Incontro formativo sui temi Privacy e Cyber

Centro Congressi «La Fornace» - Via dell'Equitazione

Roma, 13 Novembre 2024

Domenico Vozza
Responsabile Security & Cyber Defence Acea S.p.A.

Roma, 13 Novembre 2024

Il Gruppo Acea

Acea è un **Gruppo industriale multiservizi** che opera nei settori dell'acqua, dell'energia e dell'ambiente, con un forte impegno verso la sostenibilità e l'innovazione. Acea è impegnata nella **transizione digitale**, adottando **soluzioni tecnologiche innovative** per rendere più efficienti e sostenibili i **processi operativi** delle aree di business

Primo operatore in Italia nei servizi idrici con **10 milioni di abitanti serviti** in Lazio, Toscana, Umbria, Campania e Molise (Sicilia di recente acquisizione)

Presente nel settore della **produzione di energia elettrica** con focus sulle rinnovabili con circa **750 GWh di energia prodotta**

Tra i principali operatori in Italia nella **distribuzione dell'energia** con circa 9 **TWh di energia distribuita**

Tra i principali operatori in Italia nel **Waste Management con** circa **1,8 milioni di tonnellate di rifiuti gestiti**

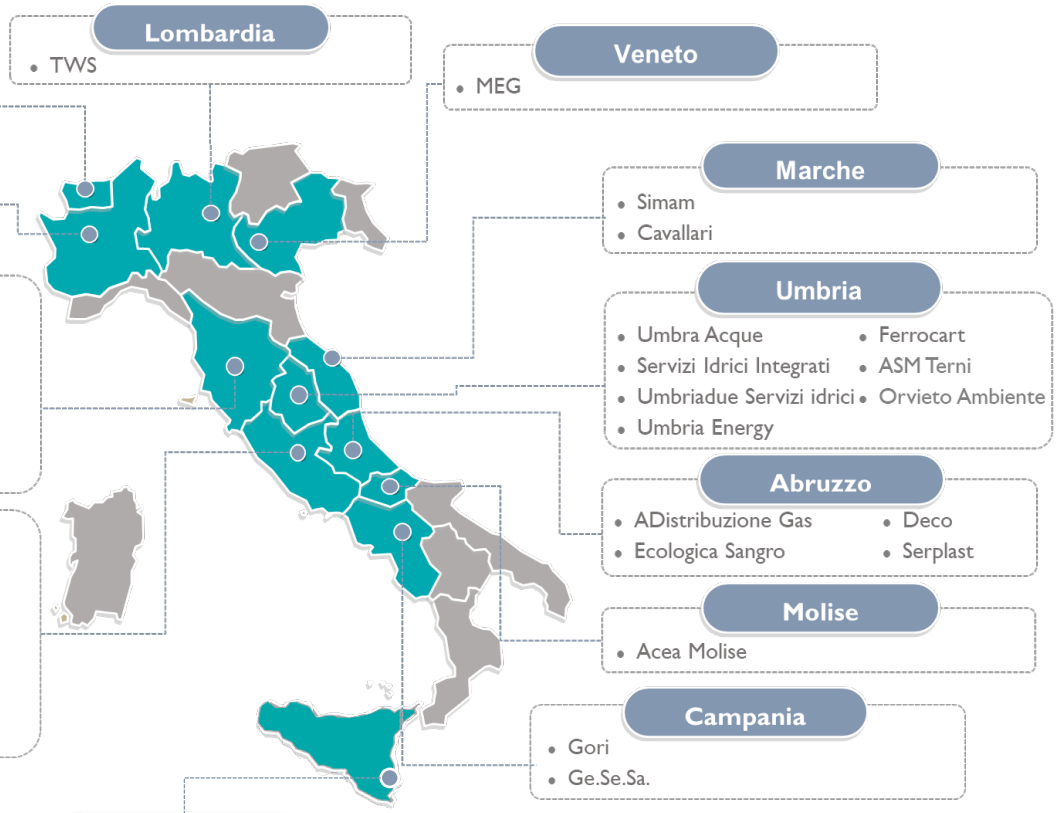
Tra i principali operatori nazionali nel **mercato dell'energia** con circa **7 TWh di elettricità venduta**

Presenti con 4 società operative operanti nei servizi idrici e circa **10 milioni di abitanti serviti in America Latina**

Presenti con 4 società dedicate ad attività di Ingegneria: **461.799 analisi sulle acque potabili 160.862 analisi sulle acque reflue**

Presenza Territoriale del Gruppo Acea

Presenza di Acea sul territorio nazionale



Valle d'Aosta
- ISECO

Piemonte
- Demap

Lombardia
- TWS

Veneto
- MEG

Marche
- Simam
- Cavallari

Toscana
- Acquedotto del Fiora
- Publiacqua
- Le Soluzioni Scarl
- Acque e Acque Servizi
- Ingegnerie Toscane
- GEAL
- Acque Industriali
- Acea Ambiente

Umbria
- Umbra Acque
- Servizi Idrici Integrati
- Umbriadue Servizi idrici
- Umbria Energy
- Ferrocart
- ASM Terni
- Orvieto Ambiente

Abruzzo
- ADistribuzione Gas
- Ecologica Sangro
- Deco
- Serplast

Lazio
- Acea
- Acea ATO2
- Acea ATO5
- Areti
- Acea Infrastructure
- Acea Ambiente
- Aquaser
- Berg
- Acea Energia
- Acea Innovation
- Acea Produzione
- Ecogena
- Tecnoservizi

Molise
- Acea Molise

Campania
- Gori
- Ge.Se.Sa.

Sicilia
- Aretusacque

Presenza di Acea all'estero

Repubblica Dominicana
- Acea Dominicana

Honduras
- Aguas de San Pedro

Peru
- Consorcio Agua Azul
- Acea Peru

Agenda della giornata (1/2)

Orario	Argomento	Relatori	Introduzione
9.30 – 10.15	Protezione dei dati, sicurezza aziendale e modello di governance privacy/cyber di Acea	• Domenico Vozza - *Responsabile Security & Cyber Defence Acea S.p.A.* • Stefano Scoccianti - *Responsabile Risk & Compliance Acea S.p.A.* • Gilda Salmè - *DPO Acea S.p.A.*	La trasformazione digitale ha portato le aziende a operare in un contesto sempre più interconnesso e orientato ai dati. La gestione dei dati, un tempo considerata un aspetto secondario, è diventata una componente strategica per il successo aziendale. Uno degli scopi di questo incontro sarà **esplorare le sfide e le opportunità legate alla protezione dei dati in un'era caratterizzata da una rapida evoluzione tecnologica** e da un panorama delle **minacce informatiche in costante mutamento**.
10.15 – 11.00	Aggiornamenti sull'A.I. Act	• Francesco Giorgianni - *DPO Gruppo FS, Prof a c. in Diritto della Privacy e in Trasformazione Digital e Intelligenza artificiale e Smart Cities presso PUL* • Mario Valentini - *Partner Studio Pirola Pennuto Zei, Assistente alla Cattedra di Macchine Intelligenti e Diritto presso LUISS Guido Carli*	L'AI Act è un regolamento europeo che mira a disciplinare l'uso dell'intelligenza artificiale, stabilendo regole chiare per lo sviluppo e l'utilizzo di sistemi di IA, al fine di garantire la sicurezza, l'etica e la tutela dei diritti fondamentali. L'obiettivo dell'AI Act, che approfondiremo in questo incontro, è quello di creare un **quadro normativo che consenta all'innovazione nell'ambito dell'intelligenza artificiale di procedere in modo sicuro e responsabile.**

Agenda della giornata (2/2)

Orario	Argomento	Relatori	Introduzione
11.00 – 11.30	La Direttiva NIS 2 e aggiornamenti in merito alla conservazione dei metadati	• Stefano Aterno - *Socio dello Studio Legale E-Lex* • Massimiliano Bondanini - *Direttore Affari Legali Unindustria*	La NIS 2 rappresenta un importante passo avanti nella regolamentazione della sicurezza informatica a livello europeo, imponendo nuovi obblighi alle organizzazioni. L'obiettivo dell'incontro è **approfondire gli aggiornamenti introdotti dalla normativa, recepita in Italia con il Dlgs 138/2024.**
11.45 – 13.15	The CISO Game	• Andrea Guarino - *Cyber & Information Security Acea S.p.A.*	La nuova direttiva NIS2 sottolinea l'importanza di coinvolgere attivamente il top management in campagne di sensibilizzazione. In questo contesto si inserisce l'attività del CISO Game che vedrà coinvolto il pubblico nella simulazione di uno **scenario di crisi connesso ad un attacco cyber**.

Francesco Giorgianni
DPO Gruppo FS, Prof a c. in Diritto della Privacy e in Trasformazione Digitale Intelligenza artificiale e Smart Cities presso PUL

Roma, 13 Novembre 2024

Introduzione all'AI Act

Il nuovo regolamento sull'Intelligenza Artificiale (AI Act) è il primo quadro normativo al mondo dedicato specificamente all'IA. Stabilisce regole per un uso sicuro, etico e trasparente dell'intelligenza artificiale nell'Unione Europea.

Obiettivi dell'AI Act

L'AI Act mira a proteggere i diritti fondamentali, garantire la sicurezza, promuovere l'innovazione responsabile e armonizzare gli standard di IA in tutta l'Unione Europea.

Classificazione del rischio

L'AI Act classifica i sistemi di IA in tre categorie di rischio: inaccettabile, alto e basso. Questa classificazione aiuta a determinare le regole applicabili e le misure di conformità.

Vantaggi dell'AI ACT

PROTEZIONE DEI DIRITTI FONDAMENTALI

ARMONIZZAZIONE DEL MERCATO UNICO

PROMOZIONE DI UN'INNOVAZIONE RESPONSABILE

AUMENTO DELLA FIDUCIA DEI CONSUMATORI

Sfide dell'AI ACT

ONERE DI CONFORMITÀ ELEVATO, SOPRATTUTTO PER LE PMI

RISCHIO DI SOVRA-REGOLAMENTAZIONE

DIFFICOLTÀ DI APPLICAZIONE PRATICA E COSTI ELEVATI

PROBLEMI DI INTEROPERABILITÀ CON NORMATIVE INTERNAZIONALI.

Confronto con il GDPR

L'AI Act e il GDPR condividono un approccio simile: entrambi mirano a proteggere i diritti fondamentali e prevedono requisiti di conformità stringenti. Tuttavia, il GDPR si concentra sulla protezione dei dati personali, mentre l'AI Act regolamenta l'intero ciclo di vita dei sistemi di IA.

Il Rapporto Draghi e l'AI Act

Il Rapporto Draghi ha sottolineato il ruolo centrale dell'Intelligenza Artificiale per il futuro economico dell'Europa, evidenziando:

- Il potenziale di trasformazione economica attraverso l'adozione dell'IA
- La necessità di un quadro normativo che bilanci innovazione e protezione dei diritti fondamentali
- L'importanza di armonizzare le normative per garantire la competitività globale dell'UE

Il Rapporto Draghi e l'AI Act

- **Eccessivo onere di compliance**: Il Rapporto Draghi ha sottolineato come il carico normativo combinato del GDPR e dell'AI Act possa risultare particolarmente pesante per le PMI, creando difficoltà operative e costi aggiuntivi per adeguarsi a entrambi i regolamenti.

- **Problemi di sovrapposizione normativa**: Il Rapporto critica la **sovrapposizione tra il GDPR e l'AI Act**, evidenziando che i requisiti di valutazione del rischio e di conformità possono risultare duplicati o ridondanti, aumentando la complessità e diminuendo l'efficienza delle misure di protezione dei dati e di impatto sui diritti fondamentali.

- **Rischio di frenare l'innovazione**: Secondo il Rapporto Draghi, l'eccessiva regolamentazione combinata del GDPR e dell'AI Act potrebbe ostacolare l'innovazione tecnologica, specialmente nei settori emergenti come l'IA applicata alla sanità e all'automazione industriale. Viene segnalato che l'Europa potrebbe rischiare di rimanere indietro rispetto ad altre giurisdizioni, come gli Stati Uniti e la Cina, che hanno quadri normativi più flessibili.

Quali altre opzioni erano sul tavolo?

Un'alternativa avrebbe potuto essere l'uso di **codici di condotta e autoregolamentazione**, lasciando all'industria la definizione di standard etici e di conformità.

Utilizzare **linee guida tecniche** e standard, come quelli del NIST, avrebbe potuto consentire una regolamentazione più flessibile e adattabile ai cambiamenti tecnologici.

Un'altra opzione sarebbe stata la **regolamentazione specifica per settore**, con norme dedicate a settori ad alto rischio come sanità, finanza e trasporti.

Le **sandbox regolamentari** avrebbero permesso di testare nuove tecnologie in un ambiente controllato, favorendo l'innovazione e raccogliendo feedback per migliorare le normative.

Un approccio basato su una **normativa più leggera**, accompagnata da incentivi, avrebbe potuto promuovere l'adozione volontaria di pratiche responsabili da parte delle aziende.

Rischi e vantaggi di un approccio alternativo

RISCHI APPROCCIO ALTERNATIVO

- Minore protezione dei diritti fondamentali
- Mancanza di uniformità nelle normative
- Difficoltà di applicazione e monitoraggio

VANTAGGI APPROCCIO ALTERNATIVO

- Promuovere l'innovazione e la competitività
- Ridurre il carico burocratico per le PMI
- Favorire una maggiore adattabilità ai cambiamenti tecnologici.

Conclusione e Riflessioni Finali

L'AI Act è una scelta ambiziosa per regolamentare l'IA in Europa, ma esistono **approcci alternativi che potrebbero offrire maggiore flessibilità** e incentivare l'innovazione. Tuttavia, è essenziale **trovare un equilibrio** tra protezione dei diritti e promozione dell'innovazione.

Stefano Scoccianti

Responsabile Risk & Compliance Acea S.p.A.

Roma, 13 Novembre 2024

Gilda Salmè
DPO Acea S.p.A.

Roma, 13 Novembre 2024

Mario Valentini
Partner Studio Pirola Pennuto Zei, Assistente alla Cattedra di Macchine Intelligenti e Diritto presso LUISS Guido Carli

Roma, 13 Novembre 2024

Introduzione

Panoramica sull'Intelligenza Artificiale e la Proprietà Intellettuale

L'avvento dell'Intelligenza Artificiale («IA») ha realizzato una rivoluzione tecnologica che attraversa ogni aspetto della società contemporanea, incluso il complesso ambito della proprietà intellettuale. Questa innovazione prorompente, capace di generare design, contenuti artistici e prodotti commerciali, solleva anche questioni fondamentali riguardo alla natura della creatività e alla tutela dei diritti d'autore nell'era digitale.

Introduzione

- **IA**: Sistemi che simulano l'intelligenza umana per eseguire compiti complessi, come il riconoscimento vocale, la traduzione automatica e la guida autonoma. L'IA può apprendere e migliorare dalle esperienze, rendendola una tecnologia potente e versatile.

- **Proprietà intellettuale**: Protegge le creazioni dell'ingegno umano, incentivando l'innovazione e garantendo che gli autori ricevano riconoscimento e compenso per il loro lavoro. La proprietà intellettuale include brevetti, diritti d'autore, marchi e segreti commerciali, essenziali per promuovere la creatività e lo sviluppo economico.

Sfide Giuridiche

Le sfide giuridiche dell'IA

Nel campo della proprietà intellettuale emergono **due questioni di fondamentale rilevanza** connesse al tema dell'IA:

- identificazione dei soggetti legittimati a detenere i diritti di una creazione generata da un sistema di IA,
- fattibilità di proteggere sistemi di IA tramite strumenti di proprietà intellettuale, in particolare tramite i brevetti.

Sfide Giuridiche

Complessità della titolarità dei diritti d'autore

Il paradigma tradizionale della proprietà intellettuale, incentrato sulla figura dell'inventore come persona fisica o giuridica, si trova oggi a confrontarsi con scenari inediti.

Quando un'opera viene generata da un sistema di IA, la questione della titolarità dei diritti diventa complessa.

Chi detiene i diritti su opere create da IA?

Il proprietario del sistema IA può reclamare la titolarità delle opere generate?

O tale diritto spetta al programmatore che ha sviluppato l'algoritmo?

Possiamo concepire il sistema di IA stesso come titolare dei diritti, privo di qualsiasi caratterizzazione umana?

Sfide Giuridiche

Complessità della titolarità dei diritti d'autore

La questione se un sistema di IA possa essere riconosciuto titolare di un diritto di proprietà industriale è ancora oggetto di dibattito.

- Attualmente solo le persone fisiche o giuridiche possono essere titolari di diritti di proprietà industriale.
- Inoltre, solo le persone con capacità legale possono essere inventrici di diritti di proprietà industriale (diritti morali).

Nel sistema legale tradizionale, i diritti di proprietà intellettuale sono assegnati agli autori dell'opera, che hanno investito tempo e sforzo nella creazione di opere creative, e nascono in contemporanea alla nascita dell'opera stessa.

Questi diritti forniscono agli autori il controllo sull'uso e la distribuzione delle loro opere e consentono loro di trarre profitto dal loro lavoro.

Complessità della titolarità dei diritti d'autore

Quando un'opera è generata da un algoritmo di IA senza l'intervento diretto di un essere umano.

Alcuni Paesi stanno cercando di affrontare la questione attraverso modifiche delle leggi esistenti.

Ad esempio, in alcuni casi, i diritti di proprietà intellettuale sono stati assegnati al proprietario dell'IA generativa o al programmatore che l'ha sviluppata.

Recentemente, l'Australia ha riconosciuto un brevetto a un sistema di IA come inventore, ma questo è un caso isolato e non rappresenta ancora una norma consolidata.

Il Regolamento europeo n. 1689/2024 sull'intelligenza artificiale ("AI Act") e la tutela della proprietà intellettuale

L'AI Act mira a garantire che l'IA sia sicura, trasparente, etica e rispettosa dei diritti fondamentali. Stabilisce regole per lo sviluppo, la commercializzazione e l'uso dell'IA in Europa.

L'obiettivo è creare un quadro normativo armonizzato che favorisca l'innovazione e la competitività, proteggendo al contempo i cittadini europei dai rischi associati all'IA.

Art. 53 dell'AI Act

L'approvazione dell'AI Act il 13 marzo 2024 rappresenta un tentativo significativo di affrontare queste sfide a livello normativo. Il capitolo V dell'AI Act, dedicato ai "*General Purpose AI Model*" («GPAI»), introduce **meccanismi di compliance con la normativa comunitaria in materia di diritto d'autore**.

L'art. 53 del AI Act fa riferimento all'articolo 4.3 della Direttiva (UE) 2019/1970, che consente ai titolari del diritto d'autore di manifestare il proprio dissenso (*opt-out*) per impedire l'estrazione di testo e dati dalle loro opere per finalità commerciali.

Questa disposizione mira a bilanciare gli interessi degli autori con le esigenze di sviluppo dell'IA.

Articolo 53 dell'AI Act

Il secondo comma dell'art. 53 dell'AI Act introduce una deroga per i fornitori di GPAI rispetto agli obblighi di documentazione, se i modelli sono rilasciati a condizioni aperte e libere, salvo presentino notevoli rischi sistematici.

Questa disposizione mira a promuovere l'innovazione, pur mantenendo un controllo sui rischi potenziali.

Caso dell'Industria Musicale

L'industria musicale offre un esempio delle sfide poste dall'IA alla proprietà intellettuale.

Il recente caso della Recording Industry Association of America («RIAA») contro i fornitori di servizi IA Suno e Udio illustra la complessità della questione.

L'accusa di violazione del diritto d'autore si basa infatti sull'utilizzo non autorizzato di brani musicali per addestrare sistemi IA capaci di generare registrazioni audio da input testuali.

Questo caso solleva questioni cruciali sulla natura del consenso e della compensazione nel contesto dell'IA.

Gli artisti e i professionisti del settore musicale si trovano in pratica di fronte a una tecnologia in grado di replicare le loro voci e stili senza autorizzazione preventiva o compenso. Ciò non solo minaccia il loro modello di business, ma mette in discussione i valori fondamentali della creatività artistica.

Caso Dabus (Device for the Autonomous Bootstrapping of Unified Sentience)

è diventato uno dei punti focali nel dibattito legale ed etico riguardante i diritti delle opere create da sistemi di IA.

L'intelligenza artificiale chiamata Dabus, aveva creato in modo autonomo due invenzioni, una riguardante un contenitore alimentare per migliorare la sicurezza del prodotto contenuto e l'altra riguardante un dispositivo lampeggiante per attirare l'attenzione in situazioni di emergenza.

Le invenzioni prodotte da Dabus sono state oggetto di domande di brevetto, depositate dall'imprenditore americano Steven Thaler presso numerosi uffici brevetti in tutto il mondo, con la particolarità che Dabus stesso è stato designato come inventore per entrambe le domande. Questa scelta ha sollevato questioni complesse riguardanti la legittimità dell'assegnazione dei diritti di proprietà intellettuale a un'entità non umana e senza personalità giuridica.

Caso Dabus

Molti degli uffici interessati hanno rigettato la domanda con la motivazione che, in base alla normativa vigente, l'inventore designato nella domanda stessa deve essere una persona fisica.

Ad esempio, per quanto riguarda la domanda di brevetto europea, la Legal Board of Appeal (Commissione giuridica di ricorso) dell'European Patent Office («EPO») ha annunciato, il 21 dicembre 2021, la decisione di respingere entrambe le domande di brevetto sopra citate, confermando che, ai sensi della Convenzione sul brevetto europeo («EPC»), un inventore designato in una domanda di brevetto deve essere un essere umano. In particolare, la Legal Board of Appeal ha ritenuto che la designazione presentata dal richiedente non fosse coerente con l'articolo 81 EPC.

Caso Dabus

Al contrario, l'ufficio brevetti sudafricano ha deciso di non procedere al rigetto della domanda di brevetto relativa al caso Dabus.

Si è ipotizzato che il rilascio sia avvenuto senza che la designazione del sistema di IA come inventore fosse rilevata dall'ufficio.

Un'altra, ed ultima, eccezione riguarda l'Australia, ove l'ufficio brevetti ha stabilito che un sistema di IA può essere designato come inventore.

In particolare, l'ufficio brevetti australiano aveva inizialmente rigettato la domanda di Thaler osservando che, nel caso in cui inventore e titolare del brevetto non coincidano, è necessario che il titolare della domanda di brevetto ottenga il trasferimento della proprietà dell'invenzione dall'inventore.

Ma Dabus, essendo una IA, non poteva detenere una proprietà e quindi non era in grado di trasferirla.

Caso Dabus

Thaler ha presentato ricorso contro la decisione dell'ufficio, come ha fatto anche in altri paesi in cui le sue domande sono state rigettate.

La sentenza della corte australiana del 30 luglio 2021 ha dato ragione al ricorrente, stabilendo che la legge brevetti australiana non impone che l'inventore detenga la proprietà dell'invenzione, bensì richiede che il titolare della domanda abbia ottenuto attraverso vie legali la proprietà dell'invenzione.

La sentenza stabilisce che Thaler è proprietario dell'invenzione poiché possiede non solo il codice di Dabus, ma anche i prodotti con esso generati; e conclude che un sistema di IA può quindi essere designato come inventore, sebbene non come titolare del brevetto.

Impatto dell'IA sulle Professioni Intellettuali

Trasformazione delle Professioni Intellettuali

Esempi nel settore legale

L'avvento dell'IA sta trasformando profondamente anche le professioni intellettuali, come quella legale.

La "prodottizzazione" delle prestazioni professionali, ovvero la creazione di prodotti scalabili basati su IA, offre nuove opportunità ma solleva anche preoccupazioni sulla natura intellettuale di queste professioni.

Anziché vedere l'IA come una minaccia, è possibile concepirla come uno strumento complementare che può arricchire e potenziare le capacità dei professionisti. L'integrazione dell'IA nelle pratiche professionali richiede un continuo aggiornamento e adattamento, sfidando i professionisti a innovare i loro metodi di lavoro e di relazione con i clienti.

Prospettive Future e Armonizzazione

L'AI Act rappresenta un primo passo significativo verso l'armonizzazione della disciplina dell'IA a livello europeo.

Tuttavia, spetterà ai singoli Stati membri implementare efficacemente queste disposizioni, e alle corti nazionali il compito di bilanciare gli interessi in gioco:

da un lato, la tutela della creatività umana, dall'altro, le esigenze di innovazione e competitività del mercato.

In Italia, il DDL Butti, approvato il 23 aprile 2024, cerca di affrontare queste sfide, in particolare per quanto riguarda la tutela del diritto d'autore delle opere generate con l'ausilio dell'IA.

La proposta di estendere la definizione di "opera d'ingegno" per includere le opere generate dall'IA, purché il contributo umano sia prevalente, rilevante e dimostrabile, rappresenta un tentativo di adattare il quadro normativo esistente alle nuove realtà tecnologiche.

Conclusioni e Riflessioni Finali

L'IA offre enormi opportunità per l'innovazione, ma pone anche sfide significative per la protezione dei diritti di proprietà intellettuale. È essenziale trovare un equilibrio tra promuovere l'innovazione e garantire che i creatori ricevano il giusto riconoscimento e protezione.

La collaborazione tra legislatori, esperti di tecnologia e professionisti del diritto sarà cruciale per affrontare queste sfide.

Stefano Aterno
Socio dello Studio Legale E-Lex

LA DIRETTIVA NIS 2

Roma, 13 Novembre 2024

Premesse (1/2)

- Il Digitale rappresenta una leva di sviluppo economico e sociale e, allo stesso tempo, un possibile veicolo moltiplicatore di minacce
- È chiaro, dunque, che la sovranità digitale dell'UE passi (anche) per la sicurezza informatica.
- Si è così delineato il quadro strategico dell'UE in materia di ciberdifesa, che individua nel "**ciberspazio**" il **quinto dominio operativo**, accanto a quello terrestre, marittimo, aereo e spaziale.
- Con queste premesse, è stata adottata **la Direttiva 1148 del 2018** (c.d. **Direttiva NIS 1**) che, nei piani del legislatore europeo, avrebbe dovuto evitare che alcune tipologie di servizi fossero messi a rischio a causa di problematiche connesse alla cibersicurezza.
- Tale obiettivo è stato solo parzialmente raggiunto, rendendosi così necessario un intervento in materia a distanza di pochissimi anni.

Premesse (2/2)

- la Direttiva NIS aveva come obiettivo quello di instaurare e mettere in funzione un mercato interno per la cyber security mediante il rafforzamento di specifiche misure che consentissero il ravvicinamento delle normative nazionali.

- Per far ciò, la Direttiva assegnava a determinati soggetti appartenenti a uno dei sette settori strategici individuati una serie di obblighi volti a limitare i rischi di incidenti informatici e a garantire un efficace ripristino in caso di breach.

- Il legislatore italiano ha recepito la direttiva nel 2018, con il **d.lgs. n. 64** e, un anno dopo, nel 2019, ha emanato il **D.L. n. 105**, istituendo il perimetro di sicurezza nazionale cibernetica, una norma complementare alla citata Direttiva e volta ad assicurare la corretta e continua erogazione di servizi essenziali da parte di soggetti pubblici e privati.

Direttiva NIS 1: cosa non ha funzionato

- La più importante problematicità riguardava proprio le normative di recepimento: poiché la Direttiva NIS non sanciva espressamente i criteri utili all'individuazione dei c.d. "servizi essenziali", il panorama definitorio rappresentato dagli atti di recepimento appariva piuttosto disomogeneo.

- Nella realtà, infatti, si sono evidenziate notevoli divergenze nell'attuazione degli obblighi da parte degli Stati membri, con variazioni rilevanti in termini di tipo di obbligo, livello di dettaglio e metodo di vigilanza.

- Inoltre, il riesame della Direttiva NIS ha evidenziato divergenze anche nelle modalità della sua stessa attuazione da parte degli Stati membri, ai quali è stata lasciata discrezionalità sulla delimitazione dell'ambito applicativo, oltre che sull'attuazione degli stessi obblighi in materia di sicurezza e segnalazione degli incidenti.

- Un'attuazione inadeguata da parte di uno Stato può portare a ripercussioni sul livello di cybersecurity di altri Stati membri (in considerazione dell'intensità degli scambi transfrontalieri)

La Direttiva NIS 2 n. 2555/2022

- Il **14 dicembre 2022** è stata definitivamente approvata la **Direttiva n. 2555/2022**, entrata in vigore il 17 gennaio 2023, che dovrà essere recepita entro il 18 ottobre 2024.
- La direttiva NIS 2 persegue i medesimi obiettivi a cui mirava la precedente normativa.
- Le **modifiche** riguardano i **soggetti interessati**, gli **obblighi**, le **sanzioni** e, più in generale, l'approccio che deve essere tenuto nell'adempimento di quanto richiesto dal testo normativo.
- Nelle intenzioni del legislatore europeo, dunque, la NIS 2 servirà proprio a eliminare le divergenze tra i vari ordinamenti, creando un quadro normativo più uniforme e coordinato.
- In attesa che la Direttiva NIS 2 venga recepita nelle legislazioni nazionali degli Stati membri dell'UE , questi stessi operatori di servizi essenziali e digitali rimangono comunque soggetti all'attuale regime della Direttiva NIS.

Ambito di applicazione: i soggetti interessati (1/4)

- La prima innovazione riguarda il novero di soggetti interessati dalla Direttiva che appare ampliato rispetto alla precedente normativa.

- La NIS 2 supera innanzitutto la categorizzazione dei soggetti interessati in "operatori di servizi essenziali" e "fornitori di servizi essenziali" introducendo alcuni criteri uniformi per una più semplice e coerente identificazione degli operatori pubblici e privati che verranno inclusi nelle due nuove categorie di **"soggetti essenziali"** e di "**soggetti importanti".**

- In particolare, oltre che agli operatori privati dei settori ritenuti "essenziali" dall'Unione europea, ovvero quelli dell'**energia**, dei **trasporti,** delle **banche**, delle **infrastrutture dei mercati finanziari**, dell'**acqua potabile**, della **sanità** e delle **infrastrutture digitali** (che comunque rimarranno soggetti alla Direttiva NIS fino alla sua abrogazione), la NIS 2 si applicherà anche ai **fornitori di servizi digitali** che operano nei seguenti settori, anch'essi ormai essenziali:

  - e-commerce;
  - motori di ricerca;
  - cloud computing;
  - gestione dei servizi ICT, della pubblica amministrazione e dello spaziogil

Ambito di applicazione: i soggetti interessati (2/4)

Inoltre, con la Direttiva NIS 2 il legislatore europeo ha elencato anche **"altri settori critici"** includendovi i seguenti:

- i servizi postali e di corriere;
- la gestione dei rifiuti;
- la fabbricazione, la produzione e la distribuzione di sostanze chimiche;
- la produzione, la trasformazione e la distribuzione di alimenti;
- la fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro;
- la fabbricazione di computer e prodotti di elettronica e ottica;
- la fabbricazione di apparecchiature elettriche;
- la fabbricazione di macchinari e apparecchiature n.c.a.;
- la fabbricazione di autoveicoli, rimorchi e semirimorchi;
- la fabbricazione di altri specifici mezzi di trasporto;
- i fornitori di servizi digitali;
- le organizzazioni di ricerca.

Ambito di applicazione: i soggetti interessati (3/4)

- Con l'intento di superare le incertezze e disomogeneità della precedente Direttiva NIS, viene adottato il **criterio della dimensione** del soggetto da ritenere come essenziale o importante.
- La NIS 2, infatti, si applicherà a tutti quei soggetti pubblici o privati compresi nelle tipologie "alta criticità" o "altri settori critici" che:

- prestano i loro servizi o svolgano le loro attività all'interno dell'Unione;
- sono considerati medie imprese ai sensi all'**articolo 2, paragrafo 1**, dell'allegato alla **raccomandazione 2003/361/CE** (meno di 250 persone; fatturato annuo non superiore ai 50 milioni di euro; bilancio annuo non superiore a 43 milioni di euro), o che superino i massimali per le medie imprese di cui al paragrafo 1 del medesimo articolo
- È bene sottolineare che, in ogni caso, come disposto dal Considerando n. 13, gli Stati Membri dovranno adoperarsi per garantire che i soggetti esclusi dall'ambito di applicazione della NIS 2 raggiungano un livello elevato di cibersicurezza.

Ambito di applicazione: i soggetti interessati (4/4)

- In ogni caso, il criterio della dimensione del soggetto da ritenere come essenziale o importante non sarà l'unico applicato in attuazione della NIS 2: la Direttiva, infatti, si applicherà anche ad altre tipologie di soggetti quali i fornitori di reti di comunicazione o di servizi di comunicazione elettronica accessibili al pubblico, quelli che forniscono servizi di registrazione dei nomi di dominio e anche alcuni enti della pubblica amministrazione
- Infine, rientreranno nel perimetro di applicazione della direttiva anche i soggetti definiti "critici" dalla **Direttiva (UE) 2022/2557**, meglio nota come **Direttiva CER**, pubblicata anch'essa insieme alla NIS 2.

- Spetterà comunque agli Stati membri definire, entro e non oltre il 17 aprile 2025, un elenco dei soggetti essenziali e importanti che saranno chiamati a fornire le necessarie informazioni.
- Tale elenco dovrà poi essere riesaminato e aggiornato almeno ogni due anni, proprio a garanzia di una più corretta uniformità nell'applicazione della Direttiva NIS 2.

Autorità e punti di contatto: ratio e organizzazione
Art. 8 Dir. 2555/2022

- Ogni Stato membro designa o istituisce una o più **autorità competenti responsabili della cibersicurezza e** dei compiti di vigilanza.

- Ogni Stato membro designa o istituisce un **punto di contatto unico**. Se uno Stato membro designa o istituisce soltanto un'autorità competente, quest'ultima è anche il punto di contatto unico per tale Stato membro.

- Ogni **punto di contatto unico** svolge una **funzione di collegamento** per garantire la **cooperazione transfrontaliera** delle autorità del relativo Stato membro con le autorità pertinenti degli altri Stati membri, e, ove opportuno, con la Commissione e l'ENISA, nonché per garantire la **cooperazione intersettoriale** con altre autorità competenti dello stesso Stato membro.

- Gli Stati membri garantiscono che le proprie autorità competenti e i propri punti di contatto unici siano dotati di risorse adeguate per svolgere in modo efficiente ed efficace i compiti loro assegnati e conseguire in questo modo gli obiettivi della direttiva.

I compiti dei Computer Security Incident Response Team (CSIRT) e il loro coordinamento (1/2)

- ❖ Ogni Stato membro designa o istituisce uno o più CSIRT.
- ❖ È possibile designare o istituire i CSIRT all'interno di un'autorità competente.
- ❖ I CSIRT possono cooperare con team nazionali di risposta agli incidenti di sicurezza informatica di paesi terzi o con organismi equivalenti di paesi terzi, in particolare al fine di fornire loro assistenza in materia di cibersicurezza.
- ❖ I CSIRT svolgono i compiti seguenti:

a) monitorano e analizzano le minacce informatiche, le vulnerabilità e gli incidenti a livello nazionale, e, su richiesta, forniscono assistenza ai soggetti essenziali e importanti interessati per quanto riguarda il monitoraggio in tempo reale o prossimo al reale dei loro sistemi informatici e di rete;

b) emettono preallarmi, allerte e bollettini e divulgano informazioni ai soggetti essenziali e importanti interessati, nonché alle autorità competenti e agli altri pertinenti portatori di interessi, in merito a minacce informatiche, vulnerabilità e incidenti, se possibile in tempo prossimo al reale;

c) forniscono una risposta agli incidenti e forniscono assistenza ai soggetti essenziali e importanti interessati, se del caso;

I compiti dei Computer Security Incident Response Team (CSIRT) e il loro coordinamento (2/2)

d) raccolgono e analizzano dati forensi e forniscono un'analisi dinamica dei rischi e degli incidenti, nonché una consapevolezza situazionale riguardo alla cibersicurezza;
e) effettuano, su richiesta di un soggetto essenziale o importante, una scansione proattiva dei sistemi informatici e di rete del soggetto interessato per rilevare le vulnerabilità con potenziale impatto significativo;
f) partecipano alla rete di CSIRT e forniscono assistenza reciproca secondo le loro capacità e competenze agli altri membri della rete di CSIRT su loro richiesta;
g) se del caso, agiscono in qualità di coordinatore ai fini del processo di divulgazione coordinata delle vulnerabilità;
h) contribuiscono allo sviluppo di strumenti sicuri per la condivisione delle informazioni.

Cooperazione nazionale e internazionale

❖ Al fine di contribuire allo sviluppo della fiducia e di promuovere una cooperazione operativa rapida ed efficace fra gli Stati membri, è istituita una **rete dei CSIRT nazionali**.

❖ La rete di CSIRT svolge moltemplici compiti, tra cui:

- scambiare informazioni per quanto riguarda le capacità dei CSIRT;
- agevolare la condivisione, il trasferimento e lo scambio di tecnologia e delle misure, delle politiche, degli strumenti, dei processi, delle migliori pratiche e dei quadri pertinenti fra i CSIRT;
- scambiare informazioni pertinenti per quanto riguarda gli incidenti, i quasi incidenti, le minacce informatiche, i rischi e le vulnerabilità;
- su richiesta di un membro della rete di CSIRT, discutere e, ove possibile, attuare una risposta coordinata a un incidente identificato nella giurisdizione di tale Stato membro;
- fornire assistenza agli Stati membri nel far fronte a incidenti transfrontalieri a norma della presente direttiva;
- cooperare e scambiare informazioni con i centri operativi di sicurezza regionali e a livello dell'UE al fine di migliorare la consapevolezza situazionale comune sugli incidenti e le minacce informatiche in tutta l'Unione;

Cooperazione internazionale

- Ove opportuno, l'Unione può concludere accordi internazionali, conformemente all'articolo 218 TFUE, con paesi terzi o organizzazioni internazionali, che consentano e organizzino la loro partecipazione ad attività particolari del gruppo di cooperazione, della rete di CSIRT e di **EU-CyCLONe**. Tali accordi sono conformi al diritto dell'Unione in materia di protezione dei dati.

- EU-CyCLONe costituisce la rete europea delle organizzazioni di collegamento per le crisi informatiche istituita al fine di sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi di cibersicurezza su vasta scala e di garantire il regolare scambio di informazioni pertinenti tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione.

Accountability nella NIS

- Il legislatore europeo, consapevole dell'impossibilità di emanare una normativa contente obblighi puntuali, aggiornati e condivisi da tutti i settori sopra riportati, ha deciso di introdurre il concetto di accountability anche in ambito di cybersecurity. L'approccio è quello di responsabilizzare i soggetti interessati, che dovranno essere in grado di **rendicontare** il loro operato.
- Così, ai sensi dell'**art. 21** della NIS 2, viene sancito che gli Stati membri provvedano affinché i soggetti essenziali e importanti adottino misure tecniche, operative ed organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi

- Nella valutazione di adeguatezza delle misure individuate, occorre tenere in debita considerazione:
  - l'esposizione del soggetto ai rischi;
  - la grandezza del soggetto;
  - la probabilità che si verifichino incidenti e la loro gravità;
  - l'impatto sociale ed economico dell'incidente.

Misure da adottare per la gestione del rischio

Misure di gestione del rischio vengono chiaramente elencate dall'**articolo 21**, **punto 2**, e che comprendono:

- politiche di analisi dei rischi e di sicurezza dei sistemi informatici;
- gestione degli incidenti;
- continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;
- sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;
- sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;
- strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cyber sicurezza;
- pratiche di igiene informatica di base e formazione in materia di cybersicurezza;
- politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;
- sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;
- uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso.

Obblighi di segnalazione

- Gli operatori di servizi essenziali o importanti sono gravati da obblighi di segnalazione. Dovranno infatti notificare al **CSIRT** (**Computer Security Incident Response Team**) o, se opportuno, alla autorità nazionale competente, senza indebito ritardo e non oltre 72 ore dalla venuta a conoscenza tutti quegli incidenti in grado di causare una grave perturbazione del servizio oppure se l'incidente può avere conseguenze (o ha già avuto conseguenze) su altre persone fisiche o giuridiche causando perdite considerevoli (**Art. 23**).
- Inoltre, stabilisce che – quando è appropriato – la notifica debba avvenire anche a beneficio dei destinatari del servizio impattato dal cyber attacco, anche indicando le misure che detti destinatari sono in grado di adottare per reagire all'attacco.
- Il termine di notifica è ulteriormente specificato dalla direttiva che fa riferimento a **24 ore** dalla conoscenza per l'invio di un **"early warning"** che deve essere seguito dalla notifica di una analisi dettagliata dell'incidente entro **72 ore** dalla conoscenza

Giurisdizione e territorialità

I soggetti che rientrano nell'ambito di applicazione della direttiva sono considerati sotto la giurisdizione dello Stato membro nel quale sono stabiliti, ad eccezione dei casi seguenti:

- **a)** i fornitori di reti pubbliche di comunicazione elettronica o i fornitori di servizi di comunicazione elettronica accessibili al pubblico, che sono considerati sotto la giurisdizione dello Stato membro nel quale forniscono i loro servizi;
- **b)** i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i soggetti che forniscono servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, di motori di ricerca online o di piattaforme di servizi di social network, che sono considerati sotto la giurisdizione dello Stato membro in cui hanno lo stabilimento principale;
- **c)** gli enti della pubblica amministrazione, che sono considerati sotto la giurisdizione dello Stato membro che li ha istituiti.

Vigilanza ed esecuzione

- Inoltre, vale la pena ricordare che la Direttiva NIS 2 prevede obblighi di vigilanza ed esecuzione in capo agli Stati membri e norme in materia di condivisione delle informazioni sulla cibersicurezza tra le varie Autorità europee.

- Gli Stati membri possono consentire alle proprie autorità competenti di conferire priorità ai compiti di vigilanza. Tale priorità si fonda su un **approccio basato sul rischio**.

- La Direttiva NIS2 prevede dei poteri minimi di indagine che le autorità locali devono avere per valutare l'adeguatezza delle misure adottate dalle società fornitrici di servizi essenziali ed importanti.

- Nel caso in cui una azienda non si conformi con gli obblighi di cui alla Direttiva NIS2, gli Stati Membri devono fare in modo che tali società adottino, senza ritardo, tutte le azioni correttive appropriate e proporzionali.

- Le autorità competenti operano in stretta cooperazione con le autorità di controllo ai sensi del regolamento (UE) 2016/679 nei casi di incidenti che comportano violazioni di dati personali, senza pregiudicare la competenza e i compiti delle autorità di controllo di cui a tale regolamento.

Le sanzioni

- La Direttiva NIS 2 pone particolare attenzione ai rischi della supply chain e alla compliance della catena di fornitura, soprattutto per quanto riguarda i fornitori più critici.

- Inoltre, concede maggiori poteri delle autorità competenti, in particolare per quanto riguarda il monitoraggio delle entità essenziali che saranno soggette a vigilanza ex ante, con la possibilità di sospendere l'attività aziendale dell'impresa, ed ex post e potranno essere sanzionate fino a 10 milioni di euro, o 2% del fatturato (**articolo 34, punto 4**). Sanzioni che invece possono arrivare fino a 7 milioni di euro, o 1,4% del fatturato per i soggetti "importanti" (**articolo 34, punto 5**).

Direttiva NIS 2 e armonizzazione tra Stati UE

- Importante osservare che la Direttiva NIS 2 interviene (**articolo 16**) anche per colmare le differenze di adozione dai Paesi membri in tema di reporting sugli incidenti e successive azioni di rafforzamento
- In questo senso, la nuova norma istituisce formalmente la rete europea di organizzazioni di collegamento per le crisi informatiche (**CyCLONe,** acronimo di **Cyber Crisis Liaison Organisation Network**) che supporterà la gestione coordinata degli incidenti di sicurezza informatica su larga scala

- Infine, è previsto anche un meccanismo volontario di apprendimento tra pari che consentirà di aumentare la fiducia reciproca e l'apprendimento dalle buone pratiche e dalle esperienze nell'Unione, così da consentire di raggiungere un elevato livello comune di cyber sicurezza.

- Questo anche grazie all'allineamento della Direttiva NIS 2 con altre normative settoriali specifiche come quella sulla resilienza operativa digitale per il settore finanziario (DORA) e la Direttiva sulla resilienza delle entità critiche (CER)

- In particolare, la CER (Direttiva (UE) 2022/2557 sull'identificazione e designazione delle infrastrutture critiche europee) va di pari passo con la direttiva NIS2 accordando il concetto di sicurezza fisica con quello della sicurezza logica o cyber.
- Infatti, mentre la Direttiva NIS2 si occupa specificamente della sicurezza cyber delle entità critiche e altamente critiche, la Direttiva CER si occupa della loro resilienza, mirando a rafforzarne il livello di preparazione di fronte a una serie di minacce, tra cui quelle di stampo terroristico, quelle interne o di sabotaggio, oltre ai rischi naturali e alle emergenze sanitarie

DATA BREACH: applicazione e tempistiche

	NIS 2	DORA
AMBITO DI APPLICAZIONE	**Soggetti essenziali ed importanti** individuati secondo criteri dimensionali, merceologici e di territorialità	Si applica ad **enti finanziari** ed ai loro fornitori TIC, operando come lex specialis ATTENZIONE: RTS ATTI DI DETTAGLIO
GESTIONE DEGLI INCIDENTI	**I CSIRT sono incaricati della gestione degli incidenti**	Gli enti finanziari dovranno essere in grado di **costruire, assicurare e riesaminare** la propria integrità e affidabilità operativa per garantire l'offerta dei servizi finanziari.
COMUNICAZIONE DI INCIDENTI	Obbligo di segnalare gli **incidenti significativi**: a) preallarme in 24 ore; b) notifica entro 72 ore; c) relazione entro un mese.	Notifica obbligatoria per gli **incidenti gravi** all'autorità competente mediante: a) una notifica iniziale; b) una relazione intermedia; c) una relazione finale.

DATA BREACH: definizione e metriche

GDPR	NIS 2	DORA
VIOLAZIONE DEI DATI PERSONALI: «la violazione di sicurezza che comporta accidentalmente o in modo illecito la **distruzione, la perdita, la modifica, la divulgazione** non autorizzata o **l'accesso** ai dati personali trasmessi, conservati o comunque trattati»	**INCIDENTE:** «un evento che compromette la **disponibilità, l'autenticità, l'integrità o la riservatezza** di dati conservati, trasmessi o elaborati o ei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi»	**INCIDENTE CONNESSO ALLE TIC:** «un singolo evento, o una serie di eventi collegati non programmati dall'entità finanziaria, che compromette la sicurezza dei sistemi informatici e di rete e ha un impatto avverso sulla **disponibilità, autenticità, integrità o riservatezza** dei dati o sui servizi forniti dall'entità finanziaria»
METRICA BASATA SUL RISCHIO EPR I DIRITTI E LE LIBERTA' DEGLI INTERESSATI: • **Improbabile** non ci sono obblighi di notifica; • **Probabile** ma non elevato - obbligo di notifica all'Autorità Garante per la Protezione dei Dati Personali; • **Elevato** obbligo di notifica all'Autorità Garante per la Protezione dei Dati Personali.	**INCIDENTE SIGNIFICATIVO:** «a) ha causato o è in grado di causare una **grave perturbazione operativa dei servizi o perdite finanziarie** per il soggetto interessato; b) si è ripercosso o è in grado di ripercuotersi su **altre persone fisiche o giuridiche** causando perdite materiali o immateriali considerevoli»	**GRAVE INCIDENTE TIC:** Un incidente connesso alle TIC che ha un impatto avversi sui sistemi informatici e di rete a supporto delle funzioni essenziali o importanti dell'entità finanziaria»
	INCIDENTE SU VASTA SCALA: «un incidente che causa un livello di perturbazione superiore alla capacità di uno Stato membro di rispondervi o che ha un impatto significativo su almeno due Stati membri»	**GRAVE INCIDENTE TIC CON IMPATTO SUGLI INTERESSI FINANZIARI DEI CLIENTI:** Deve essere comunicato «senza indebito ritardo e non appena ne vengono a conoscenza, informano i loro clienti in merito a tale incidente e alle misure che sono state adottate per attenuare gli effetti avversi dell'incidente»

Decreto Legislativo n. 138, che recepisce la Direttiva (UE) 2022/2555 (NIS 2)

Il 1° ottobre 2024 è stato pubblicato in Gazzetta Ufficiale il Decreto Legislativo n. 138, che recepisce la Direttiva UE 2022/2055 (c.d. Direttiva NIS 2), in vigore a partire dal 18 ottobre 2024. L'obiettivo della NIS 2 è quello di raggiungere un livello elevato di sicurezza informatica in tutta l'Unione europea. A tal fine, il decreto di recepimento stabilisce misure che sono dirette ad assicurare un livello di cybersicurezza nazionale adeguato a fronteggiare crisi e incidenti di sicurezza, in modo da migliorare il funzionamento del mercato interno e incrementare la resilienza dei soggetti essenziali e importanti (art. 3 del decreto).

Decreto Legislativo n. 138, che recepisce la Direttiva (UE) 2022/2555 (NIS 2)

- **L'articolo 1** chiarisce che il decreto stabilisce misure atte a garantire un livello elevato di sicurezza informatica, contribuendo all'incremento del livello comune di sicurezza all'interno dell'Unione Europea.
- **L'articolo 2** fornisce definizioni per comprendere il campo d'azione della NIS 2, come la **sicurezza dei sistemi informativi e di rete**, il concetto di **incidente** e quello di **quasi-incidente**.
- **L'articolo 7** disciplina l'identificazione e la registrazione dei soggetti essenziali e importanti, i quali devono registrarsi annualmente sulla piattaforma digitale messa a disposizione dall'Autorità NIS. Entro il 31 marzo di ogni anno, l'Autorità NIS aggiorna l'elenco dei soggetti essenziali e importanti.
- **L'articolo 23** stabilisce che gli **organi di amministrazione delle organizzazioni** ricoprono un ruolo fondamentale nella gestione della sicurezza informatica. Nel dettaglio, essi devono approvare e sovrintendere l'implementazione delle misure di gestione del rischio e garantire che i dipendenti siano adeguatamente formati.

Decreto Legislativo n. 138, che recepisce la Direttiva (UE) 2022/2555 (NIS 2)

- **L'articolo 24** introduce l'obbligo di adottare **misure tecniche e organizzative proporzionate** per la gestione dei **rischi informatici**, attraverso un **approccio multirischio** che tiene conto non solo delle minacce digitali, ma anche di rischi fisici come furti, incendi e inondazioni. Le misure includono politiche di sicurezza, gestione degli incidenti, continuità operativa e sicurezza della catena di approvvigionamento. Particolare attenzione è rivolta alla gestione delle vulnerabilità e all'uso di tecnologie di sicurezza avanzate come l'autenticazione a più fattori.
- **L'articolo 25** stabilisce tempistiche stringenti per la **notifica degli incidenti** e dei **quasi-incidenti**: entro **24 ore** per la notifica iniziale e **72 ore** per fornire dettagli aggiuntivi, inclusi gli indicatori di compromissione (IoC). La notifica finale deve essere inviata entro 60 giorni dall'incidente.
- **L'articolo 38** prevede **sanzioni amministrative** rigorose per i soggetti che non rispettano le misure previste. In particolare, l'Autorità NIS può sospendere temporaneamente i certificati o le autorizzazioni in caso di mancato adeguamento da parte di un'organizzazione. Inoltre, i membri degli organi direttivi possono essere dichiarati incapaci di svolgere funzioni dirigenziali fino a quando non saranno attuate le misure necessarie per sanare le violazioni.

Decreto Legislativo n. 138, che recepisce la Direttiva (UE) 2022/2555 (NIS 2)

La Direttiva prevede adempimenti complessi e onerosi per le aziende e le pubbliche amministrazioni interessate. Per questa ragione, le scadenze sono state fissate in modo tale da assicurare il tempo necessario ad implementare le misure pianificate.

Quadro temporale:

- Entro il **31 dicembre 2024**, aziende e pubbliche amministrazioni dovranno svolgere un assessment per comprendere se siano o meno soggette agli obblighi della Direttiva NIS 2, seguendo il dettato degli artt. 6 e 7, degli Allegati I, II, III e IV, nonché di ogni altro atto che verrà emanato;
- Ogni anno, **dal 1° gennaio al 28 febbraio 2025**, i soggetti che ritengano di rientrare nell'ambito di applicazione del decreto dovranno registrarsi sulla piattaforma digitale predisposta dall'ACN fornendo le informazioni richieste dalla normativa;

Decreto Legislativo n. 138, che recepisce la Direttiva (UE) 2022/2555 (NIS 2)

- **Entro il 17 gennaio 2025** i fornitori di servizi di sistema dei nomi di dominio; i gestori di registri dei nomi di dominio di primo livello; i fornitori di servizi di registrazione dei nomi di dominio; i fornitori di servizi di cloud computing; i fornitori di servizi di data center; i fornitori di reti di distribuzione dei contenuti; i fornitori di servizi gestiti; i fornitori di servizi di sicurezza gestiti; i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network dovranno obbligatoriamente registrarsi sulla piattaforma resa disponibile da ACN fornendo le informazioni richieste dalla normativa;

Decreto Legislativo n. 138/2024, che recepisce la Direttiva (UE) 2022/2555 (NIS 2)

- **Entro il 31 marzo 2025**, l'ACN redigerà l'elenco aggiornato dei soggetti essenziali e dei soggetti importanti sulla base delle registrazioni ricevute attraverso la piattaforma;
- **Tra il 1° aprile e il 15 aprile 2025**, l'ACN comunica ufficialmente, attraverso la piattaforma, ai soggetti registrati l'inserimento nell'elenco dei soggetti essenziali o importanti o l'eventuale loro esclusione;
- **Dal 15 aprile al 31 maggio 2025** i soggetti che avranno ricevuto la comunicazione dall'ACN attraverso la piattaforma dovranno fornire le informazioni richieste dalla normativa;

Decreto Legislativo n. 138, che recepisce la Direttiva (UE) 2022/2555 (NIS 2)

- **A partire dal 1° gennaio 2026**, aziende e pubbliche amministrazioni che avranno ricevuto la comunicazione di inclusione da parte dell'ACN dovranno adempiere all'obbligo di notifica degli incidenti;
- **Entro il 1° ottobre 2026**, aziende e pubbliche amministrazioni che avranno ricevuto la comunicazione di inclusione da parte dell'ACN dovranno adempiere:
  1. agli obblighi degli organi di amministrazione e direttivi;
  2. agli obblighi in materia di misure di sicurezza;
  3. all'obbligo di raccolta e mantenimento di una banca dei dati di registrazione dei nomi di dominio, laddove applicabile.

Massimiliano Bondanini

Direttore Affari Legali Unindustria

Roma, 13 Novembre 2024

UNINDUSTRIA
UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE
ROMA • FROSINONE • LATINA • RIETI • VITERBO

Aggiornamenti sulla questione metadati

Community DPO e Privacy Unindustria

13 novembre 2024

1. Linee guida per posta elettronica ed internet 2007 / 1

Provvedimento del 5 marzo 2007 [doc web 1387978]

il Garante emana, per la prima volta in maniera organica, le “Linee guida per posta elettronica e internet”

in sintesi affermano che

- “i datori di lavoro pubblici e privati non possono controllare la posta elettronica e la navigazione in Internet dei dipendenti, se non in casi eccezionali
- Spetta al datore di lavoro definire le modalità duso di tali strumenti ma tenendo conto dei diritti dei lavoratori e della disciplina in tema di relazioni sindacali
- i datori di lavoro devono informare i dipendenti in modo chiaro e dettagliato su come utilizzare Internet e la posta elettronica, evidenziando anche la possibilità di controlli
- Vietata tuttavia la lettura e la registrazione sistematica delle email e il monitoraggio costante delle pagine web visitate dai lavoratori, poiché ciò costituirebbe un controllo a distanza del tipo assolutamente proibito dallo Statuto dei lavoratori

1. Linee guida per posta elettronica ed internet 2007 / 2

- Indica diverse misure tecnologiche e organizzative per prevenire, in casi strettamente limitati, l'analisi della navigazione online e l'apertura di email contenenti dati rilevanti per l'azienda.
- suggerisce che le aziende adottino un disciplinare interno (regolamento o policy), redatto in collaborazione con le rappresentanze sindacali, in cui siano chiaramente espresse le regole per l'uso di Internet e della posta elettronica.
- Richiede al datore di lavoro di adottare ogni misura per prevenire un uso improprio di questi strumenti, riducendo così la necessità di controlli sui lavoratori. Per l'uso di Internet, è consigliato ad esempio: stabilire in anticipo i siti web utili o meno per l'attività lavorativa; utilizzare filtri per bloccare l'accesso a determinati siti (black list) o il download di file multimediali.

1. Linee guida per posta elettronica ed internet 2007 / 3

- Per quanto riguarda la posta elettronica, l'azienda dovrebbe:
- mettere a disposizione indirizzi condivisi tra più dipendenti rendendo evidente il carattere non privato di queste comunicazioni
- considerare di assegnare ai lavoratori un indirizzo secondario per l'uso personale
- in caso di assenza del dipendente, prevedere risposte automatiche con i contatti di altri colleghi di riferimento
- consentire al dipendente di delegare un fiduciario che possa verificare i messaggi ricevuti e inoltrare quelli rilevanti per l'ufficio, in caso di assenza imprevista o prolungata per motivi di lavoro urgenti

1. Linee guida per posta elettronica ed internet 2007 / 4

Qualora tali misure preventive non risultassero sufficienti per evitare comportamenti scorretti, eventuali controlli da parte del datore di lavoro dovrebbero essere graduali. Inizialmente, si procederebbe con verifiche a livello di reparto o gruppo di lavoro, per identificare l'area da richiamare alle regole. Solo in caso di recidiva, si potrebbe passare a controlli individuali.

Negli anni, gli interventi sanzionatori del Garante hanno sempre messo in luce la natura di "corrispondenza" della posta elettronica anche negli ambienti di lavoro e quindi la protezione costituzionale della loro riservatezza

2. Primo documento di indirizzo metadati 21 dic.2023/ 1

Il 21 dicembre 2023, il Garante approva il documento di indirizzo denominato

“Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati”

volto a fornire talune indicazioni ai datori di lavoro pubblici e privati e agli altri soggetti a vario titolo coinvolti, al fine di promuovere la consapevolezza delle scelte, anche organizzative, dei titolari del trattamento, nonché a prevenire iniziative e trattamenti di dati in contrasto con la disciplina in materia di protezione dei dati e le norme che tutelano la liberà e la dignità dei lavoratori.

- **Origine dell’intervento:**

Il Garante, anche a seguito di interventi ispettivi in materia (v. Ordinanza di ingiunzione nei confronti di Regione Lazio – 1° dicembre 2022 [doc web 9833530]), ha verificato che molti fornitori di sistemi di posta elettronica, particolarmente in cloud, rilevano e registrano i metadati dei messaggi di posta elettronica relativi all’utilizzo degli account di posta elettronica in uso ai dipendenti – ad es. giorno, ora, mittente, destinatario, oggetto e dimensione, conservandoli «per un esteso arco temporale».

2. Primo documento di indirizzo metadati 21 dic.2023/ 2

- in alcuni casi tali piattaforme in cloud pongono limitazioni al cliente - datore di lavoro - in ordine alla possibilità di modificare le impostazioni di base del programma informatico al fine di disabilitare la raccolta sistematica di tali dati o di ridurre il periodo di conservazione degli stessi.
- questa pratica di conservare i metadati per un periodo di tempo esteso e comunque superiore al limite massimo di sette giorni - estendibile di ulteriori 48 ore in casi particolari da dimostrare - secondo il Garante

a) comporta la possibilità di un indiretto controllo a distanza dell'attività dei lavoratori

b) → e pertanto richiede l'esperimento delle garanzie previste dall'art. 4, comma 1, della l. n. 300/1970

2. Primo documento di indirizzo metadati 21 dic.2023/ 3

richiede l'esperimento delle garanzie previste dall'art. 4, comma 1, della l. n. 300/1970

- ancorché sul presupposto della sua necessità per finalità di sicurezza informatica e tutela dell'integrità del patrimonio, anche informativo, del datore di lavoro

- a prescindere dalle responsabilità in materia di protezione dei dati quali i) liceità del trattamento, ii) principio della limitazione della conservazione, iii) principio di protezione dei dati fin dalla progettazione e per impostazione predefinita iv) e principio di responsabilizzazione

- art. 4 della legge n. 300/1970 è

- norma richiamata dall'art. 114 del Codice il cui rispetto costituisce condizione di liceità dei trattamenti di dati personali effettuati in ambito lavorativo
- assume rilevanza penale ex art. 171

2. Primo documento di indirizzo metadati 21 dic.2023 / 4

- la raccolta e la conservazione dei metadati possono considerarsi attività necessarie ad “assicurare il funzionamento delle infrastrutture del sistema della posta elettronica” e, quindi, lecite ex art. 4, comma 2, dello Statuto dei lavoratori, solo se realizzate per un arco temporale limitato

- diversamente, la raccolta e la conservazione dei metadati per un lasso di tempo maggiore dovrebbero considerarsi funzionali al perseguimento di altre finalità: es. sicurezza informatica e tutela dell’integrità del patrimonio, anche informativo, del datore di lavoro (ma non quella sopra)

2. Primo documento di indirizzo metadati 21 dic.2023 / 4

il Garante prescrive che i titolari:

- verifichino con la dovuta diligenza che i fornitori di posta elettronica non conservino per più di 7 giorni i metadati relativi ai messaggi di posta elettronica;
- qualora i sistemi non consentano di limitare tale periodo di conservazione, i titolari (datori di lavoro) dovranno, alternativamente:

- espletare le procedure previste dalla legge 300 in merito alle autorizzazioni necessarie a escludere la possibilità di controlli a distanza dei lavoratori;

- cessare l'utilizzo di tali programmi e servizi informatici.

- nelle more dell'eventuale espletamento delle procedure di garanzia, i predetti metadati non possono comunque essere utilizzati (cfr. art. 2-decies del Codice);

- in ogni caso, deve essere assicurata la necessaria trasparenza nei confronti dei lavoratori, fornendo agli stessi una specifica informativa sul trattamento dei dati personali prima di dare inizio al trattamento.

3. Risposta alla Consultazione 12 aprile 2024 / 1

- qualificazione dei metadati come “strumento di lavoro”, nel senso di cui alla previsione dell’art. 4, comma 2, dello Statuto dei lavoratori
- anche se si volesse accedere alla definizione - rectius esemplificazione- di metadato fornita nel Provvedimento, la sua riconducibilità alla fattispecie di cui all’art. 4, comma 1, Statuto, non appare in linea con la lettera e la struttura complessiva della norma e, in particolare, con la disciplina che la stessa prescrive per gli “strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa” e per l’utilizzo delle “informazioni raccolte” dagli stessi
- quelli che l’Autorità individua come metadati non possono essere classificati e autonomamente considerati come “strumenti” (termine impiegato nell’art. 4, comma, 1 Statuto)
- i dati esemplificativamente indicati nel provvedimento (giorno, ora, mittente, destinatario, oggetto e dimensione dell’e-mail) sono infatti parte costitutiva delle e-mail stesse, dati insiti e connaturati ad uno “strumento”, qual è quello della posta elettronica complessivamente considerata data in uso ai lavoratori indispensabile per rendere la prestazione lavorativa

3. Risposta alla Consultazione 12 aprile 2024 / 2

- → **necessità disciplina uniforme**. La raccolta e la conservazione dei metadati devono necessariamente essere disciplinate in modo uniforme rispetto a quanto previsto per lo strumento di provenienza (id est il sistema di posta elettronica) e, quindi, trovano, in ogni caso, il proprio presupposto di liceità nel comma 2
- → **durata della conservazione come discrimine della natura di parte dello strumento lavorativo o meno.** Ritenere che la posta elettronica costituisca uno strumento utilizzato dal lavoratore per rendere la prestazione lavorativa, ma che i metadati conservino tale connotazione solo nel momento del loro immediato utilizzo e, al più, per 7/9 giorni successivi, perdendola dopo questo limite temporale, è una conclusione priva di fondamento tecnico
- **momento della procedura del comma 1**: in base al comma 1, per quei sistemi che non si configurano come “strumenti di lavoro”, l’accordo o l’autorizzazione devono perfezionarsi prima dell’installazione
- **definizione precisa di metadato.** Manca

3. Risposta alla Consultazione 12 aprile 2024 / 4

- **definizione precisa di metadati mancante è in contrasto con**

- → i principi costituzionali di legalità e della riserva di legge

- → il divieto di interpretazione analogica *in malam partem* previsto ex art.. 14 Preleggi e dall'art. 1 C.P., e fondato, a livello costituzionale, sul principio di legalità di cui all'art. 25, comma 2, della Costituzione

3. Risposta alla Consultazione 12 aprile 2024 / 5

Soluzione di Confindustria

- rispetto del principio di limitazione della conservazione, ricorso a strumenti di valutazione preliminare (c.d. DPIA) e trasparenza nei confronti dei lavoratori:
- tali esigenze sono assicurate dall'art. 4, comma 3, Statuto, che subordina l'utilizzo delle informazioni raccolte ex multis dagli strumenti di lavoro, al rispetto della normativa privacy e alla preventiva adeguata informazione dei lavoratori: pertanto è nella attuazione di tale previsione – e non del comma 1 – che deve essere assicurata la tutela della riservatezza dei lavoratori nell'utilizzo della posta elettronica aziendale, anche in base aspecifiche indicazioni del Garante.
- In un'ottica di accountability - principio di responsabilizzazione- su cui si fonda l'intera struttura del GDPR e si poggia la compliance in materia di protezione dei dati personali - non deve essere stabilito un termine di conservazione dei metadati degli account dei servizi di posta elettronica dei lavoratori unico e indistintamente applicabile a tutte le organizzazioni.

3. Risposta alla Consultazione 12 aprile 2024 / 6

- In forza del principio di responsabilizzazione, spetta a ciascun datore di lavoro determinare, anche in ragione del contesto di riferimento e specifiche e legittime esigenze gestionali - tra cui, anche la necessità di ottemperare a specifici obblighi normativi e principi generali - un termine di conservazione dei metadati proporzionato e congruo, che sia giustificabile in ragione delle finalità per le quali i dati personali sono trattati c.d. principio di limitazione della conservazione ex art. 5, par. 1, lett. e) del GDPR).
- il principio di limitazione della conservazione richiede al titolare del trattamento non già di fissare una data di scadenza predeterminata alla conservazione dei dati in forma personale, quanto piuttosto di legare a una finalità la conservazione stessa:
- la conservazione dei dati è lecita fintantoché la finalità alla quale la stessa è strettamente connessa risulta attuale e spetta al titolare del trattamento fissare - oltre che dimostrare, laddove richiesto - i criteri e i termini temporali di conservazione dei dati
- La determinazione di un congruo termine per la conservazione dei metadati non può essere lasciata una decisione basata su standard fissi ma deve essere il risultato di un'analisi dettagliata del contesto operativo e dei rischi specifici associati al trattamento

4. Il secondo provvedimento del garante 6 giugno 2024, n. 364 / 1

nel nuovo Provvedimento, il Garante privacy rivede le indicazioni sulla conservazione dei metadati, chiarendone

- perimetro applicativo
- ratio
- natura

4. Il secondo provvedimento del garante 6 giugno 2024, n. 364 / 2

nuova definizione di Metadati e precisazione:

non riguarda:

- la gestione della posta elettronica data in uso ai lavoratori, quanto, piuttosto, la gestione dei cc.dd. “log di trasporto”, quelle informazioni raccolte automaticamente dai sistemi di posta elettronica e funzionali a garantire le operazioni di invio e recapito delle e-mail
- non vanno confusi con le informazioni contenute nei messaggi di posta elettronica nella loro “body-part” (corpo del messaggio) o anche in essi integrate - ancorché talvolta non immediatamente visibili agli utenti dei software “client” di posta elettronica (i cosiddetti MUA - Mail User Agent) - a formare il cosiddetto envelope, ovvero l’insieme delle intestazioni tecniche strutturate che documentano l’instradamento del messaggio, la sua provenienza e altri parametri tecnici.
- le informazioni contenute nell’envelope, ancorché corrispondenti a metadati registrati automaticamente nei log dei servizi di posta, sono inscindibili dal messaggio di cui fanno parte integrante e che rimane sotto l’esclusivo controllo dell’utente, sia esso il mittente o il destinatario dei messaggi

4. Il secondo provvedimento del garante 6 giugno 2024, n. 364 / 3

riguarda:

I metadati presenti nei log dei sistemi di posta elettronica, rilevati automaticamente dal provider di posta elettronica in quanto funzionali all'instradamento dei messaggi e alla sicurezza del sistema

In dettaglio possono contenere informazioni quali:

- informazioni sul mittente (indirizzo e-mail del mittente)
- informazioni sul destinatario (indirizzo e-mail del destinatario)
- data e ora di invio
- indirizzo IP
- informazioni sui server che hanno elaborato l'e-mail
- ID messaggio
- oggetto e-mail (il contenuto non è incluso)
- informazioni sul client di posta (ad esempio, Outlook, ecc.)

4. Il secondo provvedimento del garante 6 giugno 2024, n. 364 / 4

- i metadati oggetto del provvedimento - sia quelli di origine prettamente tecnica sia quelli, come il campo “Oggetto”, determinati dagli utenti - presentano la caratteristica di essere registrati automaticamente dai sistemi di posta elettronica, indipendentemente dalla percezione e dalla volontà dell’utilizzatore.

- i log di trasporto costituiscono una “copia” dei dati contenuti nei messaggi di posta elettronica (e dei log delle relative envelope), elaborata e conservata a prescindere dalla percezione e dalla volontà dell’utilizzatore e funzionale esclusivamente al corretto funzionamento e al regolare utilizzo del sistema di posta, comprese le essenziali garanzie di sicurezza informatica

4. Il secondo provvedimento del garante 6 giugno 2024, n. 364 / 3

- Provvedimento riguarda solo i log di trasporto che, restando al di fuori della disponibilità e del controllo del lavoratore, il Garante assoggetta a una conservazione limitata nel tempo

- mentre la conservazione delle e-mail contenute nella casella di posta elettronica - eventualmente in cloud – e dei metadati dell'envelope segue il principio dell'accountability, continuando a restare a disposizione del lavoratore e del datore di lavoro per il tempo di conservazione stabilito nelle policy e/o nei regolamenti interni sull'utilizzo della posta elettronica aziendale

- si farà riferimento alternativamente ai "metadati di posta elettronica" o "log di posta elettronica"

4. Il secondo provvedimento del garante 6 giugno 2024, n. 364 / 5

Ratio del Provvedimento:

sensibilizzare e “responsabilizzare” i datori di lavoro sui trattamenti aventi a oggetto i metadati e, in particolare, sui relativi tempi di conservazione da parte dei fornitori.

in quanto il Garante ritiene che non sia infrequente l’ipotesi che né i datori di lavoro, né conseguentemente i lavoratori siano a conoscenza del fatto che i sistemi di posta elettronica registrano automaticamente i log di trasporto, conservandoli per periodi più o meno lunghi.

il titolare del trattamento, anche quando utilizza prodotti o servizi realizzati da terzi (come, infatti, i sistemi di posta elettronica), deve verificarne la conformità alla normativa sulla protezione dei dati personali

→ l’Autorità ha ritenuto di fornire indicazioni per orientare i datori di lavoro

4. Il secondo provvedimento del garante 6 giugno 2024, n. 364 / 6

Natura del Provvedimento:

il Garante ha chiarito la

natura di indirizzo

sottolineando che da questo non discendono prescrizioni, nuovi obblighi o responsabilità a carico del datore di lavoro e che il nuovo termine di conservazione dei metadati - di 21 giorni - è da considerarsi indicato a titolo orientativo e, pertanto, in applicazione del principio di accountability, superabile - senza attivare le garanzie di cui all'art. 4, co. 1 dello Statuto - in presenza di comprovate esigenze tecniche e organizzative necessarie a garantire il corretto funzionamento del sistema

4. Il secondo provvedimento del garante 6 giugno 2024, n. 364 / 7

Il Garante conferma che

- i metadati di Posta Elettronica, in questa nuova precisazione, sono comunque capaci di permettere il controllo a distanza dei lavoratori e pertanto potrebbero doversi applicare le prescrizioni dell'art.4 Legge 300/70, comma 1

- la raccolta e la conservazione dei log di trasporto possono considerarsi attività necessarie ad assicurare il funzionamento delle infrastrutture del sistema della posta elettronica e, quindi, lecite ex art. 4, co. 2 dello Statuto, solo se realizzate per un «arco temporale limitato»

- che non siano ritenute applicabili le prescrizioni del 4, comma 1 (o le soluzioni alternative) dipende comunque dalla durata della conservazione: se uguale o superiore a 21 giorni

- lasso di tempo esteso→ conservazione dei log non più funzionale ad assicurare la prestazione

Provvedimenti in materia di Posta Elettronica / 15

4. Il secondo provvedimento del garante 6 giugno 2024, n. 364 / 8

l'Autorità

- indica un termine di conservazione dei log di trasporto più ampio, pari a 21 giorni
- precisa che si tratta di una indicazione fornita a titolo orientativo,
- precisa che il datore può stabilirne uno più ampio in applicazione del principio di accountability.

in linea con una richiesta di Confindustria, consente al datore di prevedere - restando sempre nell'ambito dell'art. 4, co. 2 Statuto - e quindi, nella finalità di assicurare il funzionamento dell'infrastruttura di posta elettronica, un termine di conservazione dei metadati più esteso a condizione che sussistano comprovate esigenze tecniche e organizzative

4. Il secondo provvedimento del garante 6 giugno 2024, n. 364 / 9

in presenza di documentate

- esigenze tecniche

come per garanzie essenziali di sicurezza informatica, anche funzionale alla compliance privacy del datore di lavoro e all'adozione delle adeguate misure di sicurezza, per ottemperare alla normativa sulla cybersicurezza che impone dei tempi di conservazione dei log prolungati

- esigenze organizzative necessarie a garantire il buon funzionamento del sistema di posta elettronica

come gestione centralizzata dei sistemi nei gruppi multinazionali

4. Il secondo provvedimento del garante 6 giugno 2024, n. 364 / 10

- E’ al datore di lavoro che spetta stabilire un termine di conservazione dei metadati che sia proporzionato rispetto alle finalità legittime perseguite secondo il principio di limitazione della conservazione, art. 5, par.1, lett e) GDPR

- E’ sul datore di lavoro, in qualità di titolare del trattamento, che ricade la “responsabilità generale” dei trattamenti dei log di trasporto, anche se conseguenti all’utilizzo di servizi forniti da terzi.

- lo stesso Provvedimento invita i fornitori dei servizi di posta elettronica a tenere conto del diritto alla protezione dei dati conformemente allo stato dell’arte e a contribuire a far sì che i datori di lavoro possano adempiere ai loro obblighi di protezione dei dati, contemperando le esigenze di commercializzazione su larga scala dei propri prodotti con la conformità degli stessi.

5. La Nota Confindustria 22 luglio 2024 / 1

- Confindustria ribadisce e chiarisce le modifiche intervenute nel Provvedimento rispetto alla prima versione in particolare con riferimento a:

- Definizione di metadati/log
- Natura dell'atto e indicazione orientativa
- Ratio: sensibilizzare e "responsabilizzare" i datori di lavoro sui trattamenti aventi a oggetto i metadati e, in particolare, sui relativi tempi di conservazione da parte dei fornitori
- Nuovo termine di conservazione «arco temporale limitato»
- Eccezione delle comprovate esigenze tecniche e organizzative nel rispetto dei principi del GDPR

5. La Nota Confindustria 22 luglio 2024 / 2

Confindustria

- conferma che con riferimento alla liceità del trattamento, il ricorso a sistemi e soluzioni di gestione e conservazione dei log delle comunicazioni elettroniche può considerarsi rientrante nell'eccezione di cui all'art. 4, co. 2 nei casi, alle condizioni e per le finalità indicate nel Provvedimento stesso
- Conferma che spetta al datore di lavoro, in qualità di titolare del trattamento, accertare che i programmi e i servizi informatici di gestione della posta elettronica in uso ai dipendenti consentano di gestire i metadati in conformità alla normativa sulla protezione dei dati personali e a quella di settore
- Suggerisce, specialmente nel caso in cui si utilizzino prodotti di mercato forniti in modalità cloud o as-a-service - di conformare il trattamento dei metadati agli indirizzi indicati dall'Autorità con 4 raccomandazioni
- Avverte che analoghe cautele vanno, altresì, implementate nel caso in cui la conservazione dei log di trasporto prescinda da esigenze di buon funzionamento e di sicurezza informatica di base e richieda l'attivazione delle garanzie previste dall'art. 4, co. 1

5. La Nota Confindustria 22 luglio 2024 / 3

Raccomandazione 1:

verificare

- i tempi di conservazione dei metadati di trasporto praticati dai propri fornitori - che andranno opportunatamente specificati nell'atto di nomina a responsabile del trattamento
- le motivazioni di carattere funzionale/tecnico dagli stessi fornite per giustificarne la conservazione per un certo periodo - anche al fine della valutazione di impatto sulla protezione dei dati personali DPIA –
- nonché l'eventuale possibilità di stabilire in autonomia tempistiche di retention differenti e di disattivare le funzioni incompatibili con le proprie finalità del trattamento.

5. La Nota Confindustria 22 luglio 2024 / 4

Raccomandazione 2:

fornire ai lavoratori una informativa chiara sul trattamento dei dati personali relativi alle comunicazioni elettroniche che li riguardano, ad esempio, aggiornando, anche ai fini dell'art. 4, co. 3 dello Statuto dei lavoratori, le informative e/o le policy e/o i regolamenti interni sull'utilizzo della posta elettronica aziendale.

E' essenziale che i lavoratori siano resi pienamente consapevoli delle complessive caratteristiche del trattamento e che agli stessi siano forniti elementi informativi adeguati, ad es:

i tempi di conservazione dei dati

le finalità

lo svolgimento di eventuali controlli

5. La Nota Confindustria 22 luglio 2024 / 5

Raccomandazione 3:

effettuare ovvero eventualmente aggiornare la DPIA, documentando altresì le esigenze tecniche e organizzative che giustificano, ex art. 4, co. 2 dello Statuto dei lavoratori, l'individuazione di un termine di conservazione dei log di trasporto superiore ai 21 giorni e aggiornando il registro delle attività di trattamento

5. La Nota Confindustria 22 luglio 2024 / 6

Raccomandazione 4:

adottare tutte le misure tecniche e organizzative per garantire il rispetto della normativa sulla protezione dei dati personali e di quella di settore, assicurando, tra l'altro:

i) il rispetto del principio di limitazione della finalità, facendo cioè in modo che i log siano trattati in modo compatibile con le finalità per cui sono stati raccolti (es. disattivando le funzioni incompatibili con le finalità di trattamento perseguite; chiedendo al fornitore del servizio di anonimizzare i metadati raccolti nei casi in cui non si intenda effettuare una conservazione più prolungata degli stessi; commisurando adeguatamente i tempi di conservazione dei dati)

ii) l'accessibilità selettiva da parte dei soli soggetti autorizzati e adeguatamente istruiti

iii) la tracciatura degli accessi effettuati

Esempio: Microsoft

- ritiene che il limite di 21 giorni indicato dal Garante abbia carattere orientativo, concordando con l'interpretazione di Confindustria che permette una conservazione prolungata per necessità tecniche o organizzative fondate su i) requisiti di legge, ii) sicurezza informatica e iii) integrità del sistema.
- sottolinea che ciascun cliente ha responsabilità nell'assicurare la conformità alle normative locali e raccomanda valutazione caso per caso, considerando le specifiche esigenze normative di settore e di localizzazione.
- fornisce una serie di giustificazioni a sostegno della adozione di una conservazione estesa (per il proprio trattamento dei log di sistema da parte di Microsoft in qualità di Titolare del trattamento)

Esempio: Microsoft

- Microsoft Exchange Online traccia i “metadati” tramite la funzionalità di “Message Trace,” che registra l’attività dei messaggi mentre attraversano i server, garantendo così la funzionalità e la sicurezza del servizio

- I log di tracciamento sono conservati per 90 giorni, supportano la risoluzione di problemi come ritardi nella consegna e consentono il monitoraggio delle operazioni per garantire continuità di servizio, conformità e sicurezza

Esempio: Microsoft

- Le principali motivazioni per la conservazione dei metadati di MEO

1) Manutenzione e Funzionamento del Servizio Email:

Diagnosi e Risoluzione degli Errori: In caso di ritardi o mancata consegna delle email, i log di Message Trace sono utilizzati per identificare cause di errore o malfunzionamenti.

2) Sicurezza IT:

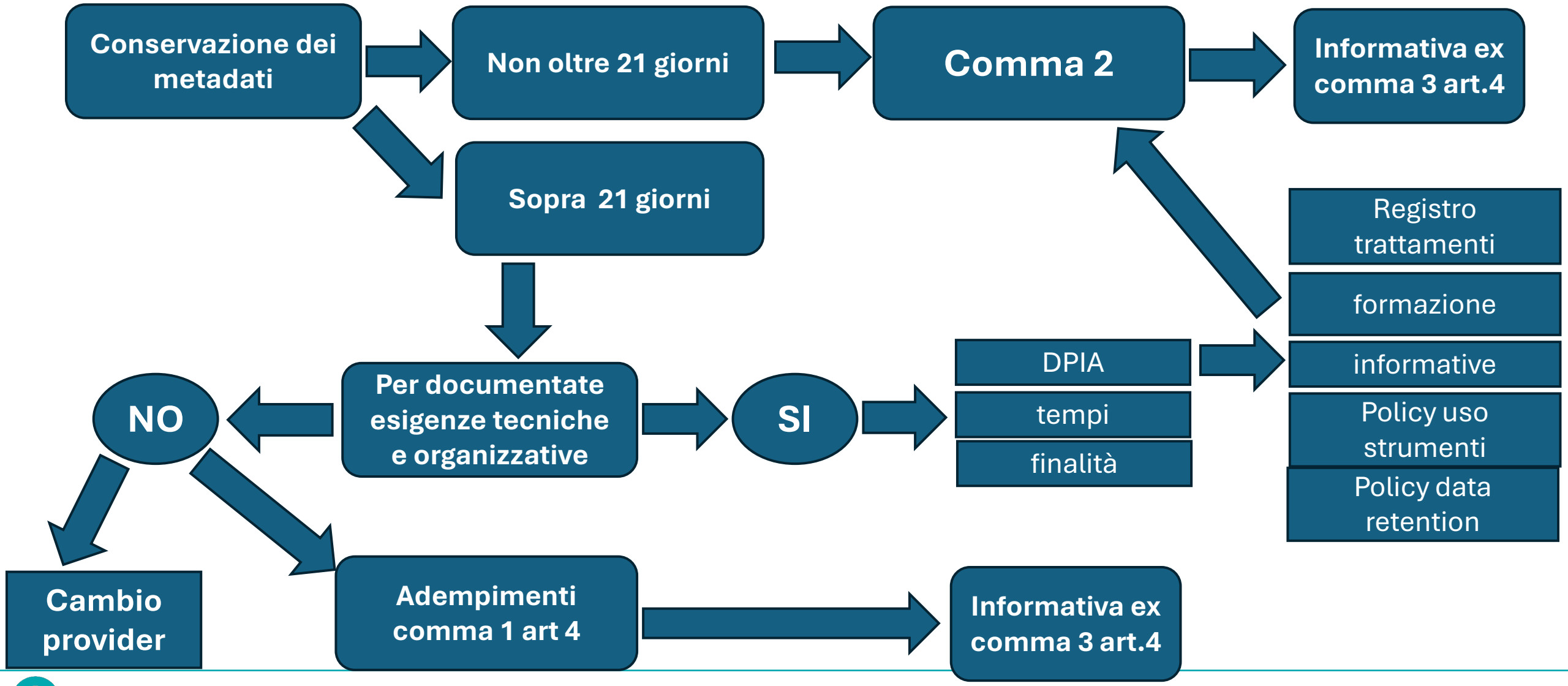
Individuazione degli Incidenti di Sicurezza:

Autenticità dei Messaggi e Verifica dell'Autenticità:

Supporto ai Team di Sicurezza: I team usano i metadati per identificare modelli di minacce e anomalie, essenziali per prevenire attacchi futuri.

3) Supporto alla Conformità e Monitoraggio dei Clienti: il monitoraggio della consegna delle email consente ai clienti di gestire indagini in ambiti come privacy, sicurezza e risoluzione di conflitti.

4. Il secondo provvedimento del garante 6 giugno 2024, n. 364 / 10



Andrea Guarino
Cyber & Information Security Acea S.p.A.

Roma, 13 Novembre 2024