INTELLIGENZA ARTIFICIALE E SICUREZZA DEI DATI NELLA PUBBLICA AMMINISTRAZIONE

ABSTRACT

Il rapido sviluppo delle tecnologie informatiche e telematiche ha posto la Pubblica Amministrazione innanzi alla necessità di adeguare le conoscenze e gli strumenti necessari per il trattamento digitalizzato dei dati personali che sia allo stesso tempo versatile e semplice da utilizzare ma anche sicuro e affidabile. I dati personali rappresentano, infatti, un patrimonio della persona fisica di eccezionale valore per le molteplici possibilità di sfruttamento economico che lo rendono altresì bersaglio di condotte criminose di vario tipo. In questo contesto, la gestione degli attacchi informatici sarà possibile solo attraverso l'automatizzazione dei processi, l'uso dell'intelligenza artificiale e la collaborazione tra tutti gli operatori del settore. Il Corso si propone l'obiettivo di soddisfare le nuove esigenze delle Pubbliche Amministrazioni nella gestione e nella protezione dei dati personali dei dipendenti e degli utenti in modo da aumentare i livelli di sicurezza informatica attraverso l'uso dell'intelligenza artificiale e gestire in maniera più consapevole i molteplici adempimenti richiesti in materia di trattamento dei dati personali. Una indagine in questo senso consentirà, dunque, non soltanto di conoscere l'apparato legislativo e regolamentare ma anche di cogliere, attraverso l'individuazione degli strumenti più idonei a garantire alti livelli di legalità e d'integrità dell'azione amministrativa, le peculiarità del sistema e prepararsi ad affrontare le prossime sfide nonché i pericoli e i rischi determinati dalla frenetica evoluzione delle tecnologie digitali e di apprestare rimedi idonei a disinnescare le minacce incombenti sulla sicurezza.

DATI RELATIVI ALLA PROPOSTA

1. Denominazione del soggetto proponente

Università di Foggia

2. Area tematica

Corso di II livello A – Intelligenza artificiale: Come funziona, perché interessa, come si può utilizzare. I sistemi di intelligenza artificiale per la cyber security.

3. Titolo del corso

Intelligenza artificiale e sicurezza dei dati nella Pubblica Amministrazione

4. Direttore/coordinatore didattico

Prof.ssa Donatella Curtotti

5. Faculty interna

Prof.ssa Valentina Vincenza Cuocci

Prof. Pasquale Annicchino

Dott.ssa Wanda Nocerino

5. Tutor

Dott. Christian Pallante

6. Durata del corso

50 ore on-line

7. Sede del corso

Università di Foggia

OBIETTIVI FORMATIVI

Il tema della sicurezza dei dati in Rete rappresenta la nuova sfida della Pubblica Amministrazione. Come noto, il Regolamento UE 2016/679 (recepito con D. Lgs. 101/2018) ha obbligato la P.A. ad un effettivo controllo sul trattamento dei dati in suo possesso, prevedendo anche l'introduzione di nuove figure professionali, fra cui il *Data Protection Officer* (DPO). Con il GDPR sono imposti nuovi adempimenti e metodologie, secondo i principi della *privacy by design* e della *privacy by default:* dalla valutazione dei rischi dei trattamenti dei dati alla valutazione di impatto, dal registro dei trattamenti al censimento delle banche dati con i dati personali. Il titolare del trattamento deve dimostrare di aver messo in atto – e di tenere aggiornate – le nuove misure tecniche e gestionali, monitorando i singoli adempimenti, documentando le scelte fatte e verificando la concreta applicazione delle nuove regole da parte dei diversi soggetti coinvolti all'interno e all'esterno dell'Amministrazione.

L'esigenza di garantire da parte della PA la tutela della *privacy* e la sicurezza dei dati dei dipendenti e degli utenti (specie quelli sanitari) richiede una specifica indagine anche a seguito del massiccio ricorso al lavoro agile determinato dalla pandemia da Covid-19, che ha realizzato una sorta di "delocalizzazione" della prestazione lavorativa. La circostanza che quest'ultima si svolge non più presso gli ambienti predisposti dal datore di lavoro ma in luogo scelto dal lavoratore richiede la predisposizione di nuove misure tese ad impedire o ad evitare che tale trasferimento possa incidere negativamente sulla sicurezza del trattamento dei dati.

In effetti, soprattutto nell'ultimo tempo, si registra un generale incremento delle aggressioni in Rete, che, quanto alla tipologia di bersagli, hanno riguardato per lo più sistemi IT di soggetti pubblici (si è passati da 567 attacchi al secondo a livello globale a più del doppio, con 1.287 al secondo).
La gestione di questo volume crescente di attacchi sarà possibile solo attraverso l'automatizzazione dei processi, l'uso dell'Intelligenza Artificiale (IA) e la collaborazione tra tutti gli operatori del settore della sicurezza informatica. In questo modo, ricorrendo alle tecniche di IA, si possono migliorare le strategie di cyber security per monitorare i comportamenti sospetti, anticipando gli eventi attraverso processi di apprendimento e analisi.
Di qui, la necessità di istituire un nuovo Corso di Alta Formazione, il cui obiettivo è quello di fornire ai partecipanti conoscenze dettagliate in materia di Intelligenza Artificiale e di *Cybersecurity*, per migliorare la capacità di analisi, prevenzione degli attacchi informatici e, al contempo, favorire la corretta gestione dei dati personali (dei dipendenti e dei fruitori dei servizi) sia sotto il profilo della sicurezza, sia sotto il profilo dello studio, dell'analisi, della profilazione e della monetizzazione delle informazioni.
Più nel dettaglio, il Corso, partendo dallo studio delle tecniche di Intelligenza Artificiale e dall'analisi della recente normativa nazionale ed europea, si propone l'obiettivo di formare il personale dipendente delle Pubbliche Amministrazioni, fornendo le conoscenze e le competenze necessarie per analizzare i processi di sicurezza informatica ed approfondire le problematiche relative alla prevenzione e al contenimento del crimine in Rete. Inoltre, nell'ambito della sicurezza informatica, verranno analizzati i rimedi per contenere le minacce ai sistemi informatici della PA e le tecniche di risposta agli eventuali attacchi *cyber*.
Al termine del Corso, il partecipante sarà in grado non soltanto di conoscere l'apparato legislativo e regolamentare vigente ma anche di svolgere una corretta diagnosi delle problematiche devianti e criminali presenti all'interno delle realtà urbane e di individuare ed utilizzare, tra le strategie di sicurezza esistenti, quelle maggiormente idonee ed efficaci. L'uso ragionato e consapevole delle conoscenze teoriche maturate consentirà al corsista di valutare la complessità delle dinamiche criminose e i problemi ad esse correlati riguardanti il concetto di rischio, il controllo sociale e la tutela della legalità.

INDICATORI DI OUTPUT:

Il percorso formativo offerto contribuirà:
- approfondire lo studio delle tecniche di IA (anche alla luce del recente AI Act) per aumentare i livelli di sicurezza informatica;
- a dotare i dipendenti della PA delle competenze necessarie per comprendere e valutare i rischi connessi al trattamento dei dati personali nella dimensione digitale, specialmente con riferimento ai dati sanitari;
- a dotare i dipendenti della PA delle competenze necessarie per allestire e gestire sistemi di trattamento digitale dei dati in sicurezza;

- a dotare i dipendenti della PA delle conoscenze necessarie per fronteggiare le minacce che nella dimensione digitale possono compromettere la sicurezza dei dati personali.

INDICATORI DI OUTCOME:

Al termine del percorso formativo i partecipanti avranno implementato le proprie competenze al fine di:
- valutare la sicurezza informatica dei sistemi a disposizione della PA al fine di identificare minacce e vulnerabilità;
- gestire i processi di innovazione organizzativa;
- predisporre e mettere in opera e di monitorare i programmi operativi;
- partecipare attivamente ai processi decisionali volti allo studio delle soluzioni più adeguate.

ATTIVITÀ FORMATIVE	ORE DI LEZIONE
MODULO 1 – INTRODUZIONE	
Lezione 1 – Dati personali e Pubblica Amministrazione	2
Lezione 2 – Dati sanitari e Pubblica Amministrazione	2
Lezione 3 – Sicurezza dei dati nella dimensione digitale	2
Lezione 4 – Intelligenza Artificiale e *cyber security*: cenni introduttivi	2
MODULO 2 – LA NORMATIVA DI RIFERIMENTO	
Lezione 5 – Il Regolamento UE 2016/679 e i riflessi sulla normativa nazionale	2
Lezione 6 – Il trattamento dei dati	3
Lezione 7 – Liceità del trattamento, *accountability* e adempimenti del titolare e del responsabile	3

Lezione 8 – I diritti degli interessati	3
Lezione 9 – Il ruolo del *Data Protection Officer* (DPO).	2
MODULO 3 - Sicurezza informatica e Intelligenza Artificiale	
Lezione 10 – L'AI Act	3
Lezione 11 – Intelligenza Artificiale e *machine learning* nella *cyber security*	3
Lezione 12 – I sistemi di intelligenza artificiale	3
Lezione 13 – Identificazione e previsione delle minacce digitali	4
Lezione 14 - Il *clustering* dei dati	3
MODULO 4 - LA TUTELA PENALE DEI DATI PERSONALI E I RIFLESSI NELLA DIMENSIONE DIGITALE	
Lezione 15 – Il trattamento illecito dei dati personali	3
Lezione 16 – La tutela dei sistemi informatici	4
Lezione 17 – La tutela del domicilio digitale	2
Lezione 18 – La tutela dell'identità digitale	2
Lezione 19 – Le investigazioni digitali	2
	Tot. 50

LORENZO LO MUZIO
18.09.2024 09:57:00 GMT+02:00