Circolare del 06 maggio 2021

INDICE

WHISTLEBLOWING, COSA CAMBIA CON L'IMPLEMENTAZIONE DELLA DIRETTIVA UE 2019/1937

Il 23 ottobre 2019 l'UE ha emanato la Direttiva 2019/1937 (di seguito la "Direttiva") sulla protezione delle persone che segnalano violazioni del diritto dell'Unione. Entro il 17 dicembre 2021 l'Italia dovrà implementare la Direttiva rendendola, così, applicabile alle società con almeno 250 lavoratori (mentre per le imprese con più di 50 dipendenti e meno di 250 le norme potranno entrare in vigore entro il 17 dicembre 2023).

L'Italia, con la Legge 179/2017 (di seguito la "Legge"), aveva già regolamentato le segnalazioni, disponendo un differente regime per gli enti pubblici e gli enti privati.

Esaminando la Direttiva e comparandola con la Legge con riferimento al solo settore privato, si notano numerosi e rilevanti differenze, che andremo ora ad esaminare brevemente.

Innanzitutto, ciò che emerge chiaramente dalla lettura delle due normative è che l'ambito di applicazione della disciplina sulle segnalazioni e piuttosto differente.

La Legge prevede l'applicazione della disciplina sulle segnalazioni solamente per violazioni del Modello o del DLGS 231/2001, mentre la Direttiva si applica solo a segnalazioni relative a violazioni del diritto dell'Unione.

Inoltre, la Direttiva si applica indistintamente al settore pubblico ed al settore privato, mentre la Legge distingue i due settori, regolandoli in maniera differente.

Ancora, tra le differenze di maggiore rilievo troviamo che mentre la Legge non specifica chi può segnalare (ma sembrerebbe essere rivolta ai soli dipendenti dell'Ente coinvolto nella violazione), la Direttiva considera segnalatori coloro che hanno acquisito informazioni sulle violazioni in un contesto lavorativo, gli azionisti e i membri dell'organo di amministrazione, direzione o vigilanza di un 'impresa, compresi i membri senza incarichi esecutivi, i volontari e i tirocinanti retribuiti e non retribuiti, nonché qualsiasi persona che lavora sotto la supervisione e la direzione di appaltatori, subappaltatori e fornitori, facilitatori, terzi connessi con le persone segnalanti e c he potrebbero rischiare ritorsioni in un contesto lavorativo, quali colleghi o parenti delle persone segnalanti.

È differente anche la risposta che le due normative forniscono alla domanda "quando si ha la tutela del segnalante?".

In base alla Legge, il segnalante beneficia della relativa tutela quando le segnalazioni di condotte illecite sono (i criteri sono cumulativi) circostanziate, rilevanti ai sensi del D.Lgs. 231/2001 od in base al Modello Organizzativo, fondate su elementi di fatto precisi e concordanti e quando il segnalante ha appreso la condotta illecita in ragione delle funzioni dallo stesso svolte.

Come si vede, il segnalante, in base alla Legge, deve – prima di effettuare la segnalazione – verificare attentamente se la segnalazione che intende effettuare ha tutte le caratteristiche per permettergli di ottenere la relativa tutela.

La Direttiva, invece, ha una struttura profondamente diversa e concede tutele al segnalante se questi:

a) aveva avuto fondati motivi di ritenere che le informazioni segnalate fossero vere al momento della segnalazione e che tali informazioni rientrassero nell'ambito di applicazione della direttiva;
b) ha effettuato una segnalazione attraverso i canali indicati dalla direttiva stessa.

Anche i canali di whistleblowing sono individuati in maniera differente dalla Legge e dalla Direttiva:

la Legge prevede uno o più canali, purché almeno uno di essi sia informatico, mentre la Direttiva individua 3 canali di segnalazione: ***interno, esterno*** e ***pubblico***.

Quando il soggetto ricevente la segnalazione acquisisce la segnalazione, in base alla Legge deve svolgere l'attività ritenuta necessaria, senza particolari regole.

In base alla Direttiva, invece, il ricevente deve inviare entro 7 giorni al segnalante una comunicazione di ricevimento della segnalazione ed entro 3 mesi dal riscontro della segnalazione deve comunicare al segnalante un "esito" della segnalazione.

L'obbligo di riservatezza in capo al ricevente è, poi, disciplinato diversamente nelle due normative, seppur si possa affermare che vi siano forti punti di contatto: la Legge afferma sinteticamente che deve essere garantita la riservatezza sull'identità del segnalante mentre la Direttiva è più chiara sostenendo che non solo deve essere garantita la riservatezza sull'identità del segnalante ma anche su quelle informazioni che possano farne scoprire l'identità, fatto salvo il diritto di difesa del segnalato (purché il segnalante sia avvertito anticipatamente della comunicazione dell'identità ed i motivi di tale scelta).

Ci si domanda, a questo punto: una volta che il segnalante ha effettuato la segnalazione, quali strumenti di protezione ha?

In base alla Legge, non possono essere adottate misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni, né tantomeno può essere posto in essere un licenziamento ritorsivo o discriminatorio del soggetto segnalante o disposto nei suoi confronti un mutamento di mansioni ai sensi dell'articolo 2103 del codice civile, nonché qualsiasi altra misura ritorsiva o discriminatoria. Anzi, è onere del datore di lavoro, in caso di controversie legate all'irrogazione di sanzioni disciplinari, o a demansionamenti, licenziamenti, trasferimenti, o sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro, successivi alla presentazione della segnalazione, dimostrare che tali misure sono fondate su ragioni estranee alla segnalazione stessa.

Anche la Direttiva fornisce al segnalante una serie di protezioni: **sono**, infatti, **vietati** nei confronti del segnalante:

a) il licenziamento, la sospensione o misure equivalenti;

b) la retrocessione di grado o la mancata promozione;

c) il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;

d) la sospensione della formazione;

e) note di merito o referenze negative;

f) l'imposizione o amministrazione di misure disciplinari, la nota di biasimo o altra sanzione, anche pecuniaria;

g) la coercizione, l'intimidazione, le molestie o l'ostracismo;

h) la discriminazione, il trattamento svantaggioso o iniquo;

i) la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro permanente, laddove il lavoratore avesse legittime aspettative di vedersi offrire un impiego permanente;

j) il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;

k) danni, anche alla reputazione della persona, in particolare sui social media, o la perdita finanziaria, comprese la perdita di opportunità economiche e la perdita di reddito;

l) l'inserimento nelle liste nere sulla base di un accordo settoriale o industriale formale o informale, che possono com-portare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro;

m) la conclusione anticipata o l'annullamento del contratto per beni o servizi;

n) l'annullamento di una licenza o di un permesso;

o) la sottoposizione ad accertamenti psichiatrici o medici

La Direttiva, poi, aggiunge alle misure di protezione nei confronti del segnalante, anche delle misure di sostegno. Al segnalante devono essere, così, fornite

- informazioni e consulenze esaustive e indipendenti titolo gratuito sulle procedure e i mezzi di ricorso disponibili in materia di protezione dalle ritorsioni e sui diritti della persona coinvolta;
- un 'assistenza efficace da parte delle autorità competenti per la protezione dalle ritorsioni,
- patrocinio a spese dello Stato nell'ambito di un procedimento penale e di un procedimento civile transfrontaliero
- assistenza finanziaria e sostegno, anche psicologico, nell'ambito dei procedimenti giudiziari.

La Direttiva, dunque, appare essere più organica, più precisa e garantista nei confronti dei segnalatori e soprattutto ha una specificità, anche tecnica, ben maggiore della Legge.

L'entrata in vigore della Direttiva, dunque, comporterà la necessità da parte della Pubblica Amministrazione, delle imprese ed anche da parte delle associazioni che gravitano attorno al mondo del lavoro e dell'impresa di adeguarsi, implementando canali di whistleblowing, procedure, modalità di scambio di informazioni e così via. Insomma, l'aspettativa è che con l'implementazione della Direttiva si raggiunga un sistema di whistleblowing integrato, con una efficacia concreta ben maggiore di quella attuale.

DRAGHI: "IL NOSTRO GREEN PASS IN VIGORE DA METÀ DI MAGGIO". MA SI CONSULTI IL GARANTE PRIVACY

Il premier: "Il pass verde nazionale in vigore dalla seconda metà di maggio, quello europeo pienamente operativo da metà giusto". Ora il governo consulti il Garante per introdurre il certificato verde a prova di privacy.

L'Italia non aspetta i tempi dell'Europa e il green pass nazionale sarà obbligatorio dalla seconda metà di maggio sia per gli italiani, per entrare ed uscire dalle Regioni di colore rosso ed arancione per motivi di turismo, sia per i cittadini dell'Unione Europea che verranno in vacanza nel nostro Paese. L'ha annunciato il premier Mario Draghi, che ha invitato i turismi a prenotare le vacanze in Italia.

Draghi: "Il pass verde nazionale in vigore dalla seconda metà di maggio"

"Noi dobbiamo offrire regole chiare, semplici per garantire che i turisti possano venire da noi e viaggiare in Italia in sicurezza. A partire dalla seconda metà di giugno il certificato verde sarà pienamente operativo all'interno dell'Unione europea. Nell'attesa, non aspettiamo la metà di giugno, il governo italiano ha introdotto un pass verde nazionale, che permetterà alle persone di muoversi tra le Regioni ed entrerà in vigore a partire dalla seconda metà di maggio", ha detto Draghi introducendo le conclusioni del G20 del Turismo.

Green pass, i 3 requisiti per averlo

"Con il pass europeo, ha ricordato Draghi, "i turisti potranno spostarsi all'interno dell'Ue senza quarantena", a patto che possano dimostrare di:

- Avvenuta vaccinazione contro COVID. La durata è di 6 mesi, al momento, ma i sanitari chiedono che la validità sia almeno di 9 mesi, perché sarebbero già scoperti in estate, perché vaccinati a gennaio.
- guarigione dall'infezione da SARS-CoV-2, (validità di 6 mesi)
- l'effettuazione di un test molecolare o antigenico rapido con risultato negativo al virus.

Green pass sia in digitale sia stampabile con QR-Code

Ricordiamo che sia il pass italiano sia quello europeo sarà disponibile in versione digitale o stampabile: tutti i documenti dovranno contenere una firma qualifica e un QR-Code non falsificabile.

L'invito ai turisti, Draghi: "Prenotate le vacanze in Italia"

Al termine della conferenza stampa, Draghi si è rivolto direttamente ai turisti stranieri invitandoli a venire a trascorrere le vacanze in Italia, perché in sicurezza, grazie prima al green pass nazionale e poi a quello europeo, che prenderà il posto di quello italiano.

"È il momento di prenotare le vostre vacanze in Italia e naturalmente non vediamo l'ora di accogliervi di nuovo", ha concluso con un bel sorriso accogliente il premier.

Green pass, il Governo consulti il Garante Privacy

Ora, prima dell'entrata in vigore del green pass nazionale, il Governo è obbligato a fare quello che ancora non ha fatto: consultare il Garante Privacy, il cui parere è obbligatorio, ma non vincolante, per introdurre un certificato verde davvero a prova di privacy, perché il decreto legge che lo introduce presenza innumerevoli falle dal punto di vista della protezione dei dati, come rilevato dal Garante nel formale provvedimento di "avvertimento" inviato al Governo.

ANONIMIZZAZIONE DEI DATI: I 10 QUI-PRO-QUO SECONDO L'EDPS (*il Supervisor Europeo della protezione dei dati delle istituzioni e degli organi della UE*) E L'AEPD (*l'Autorità Garante spagnola per la protezione dei dati*)

Conoscere i più comuni fraintendimenti correlati all'anonimizzazione è il primo passo per evitare di esporre all'accesso di terzi non autorizzati informazioni anonimizzate solo in via presuntiva.

Non di rado ci si imbatte, per esempio all'interno di informative o di accordi per la nomina di responsabile del trattamento, in affermazioni del tipo "al termine del periodo di conservazione, i tuoi dati saranno anonimizzati e trattati per finalità statistiche" o "i dati, resi anonimi, potranno essere utilizzati per ulteriori finalità".

Ma siamo davvero sicuri che i dati di cui si parla vengano effettivamente anonimizzati?

Il significato di anonimo

Il concetto dell'anonimità è di primaria importanza ai fini della (dis)applicazione del GDPR, che, lo ricordiamo, non si applica al trattamento di informazioni anonime o sufficientemente anonime.

Conoscere i più comuni fraintendimenti correlati all'anonimizzazione è il primo passo da compiere al fine di acquisire maggiore consapevolezza ed evitare di incorrere in errori esponendo all'accesso di terzi non autorizzati informazioni anonimizzate solo in via presuntiva. L'EDPS e l'AEPD ne elencano dieci in un recente documento (https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf) pubblicato sui rispettivi siti istituzionali.

Il concetto di anonimizzazione

Prima di vedere quali, però, soffermiamoci brevemente su cosa debba intendersi con il termine dato "anonimizzato". È un concetto strettamente collegato all'identificabilità di una persona. Il considerando 26 del GDPR spiega che per essere considerati anonimi o sufficientemente anonimi ai sensi del GDPR, i dati, rispettivamente:

- non devono riferirsi a una persona fisica identificata o identificabile oppure
- devono impedire o non consentire più l'identificazione dell'interessato.

Il citato considerando prosegue chiarendo che per stabilire se una persona fisica è identificabile devono considerarsi tutti i mezzi di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare, direttamente o indirettamente, la persona a cui i dati si riferiscono.

GARANTE PRIVACY: AL VIA I LAVORI PER LE NUOVE REGOLE DEONTOLOGICHE IN AMBITO STATISTICO

Il Garante per la protezione dei dati personali avvia i lavori per le nuove Regole deontologiche per i trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema Statistico nazionale. Le Regole dovranno essere predisposte dall'ISTAT e dagli altri soggetti Sistan e poi approvate dall'Autorità, chiamata a verificarne la conformità al GDPR e al Codice privacy.

Le nuove Regole deontologiche sono strategiche in questo settore in ragione delle novità introdotte dal GDPR, delle rinnovate modalità di realizzazione della statistica ufficiale nel contesto europeo, nonché delle rilevanti evoluzioni tecnologiche intervenute negli ultimi anni.

Il Sistan è la rete di soggetti pubblici e privati che insieme all'ISTAT fornisce al Paese e agli organismi internazionali l'informazione statistica ufficiale.

Nella delibera, in corso di pubblicazione nella Gazzetta ufficiale, il Garante ha definito i criteri generali per individuare, nel rispetto del principio di rappresentatività, i soggetti chiamati a sottoscrivere le nuove regole nonché quelli interessati alla loro applicazione.

Il Garante invita quindi i soggetti pubblici e privati, che ritengano di avere titolo a sottoscrivere le Regole deontologiche, e i portatori di un interesse qualificato, che intendono partecipare ai lavori, a darne comunicazione e a fornire informazioni e documentazione all'Autorità all'indirizzo regoledeontologichesistan@gpdp.it, entro 60 giorni dalla pubblicazione del provvedimento sulla Gazzetta Ufficiale.

FACEBOOK NEL MIRINO: 'DATI PERSONALI DI MINORI VENDUTI ALLE SOCIETÀ DI ALCOL E TABACCO'

Questa volta i guai per Facebook arrivano dall'emisfero australe e riguardano sempre il trattamento dei dati degli utenti del popolare social. L'accusa stavolta, però, è tanto pesante quanto inquietante.

Secondo gli attivisti australiani di Reset (un'associazione mondiale di contrasto delle minacce digitali alla democrazia), la creatura di Mark Zuckerberg sembrerebbe adottare politiche scorrette in tema di trattamento dei dati, arrivando addirittura a usare le informazioni di navigazione degli adolescenti non solo all'interno del recinto della famosa piattaforma, ma anche al di fuori di essa, con grave pregiudizio per i fanciulli.

"Abbiamo accertato che non vi è differenza nella maniera in cui sono trattati i dati di adolescenti", si legge nel rapporto a firma del direttore esecutivo di Reset Australia, Chris Cooper. "Questo permette agli inserzionisti di comprare accesso a quei profili e di prendere di mira i giovanissimi attorno a interessi molto discutibili, come gioco d'azzardo, fumo e alcool, e anche di registrare lo status in siti di appuntamenti. È scioccante e preoccupante", ha aggiunto Cooper.

Secondo l'analisi degli esperti australiani, Facebook avrebbe raccolto le informazioni sui comportamenti online degli adolescenti, adottando anche un "pedinamento" digitale, seguendo le tracce dei giovanissimi non solo all'interno del social network ma anche fuori. Infatti, il j'accuse di Reset punta il dito proprio sullo spionaggio informatico adottato da Facebook ai danni dei ragazzi che, stando alle accuse mosse, verrebbero costantemente monitorati mentre navigano in Internet, con il risultato di raccogliere molte informazioni sulle loro abitudini, usi e preferenze online.

Tutte queste informazioni, successivamente, verrebbero vendute a terzi e usate per creare pubblicità personalizzate sui social, a partire dallo stesso Facebook.

"I profili personali sono quindi resi facilmente accessibili agli inserzionisti della piattaforma di Facebook. E il nostro esperimento ha dimostrato che Facebook approva pubblicità da cui gli adolescenti dovrebbero essere protetti" ha continuato Cooper. Da qui la richiesta di Reset al governo di Canberra di adottare misure per prevenire il mercimonio di dati appartenenti ai minori, sull'esempio di quanto già realizzato da Gran Bretagna e Irlanda.

CORONAPASS ALTO ADIGE: IL GARANTE PRIVACY AVVIA UN'INDAGINE

Il Garante ha aperto un'istruttoria sul progetto locale di "certificazione verde" COVID, avviato dalla Provincia autonoma di Bolzano.

In base alle dichiarazioni pubbliche rilasciate dall'Ente provinciale e al testo di una specifica ordinanza adottata dal suo Presidente, verosimilmente già dal 26 aprile solo i possessori del cosiddetto "CoronaPass Alto Adige" possono accedere a determinate strutture ricettive, luoghi ricreativi e di formazione, nonché partecipare ad altre attività, come eventi e pratiche sportive.

Il pass viene rilasciato solamente alle persone che hanno completato il ciclo di vaccinazione, a chi è guarito dal Covid o ha da poco eseguito un test negativo.

Come già segnalato al Governo in relazione al progetto nazionale di certificazione verde introdotto con il decreto "Riaperture", il Garante ribadisce che i trattamenti dei dati personali connessi all'avvio di iniziative che limitano fortemente i diritti e le libertà delle persone può avvenire solo nel quadro di un'idonea base giuridica a seguito di una valutazione dei rischi e con l'adozione di adeguate misure a tutela degli interessati.

Nella comunicazione trasmessa alla Provincia autonoma di Bolzano, il Garante segnala che si riserva ogni valutazione in ordine all'adozione di provvedimenti finalizzati ad imporre una limitazione provvisoria o definitiva del trattamento dei dati previsto nel progetto di certificazione verde locale, incluso il divieto di trattamento.

CONSIGLIO D'EUROPA: GLI STATI EUROPEI DEVONO INTENSIFICARE GLI SFORZI PER PROTEGGERE LA PRIVACY DEI MINORI NELL'AMBIENTE DIGITALE

Nel contesto della pandemia del COVID-19, gli Stati europei dovrebbero rafforzare le misure di protezione relative al trattamento dei dati personali dei minori, in particolar modo i dati riguardanti la loro salute e quelli raccolti nel quadro dell'istruzione, al fine di ridurre al minimo i potenziali effetti negativi, tra cui l'identificazione pubblica di un minore come portatore di COVID-19, ha affermato il Comitato dei Ministri del Consiglio d'Europa in una dichiarazione incentrata sulla protezione della privacy dei minori nell'ambiente digitale, adottata il 28 aprile 2021.

Il Comitato dei Ministri ha espresso preoccupazione per le conseguenze e l'impatto della pandemia del COVID-19 sui minori a causa dell'aumento delle attività online e dell'utilizzo di prodotti e servizi online, o dell'esclusione digitale.

Tuttavia, il Comitato dei Ministri ha riconosciuto anche le opportunità e i vantaggi degli strumenti online, come la didattica a distanza e la possibilità di rimanere in contatto con familiari e amici, e chiede agli Stati di "esercitare maggiore vigilanza" e adottare misure per ridurre il divario digitale tra i minori, affiché tutti possano godere appieno dei loro diritti umani.

Il Comitato dei Ministri ha ricordato che le tecnologie dell'informazione e della comunicazione sono, in generale, uno strumento importante nella vita dei minori, ma che il loro utilizzo può anche generare dei rischi.

In particolar modo, la tracciabilità delle attività dei minori nell'ambiente digitale può esporli ad attività criminali, come l'adescamento per scopi sessuali, l'estorsione sessuale, lo sfruttamento sessuale (tra cui lo sfruttamento di contenuti sessualmente espliciti generati da minori), o altre attività illegali o dannose, come la discriminazione, il bullismo, lo stalking e altre forme di molestie.