KPMG

Legal Newsletter n. 4/2023

Luglio - Agosto

—

Tax & Legal

Updates:

Corporate & Commercial

Public Sector

Governance Regulatory & Compliance

Privacy

Labour

—

kpmg.com/it

Sommario

Corporate & Commercial

Un recente provvedimento della Cassazione sulla qualificazione dei versamenti in conto futuro aumento di capitale

Nell'**ordinanza 8 agosto 2023**, n.**24093**, la Cassazione è tornata ad affrontare la questione dei versamenti effettuati dai soci.

Dopo aver illustrato la distinzione che intercorre tra le diverse tipologie di possibili dazioni da parte dei soci, distinguendole tra conferimenti, finanziamenti e versamenti, secondo l'inquadramento di cui alla propria precedente ordinanza 22 dicembre 2020, n. 29325, la Cassazione ha indicato i criteri che contraddistinguono i versamenti in conto futuro aumento di capitale rispetto a quelli c.d. a fondo perduto, che producono l'acquisizione definitiva al patrimonio della società delle somme versate a tale titolo.

Diversamente da tali apporti, da considerare definitivamente appresi al patrimonio sociale, i versamenti in conto futuro aumento di capitale vengono effettuati in funzione di un aumento di capitale, che non è ancora stato deliberato, e possono dare al socio **diritto alla restituzione** di quanto versato a tale titolo nel caso in cui tale aumento non avvenga.

Secondo la Cassazione perché la dazione da parte del socio possa essere ricondotta a tale categoria, ed essere quindi restituibile al socio che l'ha effettuata, "*è necessario che la subordinazione ad un aumento di capitale sia chiara ed inequivoca, mediante l'indicazione* ex ante *di elementi sufficientemente specifici e dettagliati, i quali inducano a ritenere effettivamente convenuta tra i soci l'effettuazione non di un versamento* tout court *a favore delle casse sociali, ma di un versamento avente titolo e causa concreta proprio nella partecipazione al capitale sociale mediante un futuro conferimento, che, sebbene meramente rinviato rispetto al momento della dazione materiale della somma, sia nondimeno sin dall'inizio volto, secondo la complessiva operazione programmata dai soci, ad aumentare la rispettiva quota di partecipazione sociale, in termini assoluti*".

La Cassazione specifica che, a tal fine, non sono da considerarsi di per sé esaustive le parole usate, dovendosi invece **verificare la sussistenza di** "*quegli* ***indici di dettaglio*** *(ad es., il termine finale entro cui verrà deliberato l'aumento, ma anche altre caratteristiche dello stesso), che soli qualificano la dazione come da ricondurre alla categoria in esame*".

Decisiva nella qualificazione della dazione come versamento in conto futuro aumento di capitale è l'interpretazione del**la volontà delle parti** di subordinare il versamento al futuro aumento di capitale, **che deve risultare chiara ed inequivoca**, potendosi a tal fine **tener conto di ogni elemento**, "*quali le clausole statutarie che tali versamenti prevedano, il comportamento delle parti, i fini perseguiti, le scritture contabili, i bilanci e qualsiasi altra circostanza del caso concreto, capace di svelare la comune intenzione delle parti e gli interessi coinvolti*".

Nel principio di diritto enunciato, la Corte ha specificato che le dazioni di denaro da parte dei soci che rientrano in tale tipologia non sono definitivamente acquisite al patrimonio sociale, "*avendo uno specifico vincolo di destinazione, con la conseguenza che, ove l'aumento non sia operato, il socio avrà diritto alla restituzione di quanto versato, per essere venuta meno la causa giustificativa dell'attribuzione patrimoniale da lui eseguita in favore della società, quale ripetizione dell'indebito*".

Ribadisce infine la Corte che "*per qualificare la dazione come versamento in conto futuro aumento di capitale, l'interprete deve verificare che la volontà delle parti di subordinare il versamento all'aumento di capitale risulti in modo chiaro ed inequivoco, utilizzando, all'uopo, indici di dettaglio (quali l'indicazione del termine finale entro cui verrà deliberato l'aumento, il comportamento delle parti, eventuali annotazioni contenute nelle scritture contabili o nella nota integrativa al bilancio, clausole statutarie), e, comunque, qualsiasi altra circostanza del caso concreto, capace di svelare la comune intenzione delle parti e gli interessi coinvolti, non essendo, all'uopo, sufficiente la sola denominazione adoperata nelle scritture contabili*".

Una recente sentenza della Cassazione conferma la validità della clausola della roulette russa

Con **sentenza 25 luglio 2023**, n.**22375**, la Cassazione si è espressa in merito alla validità ed efficacia della clausola c.d. "*Russian roulette*" o clausola della roulette russa approfondendo la questione e vagliando una serie di profili di criticità connessi al funzionamento di detta clausola con riferimento alle condizioni meramente potestative (art. 1355 c.c.), al divieto di patto leonino (art. 2265 c.c.), alle disposizioni volte a garantire una congrua valorizzazione della partecipazione del socio uscente (art. 2437 e 2437-*sexies* c.c.), nonché al principio di correttezza e buona fede nell'esecuzione del contratto ed all'abuso del diritto.

La clausola della roulette russa consiste nella pattuizione che, al fine di superare situazioni di stallo societario che rischiano di compromettere l'impresa economica e determinare la liquidazione della società, attribuisce a ciascuno dei soci la facoltà di fare all'altro socio una offerta per l'acquisto della sua partecipazione, indicando il prezzo che è disposto a pagare, con la corrispondente facoltà dell'altro socio di accettare l'offerta, vendendo la propria partecipazione al prezzo offerto, ovvero di rifiutare l'offerta e a quel punto di dover acquistare dal proponente la partecipazione di quest'ultimo al medesimo prezzo.

La Corte ha affermato che tale clausola - che nel caso al suo esame era stata inserita nei patti parasociali di una società di scopo tra due soci con identica partecipazione - è da ritenere valida ed espressione dell'interesse dei soci di evitare il rischio che, proprio a causa del paritetico diritto di voto, si possano verificare situazioni di stallo societario (*deadlock*) che portino alla liquidazione della società.

Nella sua decisione, la Cassazione ha precisato che l'inserimento di tale clausola all'interno dei patti parasociali, essendo volontariamente accettata dai soci paciscenti, esclude la necessità di applicare il principio di equa valorizzazione della partecipazione sociale di cui agli artt. 2437-*ter* c.c. (in caso di recesso del socio) e 2437-*sexies* c.c. (in caso di riscatto delle azioni), e ciò considerando che il destinatario dell'offerta fruisce di un diritto di scelta potendo decidere se vendere la propria partecipazione o, piuttosto, acquistare quella dell'altro socio, non essendo pertanto in una situazione di soggezione pura all'altrui diritto potestativo.

Public Sector

Le nuove indicazioni della Ragioneria dello Stato sulla rendicontazione delle *milestones* PNRR

La **circolare n. 26 dell'8 agosto 2023** della Ragioneria Generale dello Stato ha fornito indicazioni alle Amministrazioni Titolari di missioni del PNRR in merito alla rendicontazione delle relative *milestones* e dei *targets* in scadenza al T1 e T2 del 2023.

Oltre a contenere informazioni sul caricamento della documentazione di rendicontazione su ReGIS, la circolare reca una nuova versione della "*Dichiarazione di Gestione dell'Amministrazione titolare di Misure PNRR*" (aggiornata rispetto a quella approvata con la precedente circolare n. 30 dell'11 agosto 2022).

In aggiunta rispetto alla vecchia versione, il nuovo *format* di Dichiarazione prescrive alle Amministrazioni Titolari:

- di attestare che le Misure relative alle *milestones* e ai *targets* già indicati come raggiunti in occasione delle precedenti rendicontazioni semestrali non sono stati 'invertiti' (cioè non sono stati oggetto di c.d. "*reversal*");
- di allegare alla Dichiarazione un **documento di sintesi dei controlli effettuati** su tutte le *milestones* e i *targets* fino ad ora rendicontati, anche (ma non solo) in esito alle attività svolte durante i rispettivi *assessment periods* di cui all'art. 24, comma 3, del Regolamento UE n. 241/2021.

Regole speciali per gli appalti PNRR: il nuovo parere del MIT

Con la **circolare del 12 luglio 2023**, il Ministero delle Infrastrutture e dei Trasporti (MIT) ha fornito alcune indicazioni interpretative sul disposto dell'art. 225, comma 8, del D.Lgs. n. 36/2023 (nuovo Codice dei contratti pubblici), che fa salva l'efficacia delle disposizioni contenute nel D.L. n. 77/2021 (convertito con Legge n. 108/2021), nel D.L. n. 13/2023 (convertito con Legge n. 41/2023) e in altri provvedimenti legislativi di carattere speciale, con riguardo agli interventi soggetti, in tutto o in parte, a finanziamenti a carico del PNRR e/o del PNC.

Nello specifico, il MIT si sofferma sulle modalità di aggregazione della committenza e di svolgimento delle procedure di affidamento da parte dei Comuni non capoluogo di provincia destinatari di risorse del PNRR e del PNC.

A tal proposito, il parere in commento afferma che, fino al 31 dicembre 2023, è espressamente prorogata la possibilità, per i Comuni non capoluogo di provincia, di ricorrere alle modalità derogatorie di acquisizione di forniture, servizi e lavori di cui all'art. 1, comma 1, del D.L. n. 32/2019 (convertito con Legge n. 55/2019), così come modificato dall'art. 52, comma 1, lett. a), n. 1.2), del D.L. n. 77/2021 (convertito con Legge n. 108/2021), che consente ai predetti Comuni di effettuare affidamenti tramite "*le unioni di comuni, le province, le città metropolitane e i comuni capoluogo di provincia*", le "*centrali di committenza qualificate di diritto*" e le "*società in house delle amministrazioni centrali titolari degli interventi*".

Pubblicate da AgID le Linee guida sugli *Open data* della PA

L'Agenzia per l'Italia Digitale (AgID) con **determinazione n. 183 del 3 agosto 2023** ha adottato le Linee guida sui c.d. *open data*, in attuazione dell'art. 12 del D.Lgs. n. 36/2006 e s.m.i., come modificato dal D.Lgs. n. 200/2021, in attuazione della Direttiva UE n. 1024/2019 (c.d. Direttiva *Open Data*).

Le Linee Guida dell'AgID sono dirette a supportare le pubbliche amministrazioni, gli organismi di diritto pubblico e le società pubbliche e private nell'*iter* di accesso e riutilizzo dei dati e delle informazioni nel settore pubblico, implementando il *framework* normativo di riferimento. In particolare, tali Linee Guida contengono regole tecniche per la gestione di dati e documenti che, indipendentemente dal supporto cartaceo o elettronico, devono essere resi disponibili in condizioni di libera accessibilità e gratuità.

Tra le altre cose, le Linee Guida contengono:

- indicazioni di dettaglio in ordine ai metadati, alle licenze, alla tariffazione e ad aspetti organizzativi;
- una descrizione della qualità dei dati, che vengono suddivisi in:
  - "*dati dinamici*", soggetti a rapidi aggiornamenti (ad es. dati ambientali, metereologici o satellitari);

  - dati "*di elevato valore*", il cui riutilizzo è associato a importanti benefici per la società, l'ambiente e l'economia, in considerazione della loro idoneità per la creazione di servizi, applicazioni a valore aggiunto e nuovi posti di lavoro, nonché del numero dei potenziali beneficiari dei servizi e delle applicazioni a valore aggiunto basati su tali serie di dati;
  - dati "*della ricerca*", informatici, diversi dalle pubblicazioni scientifiche, raccolti o prodotti nel corso della ricerca scientifica e utilizzati come elementi di prova nel processo di ricerca, o comunemente accettati nella comunità di ricerca come necessari per convalidare le conclusioni e i risultati della ricerca;
- uno schema di *data governance* interna, attraverso la quale individuare i ruoli, le responsabilità e le fasi del processo, ferma restando l'autonomia di ciascuna Amministrazione nel definire un proprio modello procedurale sulla base delle risorse finanziarie, umane e strumentali a propria disposizione;
- indicazioni su aspetti organizzativi e sulla qualità dei dati, che riguardano rispettivamente:
  - attività di analisi ed elaborazione finalizzate al miglioramento della qualità e dell'accesso al dato stesso (precisandosi che le attività non si esauriscono con la mera pubblicazione dei dati, ma devono prevedere momenti continui di aggiornamento, monitoraggio e coinvolgimento degli utenti finali);
  - caratteristiche di qualità dei dati, le quali possono essere "*inerenti*" (come, ad esempio, l'accuratezza, l'aggiornamento, l'attualità, la completezza, la consistenza, la coerenza, e la credibilità), *"inerenti e dipendenti dal sistema"* (tra cui l'accessibilità, la comprensibilità, la conformità, l'efficienza, la precisione, la riservatezza e la tracciabilità) nonché *"dipendenti dal sistema"* (ossia la disponibilità, la portabilità e la ripristinabilità).

Sanità e digitalizzazione: il fascicolo sanitario elettronico 2.0 entra in fase operativa

In occasione della **Conferenza Stato-Regioni del 2 agosto 2023** è stato approvato lo schema di decreto interministeriale che rende operativo il fascicolo sanitario elettronico 2.0., che è volto al raggiungimento di un'altra *milestone* della M6C2, investimento 1.3, *sub* investimento 1.3.1, del PNRR, in tema di digitalizzazione della sanità.

Il fascicolo sanitario elettronico (FSE) 2.0 consente ai medici e agli operatori sanitari di consultare rapidamente le informazioni cliniche dei pazienti, indipendentemente dalla loro residenza, nel rispetto delle garanzie e delle misure di sicurezza sul trattamento dei dati personali e sul diritto di accesso ai dati medesimi da parte dei pazienti.

Tra le principali novità introdotte dal FSE 2.0, si segnalano in particolare:

- un **maggior numero di informazioni consultabili** per ciascun paziente, in cui rientrano i dati e i documenti riferiti a prestazioni erogate al di fuori del Servizio Sanitario Nazionale;
- la previsione del "***profilo sanitario sintetico***", che riassumerà la storia clinica dell'assistito e la sua situazione corrente conosciuta;
- l'inserimento del "***taccuino personale dell'assistito***", ossia una funzionalità della sezione riservata del FSE, che consentirà al paziente di modificare ed eliminare i dati, i documenti personali e le informazioni aggiuntive riguardanti i propri percorsi di cura;
- la possibilità, per gli operatori sanitari, di accedere al FSE in caso di **emergenza sanitaria**, anche in assenza del previo consenso da parte dell'interessato, dopo aver constatato l'incapacità fisica o giuridica di quest'ultimo ad esprimere il proprio consenso. Tale accesso sarà consentito per il tempo strettamente necessario ad assicurare al paziente le cure indispensabili e, in ogni caso, fino a quando l'interessato non sia nuovamente in grado di esprimere la propria volontà;
- la ricomprensione tra i **soggetti che possono alimentare il FSE** delle Aziende sanitarie locali, delle strutture sanitarie pubbliche del SSN, dei servizi socio-sanitari regionali e dei SASN (i "*Servizi di Assistenza Sanitaria al personale Navigante*"), delle strutture sanitarie accreditate con il SSN, dei servizi socio-sanitari regionali, delle strutture sanitarie autorizzate e degli esercenti le professioni sanitarie quando operano in autonomia;
- l'attribuzione della **facoltà di accesso al FSE** a tutto il personale sanitario che persegue finalità di cura (ad es. i medici, gli infermieri, i farmacisti), ad esclusione, invece, dei soggetti che non svolgono attività di assistenza sanitaria in senso stretto nei confronti dei pazienti (ad es. periti, compagnie di assicurazione, datori di lavoro, associazioni o organizzazioni scientifiche).

Il ‘nuovo’ soccorso istruttorio: prime indicazioni del Consiglio di Stato

La sentenza del **Consiglio di Stato, Sez. V, 21 agosto 2023, n. 7870**, nel decidere una questione concernente l’ammissibilità del soccorso istruttorio rispetto alla documentazione dimostrativa del possesso dei requisiti speciali di partecipazione ad una gara, ha svolto una comparazione tra la disciplina del soccorso istruttorio contenuta nell’art. 83, comma 9, del D.Lgs. n. 50/2016 e quella introdotta dal nuovo art. 101 del D.Lgs. n. 36/2023.

A seguito di un esame comparato delle due disposizioni, il Consiglio di Stato distingue le seguenti tipologie di soccorso istruttorio:

- **soccorso istruttorio “*integrativo o completivo*”**, contemplato da entrambe le disposizioni e diretto al recupero di carenze della documentazione amministrativa necessaria alla partecipazione alla gara, sempreché non si tratti di documenti acquisibili direttamente dalla stazione appaltante (con il limite della irrecuperabilità della documentazione di incerta provenienza soggettiva);
- **soccorso istruttorio “*sanante*”**, anch’esso ammissibile in base ad entrambe le norme sopra citate e volto a rimediare ad omissioni, inesattezze od irregolarità della documentazione amministrativa;
- **soccorso istruttorio “*in senso stretto*”**, previsto dall’art. 101, comma 3, del D.Lgs. n. 36/2023 e coerente con alcune forme di soccorso istruttorio ammesse da una parte della giurisprudenza anteriore alla nuova norma, il quale consente alla stazione appaltante di sollecitare chiarimenti o spiegazioni sui contenuti dell’offerta tecnica e/o dell’offerta economica, finalizzati a consentirne l’esatta acquisizione e a ricercare l’effettiva volontà dell’impresa partecipante (fermo restando il principio di immodificabilità delle predette offerte);
- **soccorso istruttorio “*correttivo*”**, che prescinde dall’iniziativa e dall’impulso della stazione appaltante e abilita direttamente il concorrente, fino al giorno di apertura delle offerte, alla rettifica di errori che ne inficino materialmente il contenuto.

Secondo il Consiglio di Stato, la principale differenza tra la vecchia e la nuova disciplina riguarda proprio la figura del soccorso istruttorio c.d. ‘correttivo’, la quale si configura come “***fattispecie di nuovo conio***” ed è pertanto insuscettibile di applicazione retroattiva.

Governance, Regulatory & Compliance

I nuovi Orientamenti di vigilanza di Banca d'Italia in materia di fornitori specializzati di servizi di *crowdfunding*

Il 2 agosto 2023 la Banca d'Italia ha pubblicato gli **Orientamenti di vigilanza in materia di fornitori specializzati di servizi di *crowdfunding*** (gli '**Orientamenti**').

I servizi di *crowdfunding* sono disciplinati dal Regolamento (UE) 2020/1503 ('**Regolamento CF**') e dai relativi standard tecnici (RTS e ITS) di attuazione, nonché dal Regolamento in materia di servizi di *crowdfunding* adottato con delibera della Consob n. 22720 del 1° giugno 2023, e possono essere prestati sia da **intermediari vigilati** che da **fornitori specializzati previa autorizzazione dell'autorità competente**, che il legislatore nazionale, con il D.Lgs. 10 marzo 2023, n. 30 ha individuato nella **Consob** e nella **Banca d'Italia**, dotate a tal fine di specifici **poteri autorizzativi**, **regolamentari**, di **supervisione** e **sanzionatori**.

Gli Orientamenti, finalizzati a **favorire l'omogenea e corretta applicazione dei principi e delle norme** che regolano il *crowdfunding*, hanno quali destinatari esclusivamente i fornitori specializzati di servizi di *crowdfunding,* con esclusione, di conseguenza, degli intermediari vigilati, e declinano taluni requisiti in materia di **governo societario**, **sistemi di gestione dei rischi e controlli interni**, **idoneità degli esponenti** e ***due diligence* sui titolari dei progetti**.

In specifico, con particolare riguardo a **governance e controllo**, gli Orientamenti prevedono che i fornitori di servizi specializzati di *crowdfunding:*

- predispongano (i) dispositivi di governo solidi che specifichino in forma documentata i rapporti gerarchici e la suddivisone delle funzioni; (ii) un sistema di gestione dei rischi e di controllo interno per la gestione e il controllo di tutti i rischi aziendali; (iii) efficaci flussi interni di comunicazione delle informazioni; (iv) politiche e procedure inerenti ai requisiti di competenza e conoscenza del personale; (v) idonee politiche e procedure amministrative e contabili che forniscano all'autorità di vigilanza un quadro fedele della posizione economica e finanziaria;
- definiscano la ripartizione delle competenze tra gli organi aziendali, il cui operato dovrebbe essere pertanto adeguatamente documentato nei verbali societari e valutino l'opportunità di **istituire un organo di controllo monocratico o collegiale**, il quale, tra le altre cose, dovrebbe (i) vigilare sul sistema di gestione dei rischi e di controllo interno; (ii) valutare l'adeguatezza e il funzionamento delle principali aree organizzative; (iii) promuovere interventi correttivi delle carenze e delle irregolarità rilevate.

In materia di **controlli interni e gestioni dei rischi**, tra i quali rilevano principalmente i **rischi legali, reputazionali e operativi**, ivi inclusi quelli **ICT** (Information and Communications Technology) **e di sicurezza**, i fornitori di servizi specializzati in materia di *crowdfunding* dovrebbero istituire **funzioni di controllo di conformità alle norme e di gestione dei rischi**, nonché una **funzione di revisione interna** e, laddove le prerogative, i poteri e i compiti spettanti alle singole funzioni possano essere **accentrate**, **valutare l'istituzione di un'unica funzione**. I fornitori di servizi specializzati in materia di *crowdfunding* che svolgono esclusivamente il **servizio '*investment based*'** (ovvero il servizio che ha ad oggetto il collocamento di valori mobiliari e strumenti emessi dai titolari di progetti o società veicolo) possono non prevedere l'istituzione di specifiche funzioni aziendali di controllo, **identificando**, invece, **almeno un esponente dell'organo di amministrazione con deleghe specifiche** in materia di controlli interni.

I fornitori specializzati di servizi di *crowdfunding*, data la **non obbligatorietà degli Orientamenti**, possono comunicare, in fase di autorizzazione e, in un momento successivo, nell'informativa periodica fornita nella relazione sulla struttura organizzativa, l'intenzione di adottare **misure differenti** da quelle stabilite negli Orientamenti e la **Banca d'Italia**, qualora non ritenesse adeguate le misure adottate, può prendere i **provvedimenti di vigilanza** previsti dalla legge.

Nuova consultazione IVASS sulle novità in materia di requisiti e criteri di idoneità degli esponenti aziendali

IVASS ha posto in pubblica consultazione uno schema di Provvedimento relativo ai requisiti degli esponenti aziendali (il '**Provvedimento**'), che reca modifiche ai Regolamenti IVASS 6 settembre 2016, n. 29 ('**Regolamento 29**'), relativo alle imprese di assicurazioni locali, e 3 luglio 2018, n.38 ('**Regolamento 38**'), relativo al sistema di governo societario.

Il Provvedimento ha la **finalità di adeguare** i predetti **regolamenti** alla più recente normativa emanata in materia: il riferimento è, in particolare, al D.Lgs. 14 luglio 2020, n. 84, modificativo del D.Lgs. 12 maggio 2015, n. 74 (**CAP**) e al decreto 2 maggio 2022, n. 88, del Ministero dello sviluppo economico (**MISE**) in materia di requisiti e criteri di idoneità allo svolgimento dell'incarico degli esponenti aziendali e di coloro che svolgono funzioni fondamentali ai sensi dell'art. 76, del CAP, che ha sostituito il precedente decreto del MISE dell'11 novembre 2011, n. 220.

In particolare, le principali novità riguardano:

- in relazione al **Regolamento 29**:
  - l'**obbligo di comunicare** all'IVASS il conferimento dell'incarico, il rinnovo, le dimissioni, la decadenza, la sospensione e la revoca, nonché ogni elemento sopravvenuto che possa incidere sulla valutazione di idoneità degli esponenti e dei responsabili delle funzioni di revisione interna, di gestione dei rischi e di verifica di conformità alle norme;
  - l'integrazione delle **politiche** con i criteri di correttezza e competenza;
  - l'**istituzione di procedure applicabili in merito alla valutazione d'idoneità** degli esponenti che si declinano alla luce di quanto di seguito indicato:
    (i) **in caso di nomina assembleare**, la valutazione di idoneità sia condotta dall'organo competente entro 30 giorni dalla nomina e che il relativo verbale sia trasmesso all'IVASS nello stesso termine, unitamente alla documentazione a supporto. Ove ravvisi criticità, l'IVASS dispone di un termine di 120 giorni per chiedere all'organo competente l'adozione di misure correttive ovvero avviare il procedimento di decadenza;
    (ii) **per i casi in cui la nomina non spetti all'assemblea**, la valutazione d'idoneità, salvo casi eccezionali d'urgenza, sia condotta prima della nomina. La nomina si perfeziona al decorso dei successivi 90 giorni, termine entro il quale l'IVASS potrà valutare di richiedere l'attuazione di misure correttive. Successivamente, l'impresa comunica l'avvenuta nomina entro 5 giorni ed entro 60 giorni da tale comunicazione l'IVASS può avviare un procedimento d'ufficio volto a pronunciare la decadenza;
    (iii) ai fini della valutazione, le imprese devono anche inviare dei **questionari** all'IVASS che indicano taluni elementi informativi (quali esperienze professionali, titoli di studio, iscrizione ad albi professionali, rapporti finanziari, altri incarichi di amministrazione, direzione e controllo ricoperti, disponibilità di tempo) da acquisire dagli esponenti e dai titolari delle funzioni fondamentali;
  - il potere **dell'IVASS**, nel caso in cui ravvisi il difetto di idoneità di un esponente, di avviare un procedimento d'ufficio volto a pronunciarne la decadenza;
- in relazione al **Regolamento 38**:
  - la possibilità che IVASS chieda ad esponenti di nomina assembleare di partecipare a **interviste**;
  - l'obbligo per le imprese del rispetto di una **quota pari al 33% del genere meno rappresentato** nel numero dei componenti dell'**organo di amministrazione e controllo**;
  - l'obbligo di **introdurre**, in relazione all'organo di amministrazione e controllo, **previsioni idonee a garantire il rispetto della** predetta **quota di genere a livello statutario**;
  - l'obbligo del rispetto di una **quota minima del 25%** degli **esponenti indipendenti** presenti nell'organo amministrativo;
  - il rimando all'art. 19 del decreto 2 maggio 2022, n. 88, del MISE, nel quale vengono individuati i requisiti e i criteri di idoneità applicabili ai titolari delle funzioni fondamentali;
  - l'applicabilità dei requisiti d'idoneità anche al responsabile della funzione fondamentale esternalizzata.

La **consultazione si chiude il 10 ottobre 2023**, che rappresenta la data ultima per inviare eventuali osservazioni o proposte.

ANAC: approvate con delibera del 12 luglio le linee guida definitive in materia di *whistleblowing*

Il 14 luglio 2023, ANAC ha pubblicato le **Linee Guida definitive**, chiarendo alcuni aspetti rilevanti della nuova disciplina dettata dal D.Lgs. 10 marzo 2023, n. 24 **in materia di segnalazioni *whistleblowing***, ed in particolare:

- per quanto riguarda le modalità di computo della media dei lavoratori impiegati nei soggetti del settore privato, occorre fare riferimento al valore medio degli addetti al 31 dicembre dell'anno solare precedente a quello in corso, contenuto nelle visure camerali, salvo per le imprese di nuova costituzione per le quali si considera l'anno in corso;
- posta elettronica ordinaria e PEC non sono state ritenute strumenti adeguati a garantire la riservatezza nell'ambito dell'istituzione dei canali di segnalazione interna. Per tale ragione, la soluzione attualmente raccomandata consiste nell'implementazione di una piattaforma informatica, che consenta la gestione delle segnalazioni mediante l'uso di meccanismi crittografici;
- con riferimento ai canali di segnalazione 'tradizionali' (posta cartacea), la segnalazione deve essere inserita in due buste chiuse: la prima con i dati identificativi del segnalante unitamente alla fotocopia del documento di riconoscimento; la seconda con la segnalazione, in modo da separare i dati identificativi del segnalante dalla segnalazione. Entrambe dovranno poi essere inserite in una terza busta chiusa che rechi all'esterno la dicitura: "*riservata al gestore della segnalazione*". Tali indicazioni dovranno essere riportate nelle policy interne relative alla gestione delle segnalazioni;
- nel termine di tre mesi il gestore deve fornire un riscontro al segnalante, che può consistere sia in provvedimenti definitivi, emessi a chiusura della procedura interna di segnalazione, sia in comunicazioni meramente interlocutorie rispetto allo stato di avanzamento dell'istruttoria e alle azioni da intraprendere;
- nelle ipotesi in cui un gruppo di imprese condivida un unico canale di segnalazione, gli enti coinvolti sono considerati contitolari del trattamento dei dati personali;
- è ammessa la nomina quale Gestore del canale interno dell'ufficio di *internal audit* ovvero dell'Organismo di Vigilanza *ex* D.Lgs. n. 231/2001;
- ove il gestore del canale interno si trovi in una situazione di conflitto di interessi rispetto ad una specifica segnalazione (in quanto segnalato o segnalante), ricorre una delle condizioni per poter effettuare una segnalazione esterna ad ANAC, non potendo essere assicurato che alla segnalazione sia dato efficace seguito. Sul punto, gli enti potranno gestire in via preventiva gli eventuali conflitti di interessi del gestore, prevedendo, ad esempio, in caso in cui la gestione del canale interno di segnalazione sia affidato ad un organo collegiale, l'astensione dall'istruttoria del componente che si trovi in conflitto di interessi. Allo stesso tempo, ove il gestore sia un organo monocratico, in caso di conflitto di interessi potrebbe prevedersi l'affidamento dell'incarico di gestione della segnalazione ad un consulente esterno;
- l'identità del segnalante può essere rivelata nell'ambito delle procedure interne ed esterne di segnalazione, solo in presenza delle seguenti condizioni (applicabili anche al procedimento disciplinare): i) acquisizione preventiva del consenso espresso del segnalante e ii) notifica al segnalante in forma scritta delle ragioni che rendono necessaria la rivelazione;
- in caso di trasmissione della segnalazione ad un soggetto diverso dal Gestore, la segnalazione sarà considerata *whistleblowing* ai sensi e per gli effetti del D.Lgs. n. 24/2023 solo ove la volontà di beneficiare delle specifiche tutele sia stata espressamente dichiarata dal segnalante o sia desumibile dalla segnalazione;
- l'elenco contenuto nel D.Lgs. n. 24/2023 sulle misure considerate ritorsive non è esaustivo, potendo costituire ritorsioni anche ulteriori condotte, come ad esempio la pretesa di risultati impossibili da raggiungere, una revoca ingiustificata di incarichi o un ingiustificato mancato conferimento di incarichi.

Le Linee Guida di ANAC sono state oggetto di pareri espressi dall'Autorità garante per la protezione dei dati personali. Sul punto, la versione definitiva ha recepito le indicazioni contenute nel parere favorevole espresso dal Garante per la protezione dei dati personali il 6 luglio 2023, chiarendo l'ambito delle condotte segnalabili e ribadendo la **necessità di garantire la riservatezza del segnalante e di tracciare le**

operazioni eseguite dal personale autorizzato responsabile della gestione delle segnalazioni, al fine di garantire la sicurezza del trattamento dei dati.

Reati tributari: il concorso dei componenti del CdA alla luce di una recente sentenza (Cass. pen., sez. III, 18 luglio 2023, n. 31017)

La Cassazione si è pronunciata su un ricorso presentato da due amministratori di una società, avverso la sentenza di condanna per il reato di cui all'art. 2 del D.Lgs. n. 74/2000 "*Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti*". In particolare, i ricorrenti ritenevano che i giudici del merito avessero dichiarato la loro responsabilità esclusivamente alla luce della carica ricoperta, senza considerare né l'attribuzione di poteri disgiunti ai tre amministratori né il fatto che la dichiarazione ritenuta mendace fosse stata sottoscritta solo da un terzo amministratore. Inoltre, a parere dei ricorrenti, i giudici del merito non avrebbero neppure accertato la loro eventuale consapevolezza in ordine alla fittizietà soggettiva delle fatture.

La Corte, nel dichiarare fondato il ricorso, ha affermato che "***nel caso di delitto deliberato e direttamente realizzato da singoli componenti del consiglio di amministrazione di una società di capitali nel cui ambito non sia stata conferita alcuna specifica delega, ciascuno degli altri amministratori risponde a titolo di concorso per omesso impedimento dell'evento****, ove sia ravvisabile una violazione dolosa dello specifico obbligo di vigilanza e di controllo sull'andamento della gestione societaria derivante dalla posizione di garanzia di cui all'art. 2392 c.c. (così Sez. 3, n. 30689 del 04/05/2021, Cerbone, Rv. 282714-01, proprio in tema di delitto di dichiarazione fraudolenta mediante l'utilizzo di fatture per operazioni inesistenti)*".

Il principio affermato dalla Cassazione trova conferma nella disposizione di cui all'art. 2392 c.c., secondo cui gli amministratori di una società non rispondono della violazione dei doveri ad essi imposti dalla legge o dallo statuto in relazione a fatti commessi da 'colleghi' nell'esercizio "*di attribuzioni del comitato esecutivo o di funzioni in concreto attribuite ad uno o più amministratori*" (comma 1), salva la responsabilità solidale ove, pur essendo a conoscenza di fatti pregiudizievoli, non abbiano fatto quanto in loro potere per impedirne il compimento o eliminarne o attenuarne le conseguenze dannose (comma 2).

Pertanto, a parere della Cassazione, "*gli amministratori senza delega rispondono per i fatti pregiudizievoli per la società commessi in violazione di legge o di statuto da uno di loro nell'esercizio di funzioni al medesimo attribuite 'in concreto', solo se ne erano a conoscenza e non hanno fatto il possibile per impedirne il compimento*".

Ritenendo applicabile tale principio anche in materia penale, "*sembra ragionevole ritenere che gli amministratori di una società, i quali non abbiano sottoscritto una dichiarazione fiscale fraudolenta mediante l'utilizzo di fatture per operazioni inesistenti, perché a ciò abbia provveduto un altro di essi nell'esercizio di funzioni a lui attribuite anche "in concreto", rispondono in concorso del reato di cui all'art. 2 D.Lgs. n. 74 del 2000 solo se abbiano avuto conoscenza dell'inserimento di tali documenti mendaci in contabilità e, ciononostante, non si siano attivati per impedirne l'indicazione nella dichiarazione o per impedire la presentazione di questa*".

Pertanto, poiché i giudici del merito avrebbero desunto in via meramente presuntiva la conoscenza da parte dei ricorrenti dell'utilizzazione di fatture per operazioni soggettivamente inesistenti "*in quanto titolari di poteri di amministrazione disgiunta*" e, dunque, "*effettivamente coinvolti nelle scelte gestionali delle società di famiglia*", la Cassazione ha annullato la sentenza con rinvio, al fine di accertare se i ricorrenti fossero in concreto a conoscenza della fittizietà delle fatture indicate nell'imputazione, e, in caso affermativo, se si fossero attivati per impedirne l'indicazione nella dichiarazione o, comunque, per impedirne la presentazione.

Infatti, la partecipazione dei due ricorrenti alle scelte gestionali della società, valorizzata dai giudici del merito, "***non significa necessariamente coinvolgimento nelle specifiche operazioni economiche alle quali si riferiscono le fatture per operazioni soggettivamente inesistenti, a maggior ragione perché all'impresa erano preposti tre amministratori, titolari, ciascuno, di poteri di amministrazione disgiunta***".

Privacy

Trasferimento di dati personali tra UE e USA: il nuovo *Privacy Framework*

Il problema del trasferimento di dati personali negli Stati Uniti d'America ha interessato gli operatori economici europei già prima dell'entrata in vigore del Regolamento (UE) n. 2016/679 in materia di protezione dei dati personali ('GDPR').

In precedenza, con la Direttiva 95/46/CE ('DPD'), il trasferimento di dati personali fuori dall'allora Comunità Europea richiedeva una decisione di adeguatezza della Commissione che stabilisse che il paese importatore garantiva un adeguato livello di protezione dei dati.

Al fine di permettere una più efficiente circolazione dei dati personali con gli Stati Uniti, la Commissione aveva successivamente emanato la Decisione di adeguatezza 2000/520/CE, istituendo il meccanismo di c.d. *Safe Harbour*. Tale meccanismo si basava su un sistema di autocertificazioni con le quali le aziende statunitensi, che intendevano ricevere trasferimenti di dati personali dall'Unione europea, attestavano al Dipartimento del Commercio degli Stati Uniti d'America il proprio impegno al rispetto di una serie di principi a garanzia della protezione dei dati personali precedentemente concordati con la Commissione. Il 6 ottobre 2015, tuttavia, la Corte di Giustizia europea dichiarava l'invalidità di tale Decisione con la sentenza passata alle cronache come Schrems I. La sentenza c.d. Schrems I era nata sull'onda del caso Snowden e delle conseguenti rivelazioni relativamente alla pervasività del controllo del sistema di sicurezza nazionale americano. Sul punto, la Corte di Giustizia aveva evidenziato come la Commissione, nell'adozione della Decisione di adeguatezza, avesse considerato unicamente l'idoneità a garantire la protezione dei dati personali del solo sistema di autocertificazione, omettendo di valutare l'adeguatezza dell'ordinamento giuridico statunitense nel suo complesso (come veniva invece imposto dall'art. 266 DPD).

Una sorte analoga veniva successivamente riservata al regime adottato dalla Commissione in sostituzione del *Safe Harbour*, il c.d. *Privacy Shield*, istituito con la Decisione di esecuzione (UE) 2016/1250. Quest'ultima venne infatti dichiarata invalida nel 2020 con la sentenza c.d. Schrems II. In tale pronuncia, la Corte di Giustizia aveva evidenziato come, nonostante le ulteriori misure di garanzia implementate nel nuovo meccanismo di trasferimento, il *vulnus* di fondo circa la possibilità per la *National Security Agency* americana di accedere e trattare i dati in violazione dei principi che governano il trasferimento e senza un adeguato controllo giudiziario, rimanevano inalterati nel nuovo regime, così determinandone l'inadeguatezza a garantire l'equivalenza della protezione dei dati personali al regime eurounitario.

Il 10 luglio 2023, con la Decisione di esecuzione (UE) 2023/1795, notificata con il numero C(2023)4745, è stata emanata una terza decisione di adeguatezza, con contestuale implementazione del c.d. *Privacy Framework*. Tale meccanismo, come quelli che lo hanno preceduto, si basa su un sistema di autocertificazione e di adesione ad un complesso di principi in materia di *data protection* da parte delle singole aziende statunitensi che vogliano far parte del *framework*. A differenza dei precedenti sistemi di trasferimento dati, tuttavia, il *Privacy Framework* introduce nuovi oneri per i servizi di *intelligence* statunitense in materia di *data protection*, in particolare, tramite l'*Executive Order* n. 14086 emanato dal Presidente degli Stati Uniti d'America il 7 ottobre 2022.

Fra le principali innovazioni introdotte, spiccano due elementi di particolare rilevanza: la previa definizione delle finalità per le quali è consentito all'*intelligence* di effettuare un trattamento di dati personali e l'introduzione dell'obbligo di trattare tali dati secondo i principi di necessità e proporzionalità, con autorizzazioni e supervisioni obbligatorie. Nel caso di violazioni di tali disposizioni da parte dei servizi di sicurezza, i soggetti interessati hanno la possibilità di effettuare un reclamo accedendo ad un sistema di ricorso denominato *Signals Intelligence Redress Mechanism*.

Il sistema di ricorso si articola in due diverse fasi attivabili dall'interessato per il tramite della pubblica autorità del paese esportatore. Nella prima fase il reclamo viene sottoposto al *Civil Liberties Protection Officer* ('CLPO'), che compie un'indagine sulla violazione denunciata, eventualmente ordinando l'applicazione di rimendi appropriati per l'eliminazione della situazione di illiceità o confermando al ricorrente la mancata individuazione di violazioni. In ogni caso, il CLPO avrà cura di non dare all'interessato alcuna indicazione sul fatto che siano o meno effettivamente in corso operazioni di *intelligence*. Nella seconda fase, il ricorrente, sempre tramite il filtro della pubblica autorità del paese esportatore, può chiedere la revisione delle determinazioni del CLPO dinanzi alla *Data Protection Review Court*: un organismo giudiziario composto da sei o più giudici nominati dal Procuratore Generale statunitense fra soggetti esterni al governo degli Stati Uniti d'America con garanzie di indipendenza (anche dalla procura generale stessa) e caratteristiche di inamovibilità.

In conclusione, il nuovo *Privacy Framework* rappresenta un passo significativo verso la normalizzazione e la semplificazione del trasferimento di dati personali verso gli Stati Uniti d'America. Questo nuovo meccanismo di trasferimento elimina la necessità di ricorrere a complicate soluzioni giuridiche per garantire la conformità al GDPR, come l'utilizzo delle clausole contrattuali standard della Commissione europea che ha caratterizzato l'interregno fra la sentenza Schrems II e questa nuova decisione di adeguatezza.

Gli imprenditori che intrattengono rapporti contrattuali implicanti trasferimenti di dati verso controparti statunitensi (ad esempio fornitori e partner commerciali) potranno ora verificare in modo agevole se tali soggetti rientrano nel nuovo regime di trasferimento semplicemente consultando il sito *web* ufficiale "https://www.dataprivacyframework.gov/s/" ed *ivi* cercando la relativa ragione sociale.

Diffusione di materiale audiovisivo relativo a reati violenti: due recenti provvedimenti del Garante.

Il 23 agosto 2023, l'Autorità Garante per la Protezione dei Dati Personali ('Garante') ha emesso due provvedimenti urgenti, rispettivamente con numero 357 e 358, che affrontano il complicato tema della responsabilità per la diffusione in rete di materiale audiovisivo raffigurante gravi azioni criminose, tali da ledere gravemente la riservatezza e la dignità della vittima.

Questi provvedimenti, entrambi volti ad interrompere la catena di condivisione sul *web* dei video relativi a fatti che costituiscono una grave fattispecie di reato, sono rivolti a due diverse categorie di soggetti: da un lato gli utenti della piattaforma *Telegram*, di Telegram FZ-LLC, su cui i contenuti sono stati diffusi, dall'altro la piattaforma stessa.

Con riferimento al provvedimento n. 358, rivolto a tutti gli utenti della piattaforma, il Garante avverte che le condotte degli utenti responsabili della diffusione e condivisione del materiale multimediale ritenuto illecito possono, verosimilmente, configurare una **violazione delle disposizioni del Regolamento (UE) n. 2016/679** ('**GDPR**'), con tutte le conseguenze ivi previste, anche di carattere sanzionatorio. Ad avviso del Garante, tale diffusione non può essere giustificata dalla necessità di tutelare il diritto di cronaca o da quella di garantire la libertà di manifestazione del pensiero, poiché il parametro della "*essenzialità dell'informazione*" è da intendersi rigorosamente con riferimento al trattamento di dati personali riconducibili ad un individuo vittima di violenze.

Con il provvedimento n. 357, rivolto alla piattaforma, il Garante, oltre a ribadire i medesimi ammonimenti rivolti agli utenti della stessa, affronta la tematica della propria competenza territoriale. In particolare, ribadisce la capacità di esercitare, ai sensi dell'art. 55 GDPR, i suoi poteri su soggetti non stabiliti nell'Unione europea (in questo caso, Telegram FZ-LLC è stabilita al di fuori dello Spazio Economico Europeo) che offrono dei servizi a individui situati nel territorio dell'Unione, ricadendo nell'ambito di applicazione territoriale di cui all'art. 3, par. 2, lett. a), GDPR.

I suddetti provvedimenti, prospettando l'applicazione di possibili e future sanzioni amministrative ai sensi del GDPR per le condotte della piattaforma *Telegram* e di alcuni dei suoi utenti, dovrebbero indurre i destinatari a conformarsi quanto prima alle disposizioni del GDPR ed alle indicazioni del Garante.

Dall'entrata in vigore il 25 agosto 2023 del Regolamento (UE) 2022/2065 noto come *Digital Service Act* (c.d. "DSA"), la diffusione di materiale digitale ritenuto illecito con provvedimento ufficiale del Garante richiede di essere valutata anche rispetto al regime di responsabilità dei *social network* introdotto dal DSA.

In via generale, ai sensi del DSA, le piattaforme non sono soggette a un obbligo generale di sorveglianza sulle informazioni che vengono diffuse dagli utenti (art. 8), pertanto, non sono direttamente responsabili rispetto a quanto caricato sulla piattaforma dagli utenti stessi. Sono tuttavia previste delle eccezioni all'esenzione di responsabilità qualora: 1) la piattaforma svolga un ruolo attivo che consenta la conoscenza o il controllo delle informazioni; 2) il materiale sia stato fornito dalla piattaforma stessa; 3) i contenuti siano stati elaborati sotto la sua responsabilità editoriale.

Alle fattispecie di responsabilità della piattaforma sopra elencate si aggiunge quella in cui un'autorità amministrativa nazionale emetta un provvedimento ufficiale concernente l'illegalità del materiale che viene condiviso e ordini alla piattaforma di contrastare i contenuti illegali che circolano sulla stessa. In questo caso, la piattaforma potrebbe essere ritenuta responsabile qualora non dia attuazione al provvedimento dell'autorità adottando le misure necessarie per impedirne la continua diffusione del materiale multimediale illecito, ai sensi dell'art. 9 del DSA.

In tal senso, potrebbero essere intesi i provvedimenti d'urgenza emanati dal Garante, che esortano la piattaforma *Telegram* a **contrastare la circolazione dei video in rete da parte dei propri utenti. In questo caso, la responsabilità non si limiterebbe soltanto ai singoli utenti del noto *social network* che hanno**

salvato e inviato il materiale multimediale tramite i loro dispositivi, ma si estenderebbe anche alla piattaforma stessa qualora non provveda a fermare la diffusione del materiale, rappresentando un primo possibile caso di applicazione del regime di responsabilità introdotto dal DSA nei confronti di una piattaforma *social media*.

Caso ASPI - Free to X: l'importanza della corretta definizione dei ruoli privacy

A seguito dell'accordo transattivo con il Ministero delle Infrastrutture e dei Trasporti, Autostrada per l'Italia S.p.A. (ASPI) ha implementato un sistema di rimborso dei pedaggi nominato *Cashback*. Nell'implementazione del sistema, ASPI si è affidata alla società Free to X S.r.l. (interamente posseduta da ASPI stessa), incaricandola di predisporre il predetto sistema di rimborso attraverso un *software mobile ad hoc*. Relativamente agli aspetti di protezione dei dati personali, Free to X rilasciava un'informativa all'interno della quale veniva chiarito come nell'ambito del servizio *Cashback*, quest'ultima fosse l'unica titolare del trattamento.

Sul punto, è intervenuto il Garante della Protezione dei Dati Personali (Garante), contestando la riconducibilità in capo a Free to X della titolarità del trattamento. A seguito dei rilievi del Garante, ASPI e Free to X replicavano chiarendo che nel caso di specie la prima operasse come responsabile del trattamento dei dati personali e la seconda come titolare. In particolare, le parti hanno sostenuto che, sebbene ASPI avesse appaltato a Free to X la realizzazione del servizio *Cashback*, ai fini dell'individuazione dei ruoli privacy quest'ultima fosse da considerarsi unica titolare del trattamento, avendo essa pieni e autonomi poteri decisionali in ordine alla determinazione di finalità e mezzi del trattamento, anche considerando come ASPI non avesse mai fornito alcuna istruzione in merito al trattamento di dati personali, ma solo macro parametri relativi agli importi da destinare agli utenti del servizio.

Dopo un'approfondita indagine condotta dal **Garante**, nonostante le affermazioni delle società coinvolte, l'autorità indipendente **contestava ad ASPI l'erronea configurazione del rapporto**. Infatti, come rilevato dal Garante, il soggetto che determina le finalità ed i mezzi del trattamento con riferimento al servizio *Cashback* risulta essere proprio ASPI che, anche in virtù dell'accordo da essa concluso con il Ministero, ha incaricato la società *Free to X* di implementare il sistema sulla base di criteri specificamente predeterminati. Inoltre, il Garante ha evidenziato come nell'ambito del servizio prestato da Free to X vadano distinti i trattamenti rispetto a cui essa operi in qualità di responsabile da quelli rispetto a cui essa operi come titolare. In particolare, infatti, *Free to X* determina mezzi e finalità dei trattamenti relativi alla registrazione dell'utente sull'applicazione e la gestione del relativo *account,* mentre, viceversa, opera come mero responsabile del trattamento con riferimento all'erogazione del servizio *Cashback*. A seguito di tali rilievi, veniva pertanto rinvenuta nella condotta di ASPI la violazione dei principi di trasparenza e correttezza, nonché degli artt. 13 e 28 del GDPR con la conseguente irrogazione di una sanzione amministrativa di un milione di euro.

Questa vicenda offre alcuni spunti per una **riflessione sull'importanza di una corretta individuazione delle responsabilità e dei ruoli in materia di trattamento dei dati personali**. Innanzitutto, nella vicenda sopra narrata, emerge l'importanza di una chiara e corretta definizione dei ruoli tra titolare e responsabile del trattamento, soprattutto nei casi in cui nell'ambito di una singola attività siano rinvenibili diversi trattamenti di dati personali con titolarità differenti.

A tal riguardo, va sottolineata l'importanza di una chiara definizione dei termini e delle condizioni dei contratti di *outsourcing* dei servizi che implichino potenziali trattamenti di dati personali. Infatti, come chiarito anche dall'*European Data Protection Board* (Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento), gli accordi contrattuali nell'ambito di un servizio di *outsourcing* hanno un ruolo fondamentale nella determinazione della titolarità del trattamento, essendo tali contenuti idonei a rivelare quale sia la parte che, nell'ambito di uno specifico trattamento, contribuisca all'effettiva determinazione delle finalità e dei mezzi del trattamento dei dati. Infatti, la parte che risulta titolare del trattamento è sempre tenuta a valutare i termini contrattuali con la parte responsabile e, nella misura in cui li accetta e si avvale del servizio, a vigilare sull'attività del responsabile, nonché ad assumersi la piena responsabilità del rispetto del GDPR nell'ambito del trattamento.

Infine, la decisione del Garante di infliggere una sanzione amministrativa ad ASPI per la violazione sopra menzionata rivela come anche l'errata configurazione dei ruoli in materia di dati personali possa essere causa di sanzioni amministrative di ammontare rilevante e di come l'autorità di vigilanza italiana si sia già attivata sul tema. Le organizzazioni devono quindi essere consapevoli delle loro responsabilità e porre particolare cura ed attenzione agli adempimenti di *compliance* che permettono una corretta gestione degli aspetti di *data protection*, a partire dalla corretta tenuta di un registro dei trattamenti idonea a garantire una mappatura affidabile dei trattamenti in corso di svolgimento fino ad arrivare al censimento dei fornitori e, quando necessario, delle relative nomine a responsabile del trattamento.

Labour

DVR: il rischio interferenziale esterno

La gestione dei rischi per la salute e la sicurezza negli ambienti di lavoro risulta spesso complessa, **soprattutto quando tali rischi hanno una natura interferenziale dovuta alla presenza, all'interno di uno stesso luogo di lavoro, di lavoratori alle dipendenze di datori di lavoro diversi**.

Negli ultimi anni, peraltro, la giurisprudenza ha assunto una posizione specifica (che si sta consolidando) anche con riferimento ai fenomeni naturali relativi ai rischi che devono essere presi in debita considerazione all'interno dei luoghi di lavoro. A tal proposito, la sentenza della **Cassazione pen., sez IV, 24 luglio 2023, n. 31816** ha espresso la propria posizione di indirizzo volta proprio alla tutela dei lavoratori di terze parti nei luoghi di lavoro, nonché circa la prevedibilità di eventi esterni.

La vicenda in questione riguarda il disastro ferroviario verificatosi nel dicembre 2009 sulla tratta ferroviaria Sassari-Chilivani, in cui rimase vittima un macchinista di T. S.p.A. per un **violento impatto del treno che conduceva contro un masso di grandi dimensioni**, caduto accidentalmente sui binari a seguito di una frana. Tribunale e Corte di appello avevano ritenuto responsabili del reato di omicidio colposo, con violazione delle norme antinfortunistiche, di cui all'art. 589 c.p. il Responsabile della Direzione territoriale di produzione, ritenuto datore di lavoro-dirigente, e quello della Gestione operativa territoriale dell'impresa concessionaria della gestione della rete ferroviaria.

A tal riguardo, la giurisprudenza di legittimità ha già in varie occasioni avuto modo di precisare che **le norme antinfortunistiche devono essere a tutela non solo dei lavoratori dell'impresa interessata, bensì anche dei terzi che si trovino nell'ambiente di lavoro**, indipendentemente dall'esistenza di un rapporto di dipendenza con il titolare dell'impresa. Pertanto, qualora si verifichino eventi che possano ledere i diritti alla salute e sicurezza di terzi, **è ravvisabile la colpa per violazione delle norme antinfortunistiche** purché sussista, tra l'eventuale violazione e l'evento dannoso, un nesso causale e che la norma violata miri effettivamente a prevenire l'incidente verificatosi, sempre che non sia stato interrotto il nesso eziologico.

Nel caso di specie, **il datore di lavoro avrebbe dovuto valutare il rischio specifico da frane all'interno del Documento di Valutazione dei Rischi (DVR)**: ad avviso della Corte, infatti, detto rischio non integrava nemmeno un rischio di natura eccezionale non prevedibile, poiché l'area in cui si è verificato l'evento **risultava classificata come altamente pericolosa e con sistemi di protezione non adeguati**. Il rischio è stato quindi considerato come "*gestibile*" non solo con un intervento di "*rimozione del versante roccioso*", ma anche tramite l'implementazione, da parte del gestore della rete ferroviaria, di sistemi volti alla prevenzione del rischio stesso (ad esempio, galleria per fungere da barriera protettiva dei binari).

Alla luce di quanto sopra, **l'evento è stato catalogato come prevedibile ed evitabile** poiché frutto della violazione delle regole cautelari, dal momento che il rischio (concretizzatosi) doveva essere valutato nel DVR (in termini di effettiva valutazione del rischio) e prevenuto con delle misure idonee, quali ad esempio la predisposizione di una galleria (in termini di effettivo intervento pratico).

Il lavoratore deceduto, pertanto, **pur se appartenente a un terzo datore di lavoro avrebbe dovuto comunque essere tutelato anche dal menzionato rischio**, pur essendo esterno all'organizzazione che gestisce la rete ferroviaria e rientrandone la gestione direttamente in capo al datore di lavoro responsabile della sicurezza della rete ferroviaria.

Accesso abusivo al sistema informatico o telematico da parte di dipendenti o collaboratori

Nel caso di accesso abusivo a un sistema informatico o telematico da parte di dipendenti o collaboratori, la Cassazione penale, con sentenza 27 giugno 2023, n. 27900, ha ritenuto che, **per sussistere il reato di accesso abusivo a un sistema informatico o telematico, sia necessario individuare con precisione la titolarità, la disponibilità e la finalità degli accessi al sistema informatico o telematico, specialmente quando si tratti di uno spazio di archiviazione utilizzato per scopi professionali o lavorativi condivisi tra vari soggetti**.

Il caso trattato riguarda due ex dipendenti di una società che, dopo aver lasciato la società per cui lavoravano, avevano creato una nuova società nello stesso settore. La società per cui avevano lavorato in precedenza li aveva denunciati per accesso abusivo al sistema informatico (inizialmente in base all'art. 635-

quater c.p. e, successivamente, ai sensi dell'art. 615-*ter* c.p.), vedendosi i medesimi **condannati per accesso abusivo a un sistema informatico sia in primo grado che in appello**.

La questione centrale era se i due imputati fossero effettivamente titolari del sistema informatico in questione, poiché, in base all'impianto accusatorio, la **condotta di accesso abusivo al sistema informatico della società consisteva nella modifica dell'indirizzo e-mail collegato all'account Dropbox condiviso e in uso ai dipendenti** della società originaria, rendendo inaccessibile il contenuto condiviso precedentemente. Questo, secondo l'accusa, configurava una violazione dei limiti imposti dalla società titolare del sistema informatico in quanto "*una operazione idonea a vietare l'accesso al sistema proprio al titolare del sistema stesso, configura ex se una violazione dei limiti imposti a terzi in possesso delle password*".

Gli imputati sottolineavano come fosse impossibile individuare il proprietario del**lo spazio di archiviazione Dropbox** conteso nella società originaria, poiché tale spazio **era nella disponibilità dei due dipendenti che ne erano proprietari in quanto creatori di detto spazio**, dal momento che dal sito della piattaforma si evinceva come il creatore di una cartella condivisa fosse automaticamente designato come proprietario della medesima. Essendo i legittimi proprietari delle credenziali di accesso, dopo essersi licenziati, essi avevano pertanto il diritto di utilizzare il sistema come preferivano.

In aggiunta, l'ulteriore tesi difensiva degli imputati verteva sulla **mancanza** del necessario elemento psicologico **del dolo** poiché **gli imputati ritenevano di agire legittimamente su un archivio di loro proprietà** e non avevano, quindi, la consapevolezza di commettere un reato.

La Corte di Cassazione ha chiarito come **il reato di accesso abusivo può sussistere non solo quando un soggetto non autorizzato accede al sistema, ma anche quando un soggetto autorizzato viola le condizioni imposte dal titolare del sistema o compie azioni non consentite dallo scopo originario dell'accesso. L'elemento psicologico essenziale è la consapevolezza e la volontà di accedere o restare nel sistema contro la volontà del titolare**.

In sintesi, la sentenza della Cassazione penale ha sottolineato che **il reato di accesso abusivo a un sistema informatico o telematico può sussistere anche quando il soggetto abbia legittime credenziali di accesso, ma violi le condizioni o le finalità dell'accesso**, a condizione che agisca con la consapevolezza di comportarsi contro la volontà del titolare del sistema.

I sistemi decisionali e di monitoraggio automatizzati sul luogo di lavoro: indicazioni operative

Con il decreto-legge 4 maggio 2023, n. 48 (c.d. Decreto Lavoro), convertito dalla Legge 3 luglio 2023, n. 85, il legislatore è intervenuto stabilendo per il datore di lavoro l'obbligo di informare il lavoratore – nonché le organizzazioni sindacali – in merito **all'utilizzo di sistemi decisionali o di monitoraggio 'integralmente' automatizzati**, escludendo in tal modo quei sistemi che prevedono un coinvolgimento umano.

Ma andiamo con ordine.

Al fine di conformarsi ai dettami dell'Unione europea, volti a garantire lo sviluppo delle nuove tecnologie nel rispetto dei diritti fondamentali e della dignità umana, il legislatore nazionale ha recepito la Direttiva (UE) 2019/1152, riguardante la trasparenza e la prevedibilità delle condizioni di lavoro. Da ciò scaturisce, tra i vari, l'obbligo per il datore di lavoro (o il committente pubblico e privato) di informare il lavoratore circa l'utilizzo di sistemi decisionali o di monitoraggio automatizzati deputati a fornire indicazioni rilevanti *"ai fini della assunzione o del conferimento dell'incarico, della gestione o della cessazione del rapporto di lavoro, dell'assegnazione di compiti o mansioni nonché indicazioni incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori*" (art. 1-*bis* D.Lgs. n. 152/1997, così come introdotto dal D.Lgs. n. 104/2022, c.d. Decreto Trasparenza).

Il Decreto Trasparenza – in attuazione della suddetta direttiva – prevede dunque **il diritto del lavoratore di conoscere, anzitutto, se il proprio datore di lavoro impieghi (o meno) dispositivi automatizzati e/o processi decisionali controllati algoritmicamente**, nonché la modalità di funzionamento degli stessi, la *ratio* sottesa al loro utilizzo ed eventuali rischi connessi alla sicurezza dei suoi dati personali.

L'introduzione di tale norma non è però risultata immune da dubbi interpretativi. Si pensi, a titolo esemplificativo, che, con non poca difficoltà, la giurisprudenza è giunta ad escludere il suddetto obbligo di informativa in merito all'utilizzo del *badge* aziendale, salvo che dall'utilizzo dello stesso non scaturisca una decisione automatica del datore di lavoro.

Tuttavia, con il recente decreto-legge n. 48/2023, tale obbligo di informativa in capo al datore di lavoro – quale titolare del trattamento dei dati dei propri lavoratori – è stato limitato ai meri sistemi decisionali o di monitoraggio totalmente automatizzati.

Al fine di fare chiarezza sul concetto di sistema 'integralmente' automatizzato, merita menzione l'orientamento espresso dal giudice del Tribunale di Palermo (sentenza del 20 giugno 2023) per il quale l'obbligo di informativa in capo al datore di lavoro sarebbe circoscritto a quei sistemi di decisione e monitoraggio "*che non prevedono alcun intervento umano nella fase finale del processo decisionale o di monitoraggio*", fatta eccezione per quei sistemi che risultino "*coperti da segreto industriale o commerciale*".

Risultano, pertanto, esonerati dal 'nuovo' obbligo informativo quei sistemi che gestiscono le suddette attività – di assunzione, gestione e cessazione del rapporto di lavoro, assegnazione di compiti/mansioni, sorveglianza, valutazione etc. – in misura parziale.

Alla luce del nuovo decreto rimane dunque in capo al datore di lavoro l'obbligo di fornire al lavoratore e alle organizzazioni sindacali le informazioni riguardanti le seguenti caratteristiche dei sistemi (integralmente) automatizzati:

- gli aspetti del rapporto di lavoro sui quali incide l'uso dei sistemi decisionali/monitoraggio automatizzati;
- la *ratio* sottesa all'utilizzo dei sistemi e il loro meccanismo di funzionamento;
- le categorie di dati e i parametri utilizzati per programmare i sistemi, ivi compresi i meccanismi di valutazione delle prestazioni lavorative;
- le misure di controllo sul funzionamento dei sistemi, le eventuali misure correttive e il responsabile della gestione della qualità dei sistemi.

Hanno contribuito a questo numero:

Emanuela Bollati
Diletta Cavicchi,
Laura Cinicola
Alessandro Colella
Lorenzo Curvo
Manfredi Ferrari Liccardi Medici
Giuditta Garattini
Silvano Geusa
Vittoria Ghisoni
Martina Iacono
Maria Paola Ingletto
Lorenzo Labruna
Federico Maria Morri
Giulia Parodi
Chiara Peja
Ludovica Puccioni
Baldassare Puccio
Marco Valdes
Federica Verdecchia

Studio Associato
Consulenza legale e tributaria

Contatti

it-fmLegalNewsletter@kpmg.it

Sedi

Milano
Via Vittor Pisani 31, 20124
Tel. 02 676441

Ancona
Via 1° maggio 150/a, 60131
Tel. 071 2916378

Bologna
Via Innocenzo Malvasia 6, 40131
Tel. 051 4392711

Firenze
Viale Niccolò Machiavelli 29, 50125
Tel. 055 261961

Genova
P.zza della Vittoria 15/12, 16121
Tel. 010 5702225

Napoli
Via F. Caracciolo 17, 80122
Tel. 081 662617

Padova
Piazza Salvemini 2, 35131
Tel. 049 8239611

Perugia
Via Campo di Marte 19, 06124
Tel. 075 5734518

Pescara
P.zza Duca D'Aosta 31, 65121
Tel. 085 4210479

Roma
Via Curtatone 3, 00185
Tel. 06 809631

Torino
C.so Vittorio Emanuele II 48, 10123
Tel. 011 883166

Verona
Via Leone Pancaldo 68, 37138
Tel. 045 8114111

kpmg.com/it/socialmedia