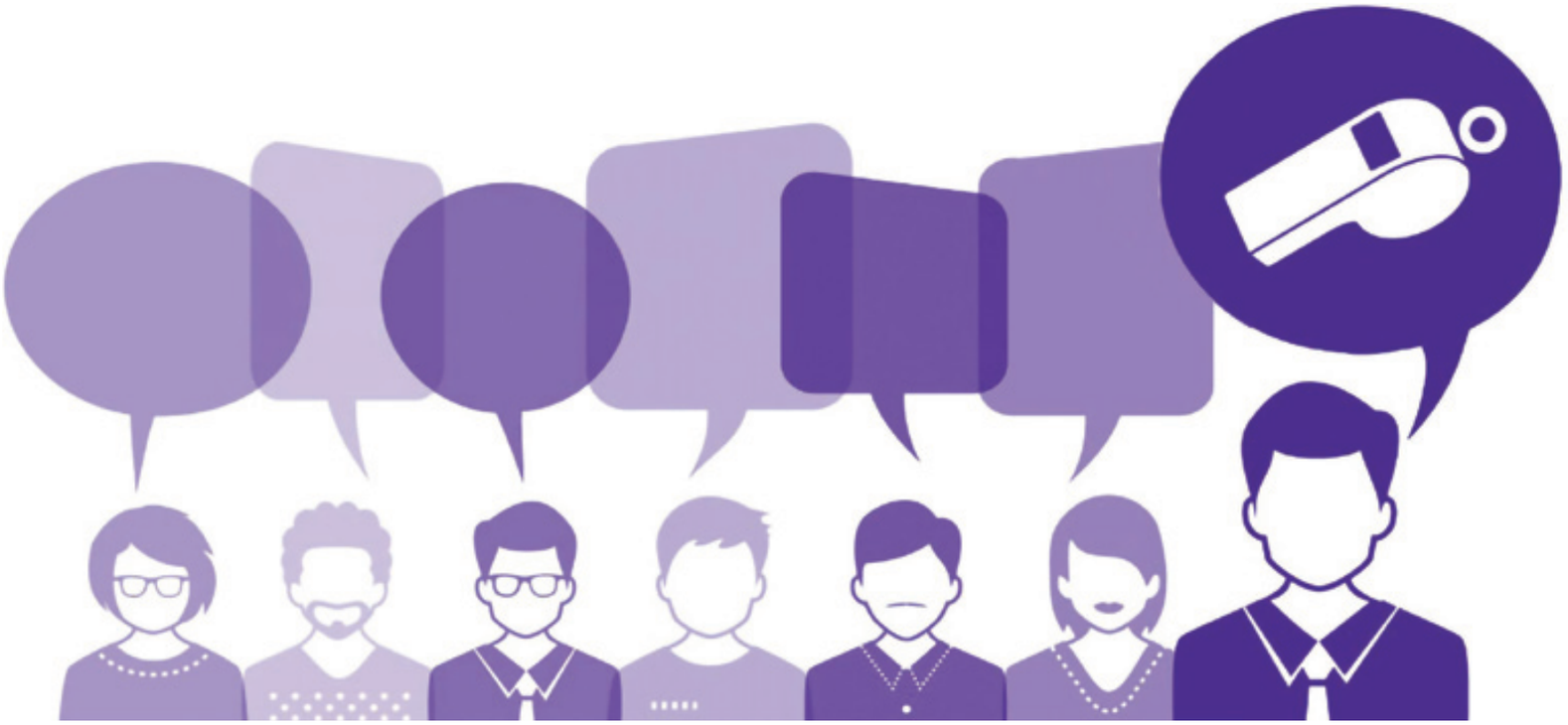
NORMATIVA

WHISTLEBLOWING LE NOVITÀ NELLA DIRETTIVA EUROPEA E L'IMPATTO SULLE AZIENDE

ARRIVA ANCHE IN ITALIA LA DIRETTIVA EUROPEA SUL WHISTLEBLOWING, OVVERO LA SEGNALAZIONE DI COMPORTAMENTI IRREGOLARI O ILLECITI ALL'INTERNO DI UN'ORGANIZZAZIONE PUBBLICA O PRIVATA. RECEPITA CON IL DECRETO LEGISLATIVO 24 DEL 10 MARZO 2023, LA NORMATIVA RAPPRESENTA UN IMPORTANTE CAMBIAMENTO RISPETTO ALLE LEGGI PRECEDENTI E HA UN IMPATTO RILEVANTE NEL SETTORE PUBBLICO COME IN QUELLO PRIVATO. PER ENTRARE NEL MERITO DELLA NUOVA NORMATIVA, D.A. ITALIA SI È RIVOLTA AD ALBERTO DI NOIA, ESPERTO DI CYBER SECURITY E AMMINISTRATORE DI NET PATROL ITALIA, AZIENDA LEADER NEL SETTORE CHE HA SVILUPPATO ACARA, UNA PIATTAFORMA DI SEMPLICE UTILIZZO PER LA SEGNALAZIONE E LA GESTIONE DI CONDOTTE ILLECITE, IN LINEA CON LE RICHIESTE DELLA DIRETTIVA.

LA NUOVA NORMATIVA SI APPLICA ALLE ORGANIZZAZIONI PUBBLICHE E PRIVATE CON OLTRE 50 DIPENDENTI O CON UN FATTURATO ANNUO SUPERIORE A 10 MILIONI DI EURO.

Con il termine "whistleblowing" si intende **la segnalazione di comportamenti irregolari o illeciti all'interno di un'organizzazione pubblica o privata**, operata da un soggetto segnalante.
I profili del soggetto segnalante (whistleblower) possono essere diversi: dipendenti, collaboratori esterni, azionisti, soci o volontari che abbiano rapporti con l'organizzazione. Il fenomeno del whistleblowing avrà sicuramente un impatto positivo all'interno delle aziende, in quanto permetterà la segnalazione di illeciti o irregolarità, con la conseguenza di gestire tali criticità e così prevenire danni alle aziende stesse ed ai loro stakeholders.
Tuttavia, il whistleblowing ha una duplice implicazione: da un lato la privacy del segnalante, dall'altro la confidenzialità delle informazioni aziendali. Per questo, prima la Direttiva europea e poi la normativa italiana di recepimento, hanno previsto specifici standard e obiettivi di protezione del segnalante e delle informazioni che transitano sui canali attivati per le segnalazioni. Infatti, se risulta fondamentale proteggere l'identità e la riservatezza del segnalante, è anche necessario evidenziare che nei canali di whistleblowing possono transitare informazioni aziendali molto sensibili come segreti industriali, informazioni contrattuali confidenziali e comunicazioni riservate.



La nuova normativa si applica alle organizzazioni pubbliche e private con oltre 50 dipendenti o con un fatturato annuo superiore a 10 milioni di euro.
Il principale nuovo adempimento per le aziende è quello di **dotarsi di canali di segnalazione sicuri**, tali da garantire, anche attraverso la crittografia, la riservatezza dell'identità della persona segnalante, delle persone coinvolte e menzionate nella segnalazione nonché del contenuto della segnalazione e della relativa documentazione.

Il consiglio è quindi di **evitare soluzioni "fatte in casa"**, come ad esempio l'uso della posta elettronica come canale di segnalazione, **da cui potrebbero derivare situazioni di insicurezza e rischi sanzionatori**, alla luce della normativa privacy e della nuova normativa sul whistleblowing. La nuova normativa prevede sanzioni da 10.000 a 50.000 euro quando l'azienda non istituisce canali di segnalazione, non adotta procedure per l'effettuazione e la gestione delle segnalazioni, oppure quando l'adozione delle procedure non è conforme alle misure di trasparenza e sicurezza previste. A questo devono aggiungersi le ben più salate sanzioni (fino a 10 o 20 milioni di euro, o 2%-4% del fatturato) previste in caso di violazione della normativa privacy o in caso di scorretta gestione del processo di segnalazione.

Come previsto dalla normativa italiana di recepimento, il canale di segnalazione dovrà essere affidato a una persona o a un ufficio interno dedicato e con personale specificatamente formato per sua la gestione. In alternativa, i soggetti del settore privato con un numero di dipendenti inferiore a 250 potranno condividere il canale di segnalazione interna e la relativa gestione.
A prescindere dalla condivisione o meno dei canali di segnalazione e della loro gestione, bisogna però porre attenzione ai ruoli dei soggetti coinvolti nel trattamento di dati personali e dei requisiti previsti dalla normativa privacy (Reg. UE 2016/679), anche in ambito contrattuale.

La nuova normativa rappresenta anche un'opportunità per le aziende, che potranno promuovere una maggiore trasparenza e responsabilità nella propria attività. I canali di segnalazione interni possono infatti consentire alle aziende di individuare e risolvere tempestivamente eventuali violazioni di legge o irregolarità, prevenendo così il rischio di sanzioni e danni all'immagine aziendale.
Secondo alcuni studi (Report to Nations, ACFE – Associations of Certified Fraud Examiners, 2020) le aziende con un sistema di segnalazione individuano gli illeciti con sei mesi di anticipo rispetto alle aziende che non hanno strumenti di questo tipo e riescono quindi a ridurre le possibili conseguenze negative (sanzioni, danni all'immagine, eccetera) di almeno il 50%. Inoltre, un sistema di whistleblowing sicuro e conforme alla normativa privacy incentiva i dipendenti a segnalare anche illeciti come accessi abusivi o danneggiamenti di dati e sistemi informatici, con la conseguenza per le aziende di poter mitigare rischi sanzionatori derivanti da violazioni di dati personali.

Le disposizioni del decreto avranno effetto quattro mesi dopo la data di pubblicazione (10 marzo 2023) e le disposizioni attuali cesseranno definitivamente entro il 17 dicembre 2023.

Fortunatamente, il mercato già offre soluzioni tecniche per dotarsi di canali di segnalazione sicuri e conformi alla nuova normativa e nel rispetto della normativa privacy. Uno di questi è **Acara, una piattaforma di whistleblowing sviluppata da Net Patrol Italia**. La piattaforma è stata sviluppata **nel rispetto della Direttiva europea sul whistleblowing e nel rispetto del GDPR**, raggiungendo una serie di obiettivi importanti ai fini dei nuovi standard europei: sicurezza dei dati e dei documenti trasmessi grazie alla crittografia, protezione totale della riservatezza dei segnalanti, trasparenza dei processi e delle azioni degli operatori grazie e piena libertà di configurazione di ogni aspetto, per adeguarlo alle necessità aziendali.