SAEV informa

Periodico di informazione ed. secondo semestre Settembre 2017
Direttore Responsabile Stefano Vecchi

EDIZIONE SPECIALE
"DATA PROTECTION OFFICER"

PRIVACY
Il nuovo diritto all'oblio

ANTIRICICLAGGIO
L'obbligo di astensione dalla prestazione

RESPONSABILITA' DEGLI ENTI
Il M.O.G. esame della normativa di riferimento

SICUREZZA SUL LAVORO
Il sistema delle responsabilità

HACCP
palestre e piscine... nuove regole

SICUREZZA AMBIENTALE
Analisi degli eco-reati

saev group

Il D.P.O.

Data Protection Officer

Spiegato in modo chiaro

LA PRIVACY È COMPLESSA ED IN CONTINUA EVOLUZIONE, QUANTO DELICATA, PROPRIO PER QUESTO L'UNIONE EUROPEA HA REGOLAMENTATO TALE NORMATIVA INTRODUCENDO LA FIGURA DEL ***DATA PROTECTION OFFICER: PER LE PUBBLICHE AMMINISTRAZIONI E PER ALCUNE IMPRESE È OBBLIGATORIO NOMINARE IL DPO!***

Pubbliche Amministrazioni e alcune tipologie di Azienda devono attivarsi da subito per far si che entro il 25 maggio 2018 sia stato nominato un DPO competente in materia di Privacy.
Il DPO può essere una figura interna o esterna all'Ente o all'Azienda. La nomina e la formazione del Data Protection Officer è la nuova avventura per Enti ed Imprese richiesta dall'UE:
trasformala in una nuova opportunità!

saev
group

EDITORIALE

CHI HA TEMPO NON ASPETTI TEMPO!

Direttore Responsabile: Dott. Stefano Vecchi

Non si può certo affermare che il 2017 sia stato un anno di quiete per i legislatori!

Negli ultimi mesi innumerevoli sono state le modifiche e le innovazioni normative intervenute su gran parte dei settori di interesse per l'esercizio dell'attività d'impresa.

Il cover article del nuovo numero di SaevInforma è in gran parte dedicato all'analisi del Nuovo Regolamento Europeo 679/16 in materia di trattamento dei dati personali. Sulla base della nuova disciplina tutte le imprese (e gli enti pubblici) saranno chiamati all'adeguamento dei propri sistemi di gestione privacy ai sensi del 679/16 entro il termine ultimo del 25 maggio 2018. Non fatevi trovare impreparati! Sebbene ci dividano ancora nove mesi dalla data limite per la "messa in regola", è importante considerare che il processo di adeguamento previsto potrà rivelarsi lungo e complesso, richiederà impegno ed energie da parte degli Amministratori e, per questo, è bene iniziare fin da subito a conoscere ed approfondire i termini della riforma e soprattutto le conseguenze dirette che questa rivolgerà nella compagine aziendale. Data la portata profonda e determinante del Nuovo Regolamento, si è voluto offrire in questo numero una panoramica dei temi chiave della normativa, dei nuovi adempimenti imposti, delle nuove sanzioni previste, avvalorata da uno speciale focus relativo alla nuova figura del D.P.O. introdotta dall'U.E. (obbligatorio per tutti gli enti e per talune imprese) con l'obbiettivo primario di fornire uno strumento di conoscenza ed analisi degli obblighi con i quali da qui al prossimo anno saremo tutti costretti a confrontarci per risultare idonei alla legge.

Il tono e la rilevanza assunta dal settore privacy nell'ultimo periodo però non ci hanno fatto dimenticare il valore degli altri ambiti che pure costituiscono la compliance normativa aziendale: l'aggiornamento continuo in tema di sicurezza sul lavoro, l'analisi delle recenti posizioni di giurisprudenza per quanto attiene l'antiriciclaggio,i contenuti sempre caldi delle normative HACCP e sicurezza ambientale continuano a rappresentare settori essenziali per uno sviluppo aziendale cosciente ed efficace, da tenere costantemente sotto controllo. Tramite approfondimenti quindi, studi e pareri su informazioni inerenti allo sviluppo di impresa, resta ferma la sfida Saev volta a decifrare ed interpretare per prima le nuove discipline in modo da permettere alle aziende di prevedere in tempo reale occasioni ed opportunità possibili di crescita favorendo incrementi ed innovazioni dell'impresa.

Buona lettura

1 I SERVIZI SAEV

2 COMPLIANCE

- La compliance normativa: un'opportunità da cogliere

3 EDIZIONE SPECIALE: IL D.P.O.

- Tratti e lineamenti della figura introdotta da Reg. UE. n.679/16
- Il D.P.O. un valore aggiunto per le Imprese
- Data Protection Officer - Nuova figura principe del sistema Privacy negli Enti Pubblici
- Il Servizio D.P.O. Saev

9 PRIVACY

- La tutela dei dati personali nei Comuni - Il ruolo chiave del Segretario Comunale
- Un confronto tra il nuovo diritto all'oblio ed il vecchio diritto di cancellazione

14 ANTIRICICLAGGIO

- L'astensione dalla prestazione in caso di segnalazione delle operazioni sospette
- Il caso dei Compro Oro - Nuovi obblighi in materia di Antiriciclaggio

18 RESPONSABILITA' DEGLI ENTI

- Il M.O.G. - punto di contatto tra D.lgs. 231/01 e T.U. 81/08

20 SICUREZZA SUL LAVORO

- Il contrasto ai rischi di interferenza - Il D.U.V.R.I.
- Il particolare caso del "Condominio commerciale"
- Quando un segnale può salvare una vita

26 HACCP

- I buoni propositi - Allenamento, palestra, piscina...e salute!

27 SICUREZZA AMBIENTALE

- Un nuovo presidio a tutela dell'ambiente - Gli Eco-Reati

Vuoi evitare dubbi, difficoltà,

problemi derivanti da adempimenti normativi?

AFFIDATI A SAEV

- *Personale qualificato*
- *Risposte immediate*
- *Garanzia di conformità*

PROFESSIONISTI NELLA

COMPLIANCE NORMATIVA

- *SICUREZZA AMBIENTALE (D.Lgs. 152/06)*
- *ANTIRICICLAGGIO (D.Lgs. 231/07)*
- *HACCP (D.Lgs. 193/07 e Reg. CE 852/04)*
- *PRIVACY (D.Lgs. 196/03 e Reg. UE 679/16)*
- *RESPONSABILITA' DEGLI ENTI (D.Lgs. 231/01)*
- *SICUREZZA SUI LUOGHI DI LAVORO (D.Lgs 81/0*

CONTATTACI

Tel. 0731 21 56 39

Viale Don Minzoni, 3/f 60035 JESI (AN)

saev@saev.biz

LA COMPLIANCE NORMATIVA: UN'OPPORTUNITA' DA COGLIERE

Nonostante la nostra società manifesti sempre più chiaramente un senso di repulsione nei confronti del concetto di responsabilità e delle sue implicazioni, sempre più spesso le imprese operanti nel tessuto economico italiano mutano la propria struttura organizzativa al fine di attuare la funzione di compliance in modo tempestivo.

Ma cosa si intende per compliance? Perché, oltre ad essere posta in primo piano dal legislatore italiano, è ritenuta così importante dalle suddette imprese? Il termine compliance, che ha radici nel verbo latino complere, traducibile con "compiere" o "completare", pur rifacendosi in epoca contemporanea al verbo inglese to comply, traducibile con "rispettare", indica la conformità ad una determinata indicazione: in ambito sanitario per esempio misura il livello di collaborazione offerto dal paziente nel seguire le prescrizioni elaborate dal proprio medico, mentre in ambito legale lo stesso definisce il livello di conformità di un'azienda alla legislazione disciplinante la propria attività.

Non a caso, la compliance normativa è stata posta all'attenzione del legislatore soltanto recentemente, ponendosi principalmente come argine agli scandali finanziari che hanno minato gli ultimi decenni di storia, una volta riconosciuta l'opportunità di operare un maggiore controllo a livello statale su determinate attività a rischio: così, il suo ruolo istituzionale consiste nel monitorare in un'ottica preventiva i rischi di carattere legale e reputazionale.

Inoltre, dal momento che l'ordinamento in materia risulta recentemente sempre più improntata ad una limitata prescrittività, offrendo alle imprese un ampio margine di manovra, è importante sottolineare che tale normativa comporti una notevole responsabilizzazione delle stesse, tanto da presentarsi come un'opportunità da cogliere per distinguersi dai competitors sul mercato, anziché come un odioso adempimento obbligatorio.

Allora, risulta ormai fondamentale rivolgersi a professionisti specializzati per conseguire il necessario adeguamento, in modo da compiere un vero e proprio salto di qualità a livello reputazionale, oltre a porsi al riparo dalle sanzioni eventualmente erogabili dalle Autorità competenti.

NASCE IL D.P.O. - TRATTI E LINEAMENTI DELLA FIGURA INTRODOTTA DAL Reg. UE n.679/16

Il Regolamento Europeo n. 679/2016 introduce mediante il suo art. 37 la figura del D.P.O. stabilendo i principi sulla base dei quali il titolare del trattamento è tenuto a nominarlo.
In particolare, il D.P.O.:

- "è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39" del Regolamento, ex c. 5;
- "può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi", ex c. 6;
- in caso di gruppo imprenditoriale, può essere unico, "a condizione che (...) sia facilmente raggiungibile da ciascuno stabilimento", ex c. 2;
- in caso di ente pubblico, può essere unico "per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione", ex c. 3.

Inoltre, l'art. 38 integra il requisito di competenza previsto dall'art. 37, c. 5 del Regolamento stesso, stabilendo che il D.P.O.:

- "è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membro", ex c. 4;
- deve essere rifornito dal titolare del trattamento delle "risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica", ex c. 2;
- deve essere "tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali" dal titolare del trattamento, ex c. 1;
- non deve ricevere "alcuna istruzione per quanto riguarda l'esecuzione di tali compiti", ex c. 3;
- non deve essere "rimosso o penalizzato dal titolare del trattamento (...) per l'adempimento dei propri compiti", ex c. 3;
- "può svolgere altri compiti e funzioni", qualora il titolare del trattamento garantisca "che tali compiti e funzioni non diano adito a un conflitto di interessi", ex c. 5.

Infine, l'art. 39 del Regolamento completa la definizione del D.P.O. affermando che i suoi compiti devono essere svolti considerando "debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo", ex c. 2:

- "sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo", ex c. 1, lett. b;
- "informare e fornire consulenza al titolare del trattamento (...) nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati", ex c. 1, lett. a;
- "fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento", ex c. 1, lett. c;
- "cooperare con l'autorità di controllo", ex c. 1, lett. d;
- "fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento (...) ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione", ex c. 1, lett. e.

IL D.P.O. - UN VALORE AGGIUNTO PER LE IMPRESE

Con l'emanazione del Nuovo Regolamento della Privacy entrato in vigore il 24 maggio 2016 il Legislatore Europeo ha introdotto obblighi e vincoli stringenti alle imprese in materia di trattamento dei dati personali.

Per trattamento dei dati personali in garante intende qualunque operazione o complesso di operazioni che abbia per oggetto dati personali. Possono allora ricomprendersi tra le altre attività, la raccolta, la registrazione, l'organizzazione, la conservazione, la modificazione, la selezione, l'estrazione, l'utilizzo, il blocco, la la comunicazione, la diffusione, cancellazione e la distruzione di dati. In ogni fase dell'esercizio dell'attività l'impresa entra in contatto con numerosi dati personali, dalla prima relazione con il cliente, all'erogazione del servizio o alla cessione del prodotto all' utenza, e in ognuna di queste fasi è fondamentale che siano garantiti il rispetto e l'osservanza da parte del dell'azienda dei precetti legislativi.

Esaminiamo a questo punto quali adempimenti comporta in concreto l'obbligo di adeguamento delle imprese alla normativa europea più recente. Sulla base di una iniziale valutazione dello stato di adeguamento dell'azienda stessa (assessment), sarà a questo punto necessario provvedere alla predisposizione di un piano di adeguamento concordato tra le parti fino alla concretizzazione nell'elaborazione ed implementazione delle procedure previste dal Regolamento quali tra tutte:

- la tenuta di un registro delle Attività da parte del Titolare e del Responsabile del trattamento,

- l'obbligo di effettuare una Valutazione d'Impatto (VIA)

- l'obbligo di notifica e comunicazione dei Data Breach;

- l'osservanza dei principi di Privacy by design e privacy By default

- il rispetto dei diritti degli interessati in special modo Diritto all'oblio e diritto alla portabilità dei dati.

Ovviamente anche per le imprese che presentino tutti i requisiti necessari all'assoggettamento alla nuova normativa privacy, **vige l'obbligo di nominare un D.P.O.**, da intendersi quale Titolare del Trattamento dei dati".

la nomina del d.p.o. e la crescita della figura all'interno dell'organico aziendale, devono essere considerate dalle imprese obbligate come opportunità ed occasioni di sviluppo ed innovazione dell'intera organizzazione. Fondamentale in questo senso risulterà allora la formazione di tutti gli attori del sistema privacy all'interno della struttura d'impresa. Tutti coloro che gravitano intorno all'apparato del trattamento dei dati dovranno avere perfetta conoscenza della materia e saranno chiamati ad un continuo aggiornamento sulla base dell'evoluzione normativa. In questo senso si sottolinea come, analogamente a quanto già indicato per gli enti pubblici, anche per le grandi aziende sarà possibile nominare un D.P.O. internamente individuando un soggetto che sia già parte dell'organico aziendale, o al contrario una figura esterna, dotata dei titoli essenziali da individuare tra figure esperte di normativa, informatica, risk management, legale e sicurezza aziendale principalmente incaricate del controllo di conformità al GDPR tramite società di consulenza ed ausilio alle aziende. In entrambi i casi comunque il soggetto designato dovrà necessariamente avere la competenza fondamentale allo svolgimento del ruolo, formato adeguatamente ed adeguatamente aggiornato.

A differenza di quanto accade in ambito di pubblica amministrazione (in cui tutti gli enti sono assoggettati alle disposizioni ex Reg. U.E. 679/16) con riferimento alle aziende, vi sono presupposti e requisiti considerati essenziali a che l'impresa possa considerarsi obbligata alle regole europee. Si prevede cioè che solo le imprese impegnate nell'attività di trattamento dei dati in larga scala debbano considerarsi obbligate all'adeguamento dei parametri normativi introdotti dalla nuova disciplina.

L'art. 37 infatti obbliga *"… b) le attività principali del titolare del trattamento o del responsabile del trattamento consistano in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedano il monitoraggio regolare e sistematico degli interessati su larga scala; oppure*
c)le attività principali del Titolare del trattamento o del Responsabile del trattamento consistano nel trattamento, su larga scala , di categorie particolari di dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché nel trattamento di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale la persona, o dati relativi a condanne penali e a reati."

Dubbi sono sorti in merito al requisito introdotto dal Regolamento con il termine "larga scala". Non fornendo il Garante Europeo una definizione puntuale di "trattamento su larga scala", un ausilio potrebbe derivare dalla previsione operata nel "considerando" n. 91 in cui il rimando è ai *"trattamenti… che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato"*. Ugualmente, sempre sulla base del dettato dello stesso "considerato", il requisito della "larga scala" *"non dovrebbe valutarsi integrato qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato"*.
In ogni caso, le linee guida emanate allo scopo di orientare ad interpretazione univoca il nuovo Regolamento ha previsto che la valutazione dell'attività di trattamento dei dati su "larga scala possa essere operata sulla base dell'analisi dei criteri di:

- numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- durata, ovvero la persistenza, dell'attività di trattamento;
- portata geografica dell'attività di trattamento.

Ad ogni diritto si sa corrisponde un dovere e ad ogni violazione si collega una sanzione. Anche alle imprese allora dovranno considerarsi applicabili le sanzioni, amministrative pecuniari già esaminate con riferimento agli enti pubblici, definite dagli artt. 83 e ss. del **Nuovo Regolamento: fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente** per omesso o inidoneo consenso on line di minori (art. 8), identificazione non necessaria dell'interessato (art.11), violazione dei principi della privacy by design e privacy by default (art. 25), violazione degli obblighi di contitolari, rappresentanti e responsabili del trattamento (artt. Da 26 a 29), omessa istituzione e tenuta del registro del trattamento (art. 30), omessa cooperazione con il garante (art. 31), omessa adozione di misure di sicurezza (art. 32), omessa notificazione e comunicazione di violazioni privacy (artt. 33 e 34), omessa o inidonea valutazione d'impatto sulla protezione dei dati e consultazione preventiva (artt. 35 e 36), violazione degli obblighi di designazione del DPO (artt. da 37 a 39) **fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente** per violazione dei principi fondamentali privacy (artt. 5-6), omesso consenso privacy (art 7), trattamento illecito di categorie particolari di dati (art. 9), omessa o inidonea informativa all'interessato (artt. da 12 a 14), violazione dei diritti dell'interessato (artt. da 15 a 21), profilazione e trattamento automatizzato illecito o non autorizzato (art. 22), trasferimento di dati personali all'estero illecito o non autorizzato (art. da 44 a 49), violazione di disposizioni statali su specifici trattamenti (artt. da 85 a 91), omessa informazione o esibizione al garante privacy (art. 8), inosservanza di provvedimenti del garante (art. 58.2) .

IL D.P.O. - LA NUOVA FIGURA PRINCIPE DEL SISTEMA PRIVACY NEGLI ENTI PUBBLICI

Il Nuovo Regolamento Europeo in materia di trattamento dei dati personali n. 679/16 introduce l'obbligo per le Amministrazioni Pubbliche di dotarsi di un D.P.O. (Data Protection Officer) deputato alla titolarità delle attività inerenti al trattamento dei dati.

Sulla base delle esperienze collaudate di paesi membri quali Germania, Ungheria, e Francia (in cui in realtà il D.P.O. esiste già da anni ma con carattere meramente facoltativo) finalmente anche in Italia il tema del trattamento dei dati personali torna ad essere al centro dei dibattiti legislativi e di conseguenza si impone l'obbligo di designare figure valide e capaci a cui assegnare compiti di vigilanza e controllo, il D.P.O. appunto.

Entro la data limite del 25 maggio 2018, infatti, gli enti pubblici dovranno obbligatoriamente addivenire alla nomina del D.P.O. individuandolo in un soggetto esterno o interno, in modo tale da garantire la realizzazione di un sistema di organizzazione rispettoso dei principi di compliance in materia di protezione dei dati personali.

E' bene sgomberare subito il campo da eventuali equivoci: tutte le amministrazioni pubbliche, in quanto tali, sono da considerarsi destinatarie del suddetto obbligo, poiché sulla base delle disposizioni del Garante, l'obbligatorietà dell'adeguamento alla normativa comunitaria non dipende tanto dalla tipologia dell'ente destinatario (dimensione, valore, ...), quanto più *dall'insieme delle attività che lo stesso compie in materia di trattamento dei dati personali.*

L'art. 37 del nuovo Regolamento infatti stabilisce espressamente che il Titolare del trattamento e il Responsabile del trattamento designino sistematicamente un "Responsabile della Protezione dei dati" o Data Protection Officer ogni qualvolta "il trattamento sia effettuato da un'Autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitino le loro funzioni giurisdizionali".

Ora, appurata la tassatività dell'obbligo di nomina del D.P.O. alle Amministrazioni Pubbliche prevista dal Garante Europeo, analizziamo i compiti e gli oneri che a questa nuova figura lo stesso Garante riconosce ed attribuisce:

- informare e fornire consulenza al Titolare o al Responsabile del trattamento, nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dallo stesso Regolamento e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

- sorvegliare l'osservanza del Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati, nonché delle politiche del Titolare o del Responsabile del trattamento in materia di protezione dei dati personali, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento;

- cooperare con l'Autorità garante per la protezione dei dati personali;

- fungere da punto di contatto con la stessa Autorità garante per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento, ed effettuare, se del caso, consultazioni relative a qualunque altra questione.

Chi può essere nominato D.P.O.? Data la qualità ed il valore delle attività che il D.P.O. sarà chiamato a svolgere, in primis assumere la responsabilità delle funzioni di verifica e supervisione e garanzia delle varie attività concernenti il trattamento dei dati personali, è fondamentale che questi sia un soggetto capace e competente in materia di privacy, adeguatamente formato ed aggiornato anche con l'ausilio di professionisti esterni.

Il Data Protection Officer potrà essere individuato internamente, tra il personale dipendente in organico, oppure esternamente, procedendo ad un affidamento dell'incarico ad un soggetto terzo, in base a un contratto di servizi. In entrambi i casi comunque, perché la nomina risulti il più possibile trasparente e garantista, si impone la pubblicità e la comunicazione dei dati relativi al Titolare o dal Responsabile del trattamento (in modo che gli interessati possano contattarlo per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti) all'Autorità garante per la protezione dei dati personali.

Il carattere obbligatorio della previsione ex art. 37 del Nuovo Regolamento U.E. è ancor più rafforzato dall'apparato sanzionatorio ad esso collegato. Il Garante infatti prevede sanzioni pesanti e rilevanti per gli enti che, derogando al termine ultimo del 25 maggio 2018 a quella data non risultino in linea con le previsioni europee.

Si prevedono sanzioni amministrative pecuniarie fino a 10.000.000€, per: omesso o inidoneo consenso on line di minori (art. 8) identificazione non necessaria de3ll'interessato (art.11), violazione dei principi della privacy by design e privacy by default (art. 25), violazione degli obblighi di contitolari, rappresentanti e responsabili del trattamento (artt. da26 a 29) omessa istituzione e tenuta del registro del trattamento (art. 30), omessa cooperazione con il garante (art. 31) omessa adozione di misure di sicurezza (art. 32), omessa notificazione e comunicazione di violazioni privacy (artt. 33 e 34), omessa o inidonea valutazione d'impatto sulla protezione dei dati e consultazione preventiva (artt. 35 e 36), violazione degli obblighi di designazione del D.P.O. (artt. da 37 a 39).

Ammontano addirittura a 20.000.000€ invece le sanzioni conseguenti a reati di: violazione dei principi fondamentali privacy (artt. 5-6), omesso consenso privacy (art 7), trattamento illecito di categorie particolari di dati (art. 9), omessa o inidonea informativa all'interessato (artt. da 12 a 14), violazione dei diritti dell'interessato (artt. da 15 a 21), profilazione e trattamento automatizzato

SERVIZIO SAEV Data Protection Officer (D.P.O.):

- OPERA IN TRANQUILLITA' E NEL RISPETTO DEL NUOVO REGOLAMENTO EUROPEO 679/16!
- NOMINA IL TUO D.P.O., GARANTISCI LA CONFORMITA' ALLA LEGGE DELLA TUA ATTIVITA' E ASSICURATI LA BUSINESS CONTINUTY

SAEV GROUP E' L'ALLEATO GIUSTO!

UN TEAM DI ESPERTI E PROFESSIONISTI E'AL TUO SERVIZIO PER PROMUOVERE IL CORRETTO ADEGUAMENTO DELL'ENTE PUBBLICO E PRIVATO ALLA NUOVA NORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI:

- VISITA PRESSO LA TUA SEDE E VALUTAZIONE DELLO STATO DI ADEGUAMENTO
- NOMINA ESTERNA DEL D.P.O. SAEV
- INDIVIDUAZIONE, FORMAZIONE E CERTIFICAZIONE DEL D.P.O. INTERNO

IN OGNI CASO TI ASSICURIAMO:

ASSISTENZA CONTINUA E SUPPORTO COSTANTE NEI PROCESSI DI RIFORMA ED INNOVAZIONE DELL'ENTE PUBBLICO E PRIVATO (INTERVENTI DI CONTROLLO, CORSI DI FORMAZIONE ED AGGIORNAMENTO AL D.P.O, AUDIT PERIODICI.

AFFIDANDOTI ALLA SAEV POTRAI CONTARE SU PERSONALE PREPARATO E CERTIFICATO, SU D.P.O FORMATI E VALIDI CHE TI SARANNO DI AUSILIO NELL'ADEMPIMENTO DEI NUOVI OBBLIGHI IMPOSTI DAL REGOLAMENTO U.E.

LA TUTELA DEI DATI PERSONALI NEI COMUNI - IL RUOLO CHIAVE DEL SEGRETARIO COMUNALE

Il Regolamento Europeo n. 679/2016 sancisce nel suo art. 37, c. 1 che il titolare del trattamento è tenuto a nominare "sistematicamente un responsabile della protezione dei dati" o Data Protection Officer (D.P.O.) qualora il trattamento di dati personali sia "effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali".

Inoltre, l'art. 37, c. 3 del Regolamento prevede che "qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione".

Sebbene non sia presente nella normativa italiana una definizione univoca di autorità pubblica o organismo pubblico, si può evidentemente annoverare il Comune tra tali enti e, in particolare, tra gli enti locali, quindi è necessario che ciascuno di essi nomini un D.P.O. entro il 25 maggio del 2018, data di applicazione del Regolamento ai sensi del suo art. 99, c. 2, mediante apposito provvedimento del sindaco, qualificabile come titolare del trattamento ai sensi dell'art. 4, n. 7 di tale Regolamento, in quanto "autorità pubblica (...) che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali", come chiarisce l'art. 50 del d.lgs. n. 267/2000, rubricato Testo unico delle leggi sull'ordinamento degli enti locali (T.U.E.L.), stabilendo che "il sindaco e il presidente della provincia sono gli organi responsabili dell'amministrazione del comune e della provincia" (c. 1) e "sovrintendono al funzionamento dei servizi e degli uffici e all'esecuzione degli atti" (c. 2).

Come sopra evidenziato, mediante la suddetta nomina, il D.P.O. potrà essere abilitato ad operare per conto di una molteplicità di autorità pubbliche o organismi pubblici, qualora la struttura organizzativa di questi ultimi lo consenta e, quindi, qualora dal delicato bilanciamento tra principio di economicità e principio di efficacia operato dalle autorità pubbliche preposte emerga una simile opportunità. In questo ambito, sarà interessante capire se i Comuni opteranno più per la riduzione dei costi o più per la congruenza dell'adeguamento.

Tuttavia, chiarito ciò, sorge spontanea una domanda di non poco conto: chi può essere nominato D.P.O. in un Comune?

Alla suddetta domanda il Regolamento risponde, da un lato, con il suo art. 37, c. 6, stabilendo che "il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento (...) oppure assolvere i suoi compiti in base a un contratto di servizi" e, dall'altro, con il suo

art. 37, c. 5 prescrivendo che "il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39" del Regolamento stesso.

Così, nel procedimento di selezione del D.P.O. i Comuni saranno innanzitutto tenuti a valutare l'alternativa tra la nomina di un professionista esterno o la nomina di un proprio dipendente competente e da formare adeguatamente ed

in maniera continuata, operando nuovamente il suddetto bilanciamento tra principi dell'attività amministrativa. Ovviamente, alla luce di tale alternativa, le imprese già impegnate nel settore della compliance provvederanno ad adeguare a loro volta le proprie strutture organizzative per soddisfare eventuali richieste di nomina o formazione.

Inoltre, il D.P.O., i cui dati di contatto sono pubblicati e comunicati al Garante per la protezione dei dati personali da parte del titolare del trattamento ai sensi dell'art. 37, c. 7 del Regolamento, deve essere dotato del massimo grado di autonomia, come previsto dall'art. 38, c. 3 dello stesso, quindi non deve ricevere "alcuna istruzione per quanto riguarda l'esecuzione" dei suoi compiti e non può essere "rimosso o penalizzato (...) per l'adempimento dei propri compiti", oltre ad essere tenuto a riferire "direttamente al vertice gerarchico del titolare del trattamento".

Infine, il D.P.O. "può svolgere altri compiti e funzioni", a patto che questi ultimi "non diano adito a un conflitto di interessi", come previsto dall'art. 38, c. 6 del Regolamento, poiché lo svolgimento dei suoi compiti istituzionali, previsti dall'art. 39, c. 1 dello stesso, rappresenta l'unica garanzia effettiva di compliance in materia di tutela dei dati personali dell'ente per cui esso opera.

I suddetti rilievi, soprattutto quello inerente al massimo grado di autonomia e quello inerente all'assenza di conflitto di interessi, inducono a ritenere nominabile come D.P.O. in un Comune soltanto il segretario comunale, che è nominato ai sensi dell'art. 99, c. 1 del T.U.E.L. dal sindaco "tra gli iscritti" all'Albo nazionale dei segretari comunali e provinciali, al fine di svolgere, da un lato, "compiti di collaborazione e funzioni di assistenza giuridico-amministrativa nei confronti degli organi dell'ente in ordine alla conformità dell'azione amministrativa alle leggi, allo statuto ed ai regolamenti", come previsto dall'art. 97, c. 2 del T.U.E.L. medesimo e, dall'altro, le funzioni di cui al secondo paragrafo dell'art. 97, c. 4 dello stesso: appare evidente che tali funzioni non si prestino a dare adito ad un conflitto di interessi con i compiti istituzionali attribuiti al D.P.O. dal Regolamento.

Il segretario comunale costituisce un organo pubblico nato dall'evoluzione della figura del cancelliere del comune, risalente all'XI secolo d.C. e recentemente sopravvissuto alla condanna sancita dall'art. 11, c. 1, lett. b, n. 4 della l. n. 124/2015, rubricata Deleghe al governo in materia di riorganizzazione delle amministrazioni pubbliche, in virtù dell'intervento dissuasivo operato dalla Sent. n. 251/2016 della Corte costituzionale.

La nomina di tale organo, che "dipende funzionalmente dal capo dell'amministrazione" ai sensi dell'art. 99, c. 1 del T.U.E.L., ha "durata corrispondente a quella del mandato del sindaco (...) che

lo ha nominato, come previsto dall'art. 99, c. 2 del T.U.E.L. medesimo, salva revoca ai sensi dell'art. 100 dello stesso "con provvedimento motivato del sindaco (...), previa deliberazione della giunta, per violazione dei doveri d'ufficio".

Tali disposizioni possono indurre a pensare che vi siano due insormontabili ostacoli alla nomina come D.P.O. del segretario comunale, quello della limitatezza della durata della sua nomina e quello della limitatezza della sua autonomia.

Tuttavia, mentre per quanto riguarda la prima obiezione il secondo periodo dell'art. 99, c. 2 del T.U.E.L. chiarisce che "il segretario cessa automaticamente dall'incarico con la cessazione del mandato del sindaco (...), continuando ad esercitare le funzioni sino alla nomina del nuovo segretario" e, quindi, non sussiste la possibilità di una vacatio né della sua funzione né della eventualmente coincidente funzione di D.P.O., per quanto riguarda la seconda obiezione è difficile trascurare il combinato disposto della dipendenza funzionale e della facoltà di revoca, sebbene questa ultima sia limitata alla sussistenza di una violazione dei doveri d'ufficio, che però risulta ampiamente interpretabile.

In aggiunta, si sottolinea che il primo paragrafo dell'art. 97, c. 4 del T.U.E.L. prevede che "il segretario sovrintende allo svolgimento delle funzioni dei dirigenti e ne coordina l'attività, salvo quando (...) il sindaco e il presidente della provincia abbiano nominato il direttore generale": tale disposizione, infatti, da un lato, ripropone con maggiore veemenza la questione della limitatezza dell'autonomia del segretario comunale, obbligandolo a svolgere compiti manageriali nei comuni con popolazione inferiore a 100'000 abitanti, in virtù del divieto di nomina del direttore generale presso tali comuni previsto dall'art. 2, c. 186, l. d della l. n. 191/2009, rubricata Legge finanziaria 2010 e, dall'altro, focalizza l'attenzione sul tema del conflitto di interessi tra funzioni non compatibili tra loro, producendo una deleteria coincidenza tra controllore e controllato.

Ad oggi, in ogni caso, l'orientamento maggioritario è quello che, riconoscendo il segretario comunale quale organo pubblico addetto al mero controllo di legittimità, presume la compatibilità dello stesso con il ruolo del D.P.O. nei comuni, venendo così incontro alle esigenze economico-finanziarie dell'Ente che in questo modo risulteranno adeguatamente tutelate.

UN CONFRONTO TRA IL NUOVO DIRITTO ALL'OBLIO ED IL VECCHIO DIRITTO DI CANCELLAZIONE: CHE COSA CAMBIA A PARTIRE DAL 25 MAGGIO 2018?

Con la pronuncia datata 28 giugno 2017 n. 296, il Garante ha dichiarato il "non luogo a provvedere" ai sensi dell'art. 149, c. 2 del D.lgs. n. 196/2003 (Codice) in seguito all'adesione spontanea della società resistente, Il Giornale on line s.r.l., in qualità di titolare del trattamento, alla richiesta inviata dall'interessato in merito all'"immediata rimozione dal sito web" del suddetto titolare "di un articolo del 2014 che lo ha riguardato".

L'interessato, coinvolto nella celeberrima "vicenda relativa alla locazione ad un noto politico di un immobile del quale egli sarebbe stato erroneamente indicato quale proprietario", ha esercitato il diritto di cancellazione previsto dall'art. 7, c. 3, lett. b del Codice in virtù del fatto che il suddetto immobile "sarebbe appartenuto ad una società della quale egli era stato, per un certo periodo, amministratore", riservandosi di esercitare in subordine il diritto di rettifica previsto dall'art. 7, c. 3, lett. a del Codice.

Il titolare, a sua volta, ricevuta la comunicazione inviata dal Garante ai sensi dell'art. 149, c. 1 del Codice, ha provveduto, sebbene non nel termine di 10 giorni previsto dallo stesso c. ma "nel corso del procedimento", a fornire un "riscontro sufficiente alla richiesta del ricorrente" mediante la dichiarazione in un'apposita nota di "avere posto in essere, 'in data successiva al deposito del ricorso, tutte le azioni necessarie finalizzate alla deindicizzazione e rimozione dalla rete dell'articolo'".

Sorvolando sulla veridicità di tale dichiarazione, comunque soggetta alla disciplina dell'art. 168 del Codice (reclusione da sei mesi a tre anni, salvo che il fatto costituisca più grave reato, in caso di dichiarazione di notizie o circostanze false in un procedimento dinanzi al Garante), è bene soffermarsi sui cambiamenti che la normativa europea apporterà dal 25 maggio 2018, data di applicazione del Regolamento U.E. n. 679/2016 ai sensi del suo art. 99, c. 2, all'esercizio da parte dell'interessato del diritto di cancellazione previsto dall'art. 17 dello stesso.

In particolare oltre ad avvalersi preventivamente del potenziato diritto di accesso ai sensi dell'art. 15 del Regolamento, l'interessato potrà invocare il proprio diritto di cancellazione, fruendo di un'ulteriore garanzia di tutela.

Evidentemente, il diritto di cancellazione rappresenta un'extrema ratio, dal momento che l'interessato può intervenire contro un eventuale abuso posto in essere dal titolare del trattamento mediante anzitutto il diritto di rettifica ai sensi dell'art. 16 del Regolamento in più con il diritto di limitazione previsto dall'art. 18 del Regolamento, che ha profondamente riformato il diritto di bloc-

co previsto dall'art. 7, c. 3, lett. c del Codice.

Tuttavia, l'interessato, qualora decida di esercitare il diritto di cancellazione, sarà in grado di "ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano" (come già previsto dalla normativa italiana ai sensi dell'art. 7, c. 3, lett. b del Codice) "senza ingiustificato ritardo" e, a sua ulteriore tutela, l'obbligo in capo al titolare del trattamento, qualora abbia reso pubblici dati personali, "tenendo conto della tecnologia disponibile e dei costi di attuazione" ad adottare le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali" (novità introdotta dalla normativa europea), come previsto dall'art. 17 del Regolamento.

Quindi, in primis, l'interessato di cui al sopra enunciato caso avrebbe potuto ricorrere al Garante anche in caso di un'eccessiva attesa imposta dal titolare del trattamento nella cancellazione dei propri dati personali, obbligando, da un lato, tale titolare ad agire con tempestività e, dall'altro, la sua impresa ad adottare "misure tecniche e organizzative adeguate", come previsto dall'art. 25, c. 1 del Regolamento, per garantire tale tempestività, affidandosi a professionisti specializzati per conseguire il necessario adeguamento.

In secundis è necessario porre l'attenzione sull'impatto positivo esercitato sulla tutela dell'interessato dal nuovo obbligo per il titolare del trattamento pubblicante dati personali: nel sopra enunciato caso, infatti, l'interessato avrebbe potuto chiedere al titolare del trattamento, oltre alla cancellazione dei propri dati personali pubblicati, la comunicazione a tutti i titolari del trattamento fruitori di tale pubblicazione di eliminare ogni traccia degli stessi. Non a caso, la dottrina qualifica ormai univocamente il potenziato diritto di cancellazione previsto dall'art. 17 del Regolamento come 'diritto all'oblio', anche sulla base della recente giurisprudenza della Corte di giustizia dell'Unione europea.

Infine, a ciò va aggiunto che ai sensi dell'art. 17, c. 1 dello stesso l'interessato può esercitare tale diritto soltanto nel caso in cui i "dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati", ex lett. a o i "dati personali sono stati trattati illecitamente", ex lett. d (come già previsto dalla normativa italiana ai sensi dell'art. 7, c. 3, lett. b del Codice), ma anche nel caso in cui l'"interessato revoca il consenso su cui si basa il consenso" e "non sussiste altro fondamento giuridico per il trattamento", ex lett. b, l'"interessato si oppone al trattamento" e "non sussiste alcun motivo legittimo prevalente per procedere al trattamento", ex lett. c, i "dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento", ex lett. e o i "dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione" ai minori, ex lett. f (novità introdotta dalla normativa europea). Anche in questo caso, risulta evidente che il legislatore europeo ha operato un potenziamento della tutela dell'interessato mediante l'ampliamento del novero di presupposti legali all'esercizio del potenziato diritto di cancellazione, anche se l'interessato di cui al sopra enunciato caso non ne avrebbe avuto bisogno.

Andando oltre il suddetto caso, l'importanza del nuovo diritto di cancellazione si può cogliere ancora meglio nel considerare il caso delle fake news, che sta minando inesorabilmente la credibilità della rete negli ultimi anni: riuscirà tale diritto di cancellazione a costituire un argine efficace ad una simile piaga?

L'ASTENSIONE DALLA PRESTAZIONE IN CASO DI SEGNALAZIONE DELLE OPERAZIONI SOSPETTE: UN'ANALISI CRITICA

L'art. 41 del d.lgs. 231/07 disciplina, in materia di tutela contro l'antiriciclaggio, l'obbligo di segnalazione delle operazioni sospette.

Secondo il dettato normativo i soggetti obbligati, prima di compiere l'operazione, devono inviare senza ritardo alla UIF (Unità di informazione finanziaria per l'Italia) una segnalazione di operazione sospetta "quando sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo o che comunque i fondi, indipendentemente dalla loro entità, provengano da attività criminosa".

Il decreto poi specifica quali sono gli indici dai quali desumere il "sospetto", anche in base agli indicatori di anomalia elaborati e periodicamente aggiornati dalla UIF.

Salvo casi specificamente indicati, l'operazione può essere compiuta solo dopo che è stata effettuata la segnalazione.

La segnalazione deve contenere dati, informazioni, descrizione delle operazioni ed i motivi del sospetto.

Sono esonerati dall'obbligo di segnalazione delle operazioni sospette i professionisti per le informazioni che ricevono da un loro cliente o ottengono riguardo allo stesso nel corso dell›esame della posizione giuridica o dell›espletamento dei compiti di difesa o di rappresentanza del medesimo in un procedimento innanzi a un›autorità giudiziaria o in relazione a tale procedimento, anche tramite una convenzione di negoziazione assistita da uno o più avvocati ai sensi di legge, compresa la consulenza sull'eventualità di intentarlo o evitarlo, ove tali infor-

mazioni siano ricevute o ottenute prima, durante o dopo il procedimento stesso.

Per i professionisti, la segnalazione di operazione sospetta deve essere inviata direttamente alla UIF ovvero agli organismi di autoregolamentazione (in questo caso un apposito decreto ministeriale stabilirà le specifiche e le modalità e garanzie di tutela della riservatezza dell›identità del segnalante).

Gli organismi di autoregolamentazione, ricevuta la segnalazione da parte dei propri iscritti, devono senza ritardo a trasmetterla integralmente alla UIF priva del nominativo del segnalante.

Per non vanificare gli obblighi di segnalazione e non esporre a rischi la persona del segnalante sono previste una serie di misure volte a tutelarne l'identità: anzitutto i soggetti obbligati e gli organismi di autoregolamentazione devono adottare tutte le misure idonee ad assicurare la riservatezza dell'identità dei segnalanti

Di contro, l'autorità giudiziaria è chiamata ad adottare le misure necessarie ad assicurare che l'identità del segnalante sia mantenuta riservata; il nominativo del segnalante non può essere inserito nel fascicolo del Pubblico Ministero né in quello per il dibattimento, e la sua identità non può essere rivelata, salvo che l'Autorità giudiziaria non disponga altrimenti, con provvedimento motivato ed assicurando l'adozione di ogni accorgimento idoneo a tutelare il segnalante se indispensabile ai fini dell'accertamento dei reati per i quali si procede, disponendo che, in caso di denuncia o comunicazione di notizia di reato non è fatta menzione dell›identità del segnalante, anche se conosciuta.

E' fatto divieto ai soggetti tenuti alla segnalazione di un'operazione sospetta e a chiunque ne sia comunque a conoscenza, di dare comunicazione al cliente interessato o a terzi dell'avvenuta segnalazione, dell'invio di ulteriori informazioni richieste dalla UIF o dell'esistenza ovvero della probabilità di indagini o approfondimenti in materia di riciclaggio o di finanziamento del terrorismo.

Si precisa che il tentativo del professionista di dissuadere il cliente dal porre in atto un'attività illegale non costituisce violazione del divieto di comunicazione previsto dal presente articolo.

Quando un soggetto si trovi nell'impossibilità oggettiva di effettuare l'adeguata verifica della clientela, questi sarà obbligato ad astenersi dall'instaurare, eseguire o proseguire il rapporto, la prestazione professionale e le operazioni e valutano se effettuare una segnalazione di operazione sospetta alla UIF.

Il legislatore infine regola le casistiche, tassative, in cui è previsto un esonero all'obbligo di astensione: ogni qualvolta l'obbligato esamini la posizione giuridica del proprio cliente o espliciti compiti di difesa o di rappresentanza del cliente in un procedimento innanzi a un›autorità giudiziaria o in relazione a tale procedimento; l'esonero è esteso anche alla consulenza sull›eventualità di intentare o evitare il procedimento.

L'obbligo di astensione vale anche in relazione alle prestazioni di cui siano, direttamente o indirettamente, parte società fiduciarie, trust, società anonime o controllate aventi sede in Paesi terzi ad alto rischio.

IL CASO DEI COMPRO ORO: NUOVI OBBLIGHI IN MATERIA DI ANTIRICICLAGGIO

Il Decreto Legislativo 25 maggio 2017, n. 90, pubblicato sulla Gazzetta Ufficiale n. 141 del 20 giugno 2017, disciplina specificamente le nuove regole per l'esercizio dell'attività di compro oro.

Il presente decreto detta disposizioni specifiche per la definizione degli obblighi cui gli operatori compro oro sono tenuti al fine di garantire la piena tracciabilità della compravendita e permuta di oggetti preziosi usati e la prevenzione dell'utilizzo del relativo mercato per finalità illegali, con specifico riferimento al riciclaggio di denaro e al reimpiego di proventi di attività illecite.

Vediamo quali sono le principali novità introdotte dal decreto entrato in vigore lo scorso mese di luglio:

anzitutto una ri-definizione dell'attività stessa di "compro oro" quale attività commerciale consistente nel compimento di operazioni di compro oro, esercitata in via esclusiva ovvero in via secondaria rispetto all'attività prevalente. Si impone inoltre agli operatori del mercato del compro oro l'iscrizione al registro degli operatori compro oro professionali, obbligatorio quando si tratti di amministratori diversi dalle banche, istituito presso l'O.A.M. (Organismo per la gestione degli elenchi degli agenti in attività finanziaria e dei mediatori creditizi);

Al fine di garantire in primis l'utenza dei compro oro e ancora di più la legittimità del mercato all'interno del quale questi operano, il legislatore ha imposto che per potersi iscrivere nel registro l'operatore deve essere in possesso della licenza per l'attività in materia di oggetti preziosi di cui all'art. 127 del Testo Unico di Pubblica Sicurezza.

Per quanto attiene ai termini e alle modalità di svolgimento dell'attività tipica del compro oro, la nuova normativa definisce nuovi obblighi di identificazione della clientela: prima di eseguire l'operazione l'operatore deve identificare il cliente in base alla normativa antiriciclaggio (art 18 del D Lgs 90/17).

Per ogni operazione di compro oro effettuata occorre compilare una scheda numerata pro-

gressivamente indicante una serie di elementi, fra i quali: i dati identificativi del cliente, il prezzo pagato e il mezzo di pagamento, la descrizione sintetica dell›oggetto prezioso, la quotazione dell'oro e dei metalli preziosi contenuti nell'oggetto, due fotografie dell'oggetto prezioso, ecc ... Al termine di ciascuna compravendita gli operatori rilasciano al cliente una ricevuta riepilogativa delle informazioni sopra elencate, informative e documenti che dovranno obbligatoriamente essere conservati per almeno 10 anni dal Titolare dell'attività.

Il legislatore ha riconosciuto anche un ruolo di controllo e sorveglianza agli operatori del settore del compro-oro: ogni qualvolta una operazioni risulti lasci adito a dubbi e perplessità, questi sono tenuti ad inviare all'UIF le segnalazioni di operazioni sospette secondo le norme in tema di antiriciclaggio (decreto legislativo n. 231/2007, nel testo modificato dal decreto legislativo n. 90/2017 che entrerà in vigore dal prossimo 4 luglio;

Fondamentale è poi l'ulteriore previsione del limite di 500 euro per l'uso del contante: la soglia è stata abbassata da 1.000 euro a 500 euro con la conseguenza che le operazioni di importo pari o superiore a 500 euro possono essere eseguite esclusivamente con mezzi di pagamento diversi dal denaro contante, che garantiscano la tracciabilità dell'operazione e la sua univoca riconducibilità al disponente

Più restrittivo è divenuto anche il sistema sanzionatorio: reclusione e multa fino ad un massimo di 4 anni e 10.000 euro per chi operi in assenza di regolare iscrizione al registro e sanzioni amministrative pecuniarie fino a 1.500 euro per l'inosservanza degli obblighi di comunicazione all'OAM (in caso di violazioni gravi, ripetute o sistematiche, la sanzione è triplicata; se la comunicazione avviene nei 30 gg. successivi dalla scadenza dei termini prescritti, la sanzione è ridotta a 500 euro: il procedimento sanzionatorio è attribuito alla competenza dell'OAM; da 5.000 a 50.000 per l'omessa o tardiva segnalazione di operazione sospetta.

I poteri di controllo sono affidati in via principale alla Guardia di Finanza; le sanzioni amministrative pecuniarie sono irrogate con decreto dal Ministero dell'economia e delle finanze e il relativo procedimento sanzionatorio è regolato dalla Legge n. 689/1981. Qualora accerti l'esistenza di due violazioni commesse nel triennio, la Guardia di finanza propone al Ministero quale sanzione accessoria la sospensione dell›esercizio dell›attività da 15 giorni a 3 mesi; l'inosservanza del provvedimento di sospensione è punita con la sanzione amministrativa pecuniaria da 10.000 a 30.000 euro.

IL M.O.G. - PUNTO DI CONTATTO TRA D.lgs. 231/01 E T.U.81/08

Il Modello Organizzativo di Gestione (M.O.G.), espressamente definito e regolato all'interno del d.lgs. n. 81/2008, rubricato Testo unico in materia di tutela di salute e sicurezza sui luoghi di lavoro (T.U.S.S.L.L.), è ulteriormente richiamato quale presupposto esimente di responsabilità dall'art. 6 del d.lgs. 231/01, rubricato Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica.

A tal proposito, l'art. 30 del T.U.S.S.L.L. stabilisce che il M.O.G. elaborato dall'ente, perché sia considerato idoneo a svolgere la sua efficacia esimente in riferimento alla responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica di cui al d.lgs. n. 231/2001, debba essere adottato ed efficacemente attuato.

Inoltre, la norma chiarisce che è il M.O.G. stesso a prevedere sistemi e mezzi di controllo atti a garantire l'osservanza delle previsioni in esso contenute e soprattutto ad assicurare il mantenimento e l'innovazione continua delle misure adottate come idonee col perdurare del tempo.

Tuttavia, è innegabile che la normativa sulla modalità di svolgimento e redazione del M.O.G. sia minata da lacune che ne rendono difficile l'interpretazione: non a caso, il T.U.S.S.L.L. si limita a riportare taluni elementi in via di principio essenziali alla formulazione del M.O.G., senza per questo definirne la struttura ed il preciso contenuto, come stabilisce l'art. 30 c. 2, 3, 4 del d.lgs. n. 81/2008, qui di seguito riportato.

"2. Il modello organizzativo e gestionale di cui al comma 1 deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività di cui al comma 1.

3. Il modello organizzativo deve in ogni caso prevedere, per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

4. Il modello organizzativo deve altresì prevedere un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

5. In sede di prima applicazione, i modelli di organizzazione aziendale definiti conformemente alle Linee guida UNI-INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) del 28 settembre 2001 o al British Standard OHSAS 18001:2007 si presumono conformi ai requisiti di cui al presente articolo per le parti corrispondenti. Agli stessi fini ulteriori modelli di organizzazione e gestione aziendale possono essere indicati dalla Commissione di cui all'articolo 6."

Accade quindi spesso che l'imprenditore sia costretto, in assenza di indicazioni precise e puntuali, a fare riferimento a modelli ed archetipi che se pure elaborati dalle associazioni di categoria sulle linee dettate dal Ministero della Giustizia, non garantiscono l'idoneità a prescindere.

D'altro canto, i modelli di organizzazione e gestione disciplinati dall'art.6 del d.lgs. n. 81/2008, che pure compaiono nella normativa in materia di responsabilità amministrativa degli enti, rappresentano un elemento di forte contatto tra le due discipline: essi cioè costituiscono il prodotto un sistema di prevenzione del rischio c.d. "complesso".

Così. pur definendo le modalità di procedimentalizzazione delle decisioni per lo sviluppo di una migliore organizzazione aziendale in ambito di salute e sicurezza sul lavoro, le suddette disposizioni si limitano a richiamare contenuti e presupposti riportati nella disciplina antinfortunistica.

Dall'analisi di quanto detto emerge, chiaro ed inequivocabile, il richiamo dell'art.30 del T.U. all'art. 6 del d.lgs. n. 231/2001, in quanto entrambi trattano di modelli organizzativi, ma, la vera domanda è la seguente: il legislatore ha inteso disciplinare lo stesso modello o modelli differenti?

La dottrina avanza a riguardo tre ipotesi:

- potrebbe ritenersi che il modello ex art. 30 del T.U.S.S.L.L. integri il modello ex art.6 del d.lgs. n. 81/2008 introducendo così ulteriori e specifici obblighi giuridici in materia di tutela della salute e sicurezza sui luoghi di lavoro;

- potrebbe derivarne che il modello ex art. 30 del d.lgs. n. 81/2008 sostituisca il modello di cui all'art. 6 del d.lgs. n. 231/01 nella parte corrispondente alla sicurezza sul lavoro costituendone così una parte speciale rispetto a quella prevista dal d.lgs. n. 231/2001;

- il modello ex art.30 del T.U.S.S.L.L. si aggiungerebbe a quello previsto dall'art.6 del d.lgs. n. 231/2001 conservando la propria autonomia e specificità:in questa ipotesi i modelli organizzativi sarebbero allora due diversi.

Infine, posti i suddetti rilievi, è bene chiarire che l'orientamento maggioritario tanto in dottrina quanto in giurisprudenza è quello secondo il quale la previsione ex art. 30 del d.lgs. n. 81/2008 costituisce una disciplina complementare a quella più ampia del d.lgs. n. 231/2001.

Dunque, pare ineccepibile che il M.O.G. paventato dal T.U.S.S.L.L., costituendo il sistema "primario" di tutela e prevenzione del rischio, vada ad affiancarsi come parte speciale alla legislazione più generale e di ampio respiro prevista dall'art. 6 del d.lgs. n. 231/2001 al fine di creare un programma di tutela e garanzia il più esaustivo, effettivo ed efficace possibile.

IL CONTRASTO AI RISCHI DI INTERFERENZA IL D.U.V.R.I.

I luoghi di lavoro e le attività produttive sono, costantemente ed irrimediabilmente, soggette ad interferenze e contatti tra soggetti e mezzi operativi chiamati a svolgere attività diverse spesso all'interno di uno stesso luogo di lavoro.

In particolare, per interferenza lavorativa deve intendersi l'ipotesi in cui più operatori afferenti ad aziende diverse, prestano la loro opera (contestualmente o meno) sullo stesso luogo di lavoro: è quindi il caso in cui diverse realtà lavorative con ragioni sociali e datori di lavoro differenti, lavorino nello stesso sito, nello stesso momento, o anche in alcuni casi in successione se comunque gli effetti del lavoro di chi precede possono ricadere in qualche modo su chi interviene successivamente.

Accade in questi casi che poiché ciascun lavoratore nell'eseguire la propria prestazione apporta dei rischi sul luogo di lavoro, la compresenza di più soggetti attori, possa in qualche modo generare delle sovrapposizioni con un aumento del livello di rischio ed una diversa tipologia di pericolo presente sul sito. Il T.U. sulla salute e sicurezza sui luoghi di lavoro, regolamenta e definisce situazioni di questo tipo all'art 26: "Obblighi connessi ai contratti d'appalto o d'opera o di somministrazione". Di regola infatti è propriamente nell'ambito di appalti e somministrazioni che vengono a crearsi le situazioni di interferenza oggetto della nostra analisi. si precisa che con "contratti di appalto" la legge intende definire la relazione tra un committente (pubblico o privato) ed un'impresa terza che riceve l'incarico per specifiche attività, nel "contratto d'opera" le attività definite dal contratto vengono svolte da un prestatore d'opera autonomo o dal titolare di una ditta individuale, mentre nei "contratti di somministrazione" il fornitore assicura prestazioni periodiche o continuative di cose o servizi. In tutti questi casi si integra un contatto ed una interferenza tra soggetti ai quali spettano oneri e responsabilità diversi.
I termini e le valutazioni dei rischi da interferenza confluiscono nel Documento Unico di Valutazione dei Rischi Interferenziali (DUVRI), un documento in cui il datore di lavoro che ha la disponibilità giuridica dei luoghi dove si svolge l'appalto, effettua la valutazione dei rischi presenti ed elabora le misure preventive e protettive rivolte ad eliminarli o ridurli al minimo.
E' ovvio che nella scelta della ditta appaltante, il committente debba ricercare un soggetto rispettoso della normativa in grado di provare la propria affidabilità in termini di gestione ed organizzazione della propria attività economica. L'interesse del committente, dunque, è nel senso di realizzare, attraverso lo strumento del DUVRI, una vera e sostanziale azione di coordinamento e di informazione nei confronti della propria controparte contrattuale".

In questo senso il DUVRI non è solo un obbligo penalmente sanzionato, ma è "un importante strumento in mano al committente per effettuare una reale valutazione dell'adeguatezza dell'organizzazione del sistema di sicurezza approntato dall'appaltatore, attraverso il coordinamento tra i Responsabili del Servizio di Prevenzione e Protezione (RSPP) del committente e dell'appaltatore".
Di regola il DUVRI non si considera obbligatorio quando il servizio di di natura intellettuale o nel caso in cui la durata del rapporto tra le varie imprese sia inferiore a 5 giorni.
Al contrario il documento andrà sempre redatto, anche quindi per attività di durata inferiore ai cinque giorni, nei casi in cui la valutazione del rischio incendio risulti elevato o in tutte le attività svolte in ambienti confinati o in cui vi sia presenza di agenti cancerogeni, mutageni, biologici, di amianto o di atmosfere esplosive, nonché nelle attività che presentino rischi particolari elencate nell'allegato XI del D.Lgs. 81/08.

IL PARTICOLARE CASO DEL "CONDOMINIO COMMERCIALE"

Il centro commerciale costituisce una realtà particolarmente strutturata e complessivamente difficile da definire tanto da un punto di vista civilistico che penalistico. Per questo motivo allora, per creare un parallelismo con elementi già conosciuti e disciplinati dall'ordinamento, la giurisprudenza ha ritenuto opportuno applicare al centro commerciale le disposizioni e le definizioni elaborate dal codice per il condominio. Tanto nel centro commerciale, infatti, che nel condominio, sussiste una condizione di comunione di spazi di tipo forzoso nella quale accanto alla proprietà esclusiva di singole unità facenti parte dell'edificio è presente un regime di comproprietà di tutti i condomini su alcune parti dell'edificio stesso. Più semplicemente quindi il Centro Commerciale, composto da negozi di proprietà esclusiva di diversi soggetti, costituisce una particolare forma di condominio con destinazione commerciale.

La gestione delle parti comuni da parte di personale diverso però costituisce spesso un'attività complessa atta a richiedere lo svolgimento di diverse funzioni, dagli adempimenti amministrativi e autorizzativi a quelli fiscali, senza tralasciare l'ambito inerente l'attività di vigilanza e di gestione della sicurezza.

Accade di norma allora che, per ragioni strategico-economiche ed organizzative, i proprietari delle unità immobiliari della Galleria del Centro Commerciale costituiscano una Società Consortile o un Consorzio, al fine di promuovere e sviluppare l'immagine e le attività imprenditoriali svolte nel centro commerciale, ivi compresa l'attività di gestione delle parti comuni. Si provvede cioè alla formazione di una "Società di Gestione" del centro commerciale deputata a diventare responsabile di quanto accade all'interno degli spazi comuni del centro.

Ne deriva la necessità di individuare soggetti e personale che abbiano le competenze indispensabili per svolgere adeguatamente tali funzioni.

Con particolare riferimento al tema dell'applicazione della tutela della salute e sicurezza dei lavoratori all'interno dei locali dei centri commerciali, occorre innanzitutto precisare che le modalità di applicazione della legge risulterà diversa a seconda che l'evento dannoso conseguente ad una condotta illecita si verifichi all'interno degli spazi di proprietà dei singoli negozi o nelle parti comuni del centro commerciale.

Nel primo caso è chiaro che il rispetto della normativa sulla sicurezza sui luoghi di lavoro prevista dal TU 81/08 debba essere demandato ai singoli titolari dei negozi facenti parte del centro commerciale. Questo significa che all'interno dei singoli punti vendita presenti nel centro commerciale ogni realtà aziendale dovrà provvedere autonomamente all'adeguamento alla normativa in materia di salute e sicurezza sui luoghi di lavoro. Dovranno perciò prevedersi la redazione della documentazione essenziale e l' individuazione delle figure fondamentali (datore di lavoro, dirigente, preposto, RSPP, ecc.) oltre

a tutti gli altri adempimenti richiesti dal T.U. Si offre in esempio il caso dei supermercati, quasi normalmente presenti nei centri commerciali: nel caso in cui si verifichino infortuni che interessino tanto i lavoratori quanto l'utenza presente all'interno del negozio, la Corte Suprema ha più volte pronunciato sentenze che imputano al solo datore di lavoro del supermercato la responsabilità dell'evento dannoso e, di conseguenza l'obbligo al risarcimento e al pagamento dei danni.

Tra tutte, si cita una recente pronuncia della Suprema Corte che, a seguito di un infortunio occorso ad una dipendente mentre apriva il cancello di accesso carrabile, ha condannato il dirigente del punto vendita, in quanto, pur in assenza di specifiche deleghe in materia di sicurezza, aveva tenuto un atteggiamento passivo consistito nell'aver omesso di segnalare alla direzione le precarie condizioni di sicurezza del cancello di cui era a conoscenza e nel non essersi adoperato per il ripristino dello stesso o per non averne impedito l'uso da parte dei lavoratori (Cass. Pen. n. 3947 del 31/01/2012).

Più complesso è altresì definire i ruoli e i termini delle responsabilità per quanto concerne invece infortuni ed incidenti occorsi all'interno dello spazio comune del centro commerciale. Laddove l'infortunio riguardi lavoratori che si trovavano al momento dell'evento dannoso in uno spazio non direttamente di proprietà di una singola attività commerciale, si tratta cioè di capire chi sia obbligato a rispondere di tale condotta illecita.

In prima battuta la risposta più ovvia al problema sembrerebbe quella volta ad imputare la responsabilità per questo tipo di incidenti ed infortuni alla Società di Gestione, direttrice dei luoghi in comunione all'interno del centro. Senonché di regola una Società di Gestione non opera mai direttamente all'interno del parco commerciale, affidando al contrario la responsabilità dell'esecuzione dell'attività di gestione e direzione del Centro ad una società specializzata in materia (cd "Società di Servizi").

La delega delle funzioni di esecuzione dalla società di gestione a quella di servizi, la rete delle relazioni giuridiche ed economiche tra le due imprese costituiscono elementi importanti anche per quello che attiene la responsabilità in caso di incidenti ed infortuni all'interno del centro commerciale.

Occorre premettere che generalmente la So-

cietà di Gestione proprio in forza dell'affidamento ad altra società dei propri ruoli dirigenziali e organizzativi spesso non conta al proprio interno alcun dipendente né lavoratore. Che conseguenze si collegano a questo fatto in materia di sicurezza sul lavoro?

Ne deriva che per la Società di Gestione, senza personale alle proprie dipendenze, non trova applicazione il TU 81/08, fatto salvo per la casistica speciale del Titolo IV.

Il T.U. 81/08 ha infatti espressamente individuato i soggetti destinatari degli obblighi di sicurezza e salute sui luoghi di lavoro definendo il lavoratore come il "soggetto che, indipendentemente dalla tipologia contrattuale, svolge un'attività lavorativa nell'ambito dell'organizzazione di un datore di lavoro...", e di datore di lavoro come "soggetto titolare del rapporto di lavoro con il lavoratore ..." (art. 2, lett. a-b ex D.lgs. 81/08). In questo senso allora nessuno dei soggetti eventualmente coinvolti in incidenti e/o infortuni all'interno del centro commerciale (nelle parti comuni dello stesso), non potendo far valere alcun rapporto giuridico di lavoro con la Società di Gestione, potrebbe rivolgersi ad essa per il risarcimento del danno. Al massimo tale responsabilità potrebbe essere riconosciuta in capo alla società di servizi.

Diverso è il caso in cui l'infortunio coinvolga lavoratori dipendenti di ditte esterne (es. edili, impiantistiche etc.) alle quali la Società di Gestione abbia dato in appalto manutenzione e lavori parti comuni del centro commerciale.

Quando a subire l'infortunio infatti sia un lavoratore della ditta appaltatrice, una responsabilità in capo alla Società di Gestione sarebbe: come committente infatti la stessa sarebbe obbligata ai sensi del Titolo IV del D.lgs. 81/08 (cantieri temporanei o mobili) al rispetto degli obblighi previsti dall'art. 90 (obblighi del committente), tra i quali, in primis, la verifica dell'idoneità tecnico professionale di ciascun soggetto chiamato ad intervenire, ecc.

Ovvio che il mancato riconoscimento di responsabilità per violazione di norme in materia di sicurezza in capo alla Società di Gestione non possano costituire una giustificazione o un'esimente della stessa a dotarsi di tutti i dispositivi previsti da T.U. o a non adempiere agli obblighi imposti dal legislatore, poiché è indubbio che la gestione delle parti comuni del centro commerciale presenti notevoli profili di rischio in materia di sicurezza. Al di là dei limiti dell'applicabilità del TU 81/08 sopra descritti, è interesse della Società di Gestione porre in essere ogni presidio possibile al fine di prevenire infortuni e gestire nel migliore dei modi la sicurezza nelle parti comuni del centro commerciale.

Si tratta di un tema di particolare rilevanza per la Società di Gestione del centro commerciale che, in caso di infortunio, potrebbe in ogni caso incorrere anche in una imputazione di responsabilità penale-amministrativa ai sensi del D. Lgs. 231/01 che tra i reati presupposto indica proprio i reati di omicidio colposo e lesioni colpose gravi o gravissime commesse in violazione della normativa della sicurezza sui luoghi di lavoro.

QUANDO UN SEGNALE PUO' SALVARE UNA VITA

Il T.U. in materia di salute e sicurezza sui luoghi di lavoro agli artt. 161 ss. definisce l'obbligo in capo al datore di lavoro di "predisporre un'adeguata segnaletica di sicurezza all'interno degli spazi di lavoro sulla base della tipologia e degli indici di rischio presenti nell'esercizio dell'attività lavorativa emersi a seguito della valutazione dei rischi ex art. 28 del T.u.".

La segnaletica c.d. di sicurezza posta a tutela della sicurezza sul luogo di lavoro, è la segnaletica che, riferita ad un oggetto, ad una attività o ad una situazione determinata è all'uopo volta a fornire una indicazione o una prescrizione comportamentale specifica da tenere da tenere all'interno degli spazi di attività in situazioni particolarmente pericolose di modo da evitare infortuni o eventi pregiudizievoli, che utilizza, a seconda dei casi, un colore, un segnale luminoso o acustico, una comunicazione verbale o un segnale gestuale. Immediati e di rapida comprensibilità essi informano i lavoratori sui rischi ed i pericoli verificabili a certe condizioni.

D'altra parte, i segnali di sicurezza danno anche indicazioni in ordine alle vie di salvataggio e dove trovare soccorso in caso di emergenza.

Ovviamente la corretta applicazione delle disposizioni ex. artt. 161 ss del T.U. da parte del datore garantisce non soltanto il personale dipendente dell'impresa ma "In tema di prevenzione nei luoghi di lavoro, le norme antinfortunistiche non sono dettate soltanto per la tutela dei lavoratori nell'esercizio della loro attività, ma sono dettate anche a tutela dei terzi che si trovino nell'ambiente di lavoro, indipendentemente dall'esistenza di un rapporto di dipendenza con il titolare dell'impresa. (Cass. Penale n. 23147 del 17 aprile 2012 cfr. Cassazione Penale, Sez. 4, 18 dicembre 2014, n. 52658).

In questo senso ne consegue che quando si verifichino danni anche a soggetti terzi integranti i reati di lesioni o di omicidio colposi comprovati dalla mancanza o dall'inidoneità di tali mezzi di segnaletica del rischio, perché possa ravvisarsi l'ipotesi del fatto commesso con violazione delle norme dirette a prevenire gli infortuni sul lavoro, di cui agli artt. 589, comma secondo, e 590, comma terzo, c.p., nonché la perseguibilità d'ufficio delle lesioni gravi e gravissime, ex art. 590

c.p., è necessario e sufficiente che sussista tra siffatta violazione e l›evento dannoso un legame causale, il quale ricorre se il fatto sia ricollegabile all›inosservanza delle predette norme secondo i principi di cui agli artt. 40 e 41 c.p., e cioè sempre che la presenza di soggetto passivo estraneo all'attività ed all'ambiente di lavoro, nel luogo e nel momento dell'infortunio non rivesta carattere di anormalità, atipicità ed eccezionalità tali da fare ritenere interrotto il nesso eziologico tra l'evento e la condotta inosservante, e la norma violata miri a prevenire l'incidente verificatosi.".

L'obbligo previsto in capo al datore di fornirsi della segnaletica idonea agli spazi di esercizio della propria attività, definisce un onere preciso che non potrà in ogni caso limitarsi ad un sistema informativo basato esclusivamente sulla parola o su segnali improvvisati ma deve necessariamente prevedere l'uso di sistemi facilmente fruibili ed inequivocabili come individuati dalla normativa tecnica di riferimento.

Analizziamo allora quali sono, ai sensi del T.U. in materia di salute e sicurezza sul lavoro, i criteri da rispettare per una predisposizione di segnaletica di sicurezza idonea e rispettosa della normativa.

Considerato che ruolo primario della segnaletica è l'essere efficace nel dare un messaggio rapido e facilmente interpretabile, si considera essenziale alla corretta osservanza della normativa:

-evitare la disposizione ravvicinata di un numero di cartelli eccessivo, ciò al fine di favorirne l'individuazione e la comprensione del messaggio;

-non utilizzare contemporaneamente segnali che possano generare confusione tra di loro (es.: fornire messaggi contraddittori).

-rendere visibile la segnaletica da tutte le posizioni ritenute critiche rispetto al messaggio che si vuole fornire.

Affinché la segnaletica sia veramente efficace, è necessario predisporre un progetto globale che tenga in considerazione, oltre ai semplici aspetti normativi, anche quelli riguardanti: la fruibilità delle informazioni che si vogliono comunicare, la corretta manutenzione dei segnali, la regolare pulizia ed i materiali impiegati. Nella eventualità di segnalazioni che richiedono fonti di energia, é necessario assicurarsi che questa sia mantenuta anche in caso di guasto all'impianto elettrico.

Per quanto attiene al modus e ai termini di applicazione della segnaletica, c'è da sottolineare come però le norme tecniche del testo unico 81/08 debbano ritenersi integrate dalle previsioni predisposte dall'UNI (Ente Italiano di Unificazione). Per quanto concerne infatti segnalazioni "particolari", più specifiche (es. quella in materia antincendio), l'Italia si è vista obbligata a provvedere un adeguamento della propria normativa alle revisioni di livello continentale, definendo a tale scopo certificazioni e provvedimenti aventi efficacia riconosciuta a livello comunitario: è il caso della UNI 7543-1 in materia di Colori e segnali di sicurezza, che regola le prescrizioni generali di applicazione di tutti i segnali non espressamente definiti dalla legislazione del T.U. o della UNI EN ISO 7010:2012, una norma che prescrive i segnali di sicurezza da utilizzare nella prevenzione degli infortuni, nella protezione dal fuoco, per l'informazione sui pericoli alla salute e nelle evacuazioni di emergenza.

Per quel concerne gli obblighi imposti in materia di applicazione della segnaletica adeguata, si sottolinea che, in caso di mancata affissione della prevista cartellonistica sanzioni e obblighi di risarcimento ricadano sul datore di lavoro, sul responsabile del servizio di prevenzione protezione e sui preposti, a meno che, il lavoratore, pur formato ed informato tramite la segnaletica sui rischi prevedibili, tenendo un comportamento eccentrico ed imprevedibile (Cass. Penale Sez. IV. N. 27543 del 2017), si renda responsabile egli stesso dell'infortunio.

I BUONI PROPOSITI: ALLENAMENTO, PALESTRA, PISCINA...E SALUTE

Per HACCP (Hazard Analysis Critical Control Point- punti critici di controllo dell'analisi dei rischi) si intende un metodo di auto-controllo igienico sanitario che ogni soggetto impegnato nella produzione e manipolazione di alimenti deve attuare, con lo scopo di valutare pericoli e rischi per gli utenti ed, in base a questi, stabilire le misure di controllo più idonea tutelare la salute del consumatore.

Spesso, erroneamente siamo portati a pensare che la disciplina dell'HACCP interessi esclusivamente gli operatori del mercato alimentare e dunque i titolari di ristoranti, supermercati, bar, etc. etc. al contrario!

I destinatari degli obblighi previsti dal d. lgs. 193/07 sono molti di più e spesso si occupano di ambiti anche parecchio distanti da quello prettamente alimentare.

Paradossalmente allora anche chi gestisca una piscina, o addirittura una palestra dovrà considerarsi obbligato ad osservare le previsioni riguardanti la legge sull'igiene dei prodotti alimentari, ogni qualvolta all'interno delle proprie strutture sia prevista la presenza di un angolo ristoro che venda e/o fornisca bevande e cibi preparati e confezionati. L'esigenza primaria che si intende garantire infatti con l'applicazione delle norme HACCP è quella fondamentale di garantire la salubrità dei preparati alimentari tramite il monitoraggio del processo produttivo in tutti i suoi stati (compresa la vendita e la somministrazione), individuando fase dopo fase i rischi che potrebbero comportare un pregiudizio all'utenza in modo da attuare strumenti utili ad evitare tali danni.

Ma quali sono gli adempimenti necessari affinché una qualsiasi struttura risulti idonea e conforme alla legge in materia di HACCP?

Nel nostro esempio (la palestra e/ o la piscina) in cui non vi è preparazione né confezionamento ma solo somministrazione dei generi alimentari in primis sarà necessario dotarsi della idoneità igienico-sanitaria relativa ad ambienti, arredi ed attrezzature rilasciata dall'ASUR del distretto di appartenenza. Una volta che la certificazione sia stata concessa, sarà necessario avviare le pratiche della procedura ex. HACCP.

Anzitutto l'ente sarà chiamato a munirsi di un Manuale di Autocontrollo HACCP che racchiuda in sé tutte le procedure che l'impresa intende applicare per provare l'effettiva e corretta applicazione delle norme.

La valutazione HACCP dovrà essere predisposta sull'intera struttura dalle sale di allenamento (nel caso della palestra) alle vasche e alle pompe (nel caso delle piscine) ad bar e caffetterie presenti in struttura. Va da sé che il manuale rappresentando una cartina tornasole della diligenza del datore nel rispetto della disciplina di salute e igiene alimentare andrà aggiornato e modificato ogni qualvolta nella struttura dell'impresa verranno approvate modifiche ed innovazioni nei procedimenti e negli stadi che riguardano la somministrazione degli alimenti. Oltretutto sarà proprio questo documento che all'occorrenza dovrà essere presentato alle autorità in caso di controlli.

Non soltanto il datore di lavoro, ma tutto il personale della struttura che sia adibito a manipolazione di alimenti ,anche per successiva vendita, (dai cuochi, ai baristi, ai camerieri) sarà chiamato a partecipare al rispetto della normativa: anzitutto adempiendo agli obblighi e alle direttive datoriali dettate in materia di HACCP (utilizzo delle divise, osservanza delle elementari regole di pulizia,..) ma anche e soprattutto seguendo e partecipando ai corsi di formazione e relativi aggiornamenti (il corso ha validità 3 anni e consta di 12 ore di lezione)in materia di sicurezza alimentare fino all'ottenimento dell'attesto HACCP titolo di certificazione ed indicatore di garanzia per l'intera struttura.

UN NUOVO PRESIDIO A TUTELA DELL'AMBIENTE - GLI ECO REATI

Quando nel 2006 il legislatore ha disposto l'emanazione del d.lgs. n. 152/2006 rendendo esecutiva la normativa in materia di tutela ambientale, gli imprenditori hanno catalogato tale previsione tra i vari aggravamenti della loro normale attività. Il Parlamento infatti imponeva ulteriori obblighi e doveri da rispettare nell'esercizio dell'attività di impresa; si imponeva cioè una rivisitazione dei vari processi produttivi aziendali finalizzata a rendere le varie fasi di lavoro rispettose dei territori senza per questo perdere l'efficacia e la funzionalità necessaria alla crescita economica dell'ente.

Di fronte ad un primo periodo di inattività della normativa, poco applicata e scarsamente sanzionata anche dalle autorità, col tempo i datori di lavoro hanno imparato a gestire la tutela ambientale come parte della propria compliance aziendale, cogliendo i risvolti più positivi e le opportunità (certificazioni di qualità, innovazione delle mansioni, crescita dell'impresa, ecc.) da essa derivanti. Sarebbe scorretto però non riconoscere l'apporto dato allo sviluppo e al diffondersi del rispetto della tutela ambientale dal legislatore quando nel 2015 ha introdotto, modificando il codice penale, ampliandolo, il reato di "inquinamento ambientale" applicando sanzioni gravi e rilevanti agli imprenditori meno diligenti, come previsto dall'art. 452-bis del Codice penale:

E' punito con la reclusione da due a sei anni e con la multa da euro 10.000 a euro 100.000 chiunque abusivamente cagiona una compromissione o un deterioramento significativi e misurabili:

1) delle acque o dell'aria, o di porzioni estese o significative del suolo o del sottosuolo;

2) di un ecosistema, della biodiversità, anche agraria, della flora o della fauna.

Quando l'inquinamento è prodotto in un'area naturale protetta o sottoposta a vincolo paesaggistico, ambientale, storico, artistico, architettonico o archeologico, ovvero in danno di specie animali o vegetali protette, la pena è aumentata.

Proprio la previsione del reato di inquinamento ambientale ha dato avvio ad un processo (si spera il più lungo e duraturo possibile) di riconoscimento giuridico dei reati contro l'ambiente. Nel 2016 infatti la Corte di Cassazione, Sez. Penale, con la sentenza n. 46170/2016 (processo di bonifica dei fondali dei moli del Golfo di La Spezia) ha definito termini di applicazione del primo c.d. eco-reato effettivamente perseguito dalla legge. Convinti che la pronuncia in esame sia da considerarsi sentenza- pilota in materia di tutela ambientale e del territorio, prendiamo in esame i passi e gli interventi più importanti della sentenza in modo da capire come la Corte intenda combattere le condotte illecite poste in essere in danno dell'ecosistema.

saev
group

SAEV Srl | Viale Don Minzoni, 3/f 60035 JESI (AN) | t el. 0731.215639 - fax. 0731.205562
posta elettronica: **saev@saev.biz** - **www.saev.biz**