoli tale funzione potrebbe essere duplice e affidata a un funzionario che faccia capo

direttamente al direttore organizzativo, come un responsabile della conformità o delle risorse umane, un responsabile delle questioni giuridiche o della privacy;

– le informazioni circa le procedure devono essere chiare e facilmente accessibili anche, per quanto possibile, a persone diverse dai lavoratori che sono in contatto con il soggetto nell'ambito delle loro attività professionali, quali prestatori di servizi, distributori e partner commerciali. Pertanto, potrebbero essere esposte in un luogo visibile, accessibile a tutti e sul sito web ed essere incluse nei corsi e nelle formazioni di etica e integrità;

– nei gruppi, la procedura di segnalazione interna dovrebbe consentire alle capogruppo di ricevere ed esaminare le segnalazioni provenienti da dipendente delle controllate o affiliate, nonché, nella misura del possibile, da agenti, fornitori del gruppo e di chiunque ottenga informazioni attraverso le sue attività professionali presso il gruppo.