REPUBBLICA ITALIANA

Regione Siciliana
Assessorato dell'Economia

Intervento di saluto al Convegno "*TUTELA DEI DIRITTI E DELLE LIBERTA' FONDAMENTALI IN RETE: Il ruolo dell'Agcom e dei Corecom*"-Messina 15.6.2018

di Gaetano Armao

Vicepresidente ed Assessore regionale per l'economia della Regione siciliana
Docente di diritto regionale e contabilità pubblica nell'Università di Palermo

Un cordiale saluto alla Prof.ssa Maria Astone, Presidente del Corecom della Regione siciliana, alla quale vanno anche i complimenti per aver organizzato questo prestigioso Convegno qui a Messina, agli autorevoli relatori, a tutti i partecipanti.

Il tema del Convegno non é - come si diceva prima - solo di grande attualità e rilievo, ma interseca una delle più importanti politiche regionali affidata alla responsabilità dell'Assessorato del quale ho assunto la responsabilità: l'Agenda digitale siciliana.

La materia della protezione dei dati personali, come noto, appartiene alle competenze dell'Unione europea e dello Stato, e non involge, se non per profili organizzativi del sistema dei controlli e delle tutele, l'ordinamento siciliano, ma refluisce sull'attuazione dell'Agenda digitale regionale e ne deve informare profondamente gli interventi.

Un'Agenda rilevante sia in termini finanziari, ammontano ad oltre 410 milioni di euro le risorse disponili di fonte europea, statale e regionale, che strutturale incidendo sull'intero territorio regionale (banda larga ed ultra larga), su amministrazioni ed enti della Regione.

La strategia digitale costituisce una grande opportunità per la proiezione strategica della Sicilia, delle sue imprese, delle sue pubbliche amministrazioni, dei suoi cittadini per una crescita crescita inclusiva, intelligente e sostenibile. L'obiettivo dell'Agenda Digitale è quello di utilizzare in termini ottimali il potenziale delle tecnologie dell'informazione e della comunicazione per favorire l'innovazione, la crescita economica e la competitività.

Della strategia digitale della Regione siciliana è asse portante la cittadinanza digitale con l'obiettivo di garantire ai cittadini e alle imprese, anche attraverso l'utilizzo delle tecnologie dell'informazione e della comunicazione, il diritto di accedere a tutti i dati, i documenti e i servizi di loro interesse in modalità digitale, nonché di garantire la semplificazione nell'accesso ai servizi alla persona,riducendo la necessita' dell'accesso fisico agli uffici pubblici, favorendo l'amministrazione aperta ed il riuso dei dati.

Ogni siciliano, ogni impresa che ha sede o opera nella Regione, per essere inclusi ed attivi, dovranno poter conseguire competenze digitali ed utilizzare al meglio infrastrutture materiali ed immateriali realizzare in attuazione di questa Agenda. In questa prospettiva l'innovazione digitale diviene investimento pubblico che costituisce essenziale riforma strutturale della Regione.

Il mercato digitale diviene così strumentale alla costruzione della società digitale mentre la realizza e questa si sviluppa nell'alveo del mercato digitale divenendo lo strumento essenziale per assicurare uno sviluppo sostenibile, coniugando investimento sulla conoscenza ed inclusione sociale. Vi é, infatti, una nuova frontiera dei diritti sociali nella Knowledge Based Society che diviene opportunità di crescita delle società a sviluppo ritardato e caratterizzate da marginalità territoriale ed economica anche a causa della condizione insulare, come la Sicilia.

Il divario economico-sociale di cui soffre la Sicilia trova un tangibile riscontro anche nel "digital divide" che connota le infrastrutture telematiche e di comunicazione; tra gli obiettivi dell'Agenda vi é il sostegno all'alfabetizzazione digitale e la diffusione dell'accesso veloce ed

economico ai collegamenti telematici e l'interoperabilità, garantendo il diritto fondamentale all'inclusione digitale dei siciliani.

Non si tratta quindi di raccogliere una serie di interventi ed investimenti nel settore ITC, correlati dalla sola ricomprensione nel paradigma del l'agenda digitale, quanto piuttosto di delineare un sistema integrato di misure che, utilizzando sinergicamente le risorse finanziarie e strumentali disponibili oltre che le potenzialità derivanti dalla interconnessione legata alla peculiare posizione geografica (da qui la scelta anche della figura di copertina), costituisca una modalità di innovazione e di perseguimento della strategia digitale della Regione, nel solco degli strumenti programmatori europei e nazionali in materia.

La geografia e la storia hanno fatto della Sicilia una regione unica del Mediterraneo. La particolare dislocazione delle interconnessioni mondiali (dorsali internet-backbones landing points) rinnova e trasforma in opportunità questa centralità.

Sarà compito dei siciliani utilizzare al meglio le opportunità che si prospettano razionalizzando e rendendo efficiente l'investimento delle risorse disponibili, ma sopratutto riuscendo a cogliere la sfida di una nuova frontiera di sviluppo e di crescita.

In questo contesto, tra le scelte strategiche dell'Agenda, si iscrive l'evoluzione degli scenari di rischio dell'Information and Communication Technology(ICT), le nuove minacce provenienti dal cyber-spazio ed i sempre più numerosi attacchi, che vedono tra i target principali gli enti pubblici, responsabili della gestione di dati critici per la collettività (fiscali, sanitari, anagrafici etc.),è il quadro per cui la Regione ha scelto di adottare le più avanzate soluzioni progettuali nell'ambito della Sicurezza ICT dei Sistemi Informativi a supporto delle attività istituzionali, amministrative e di governo regionale, ma soprattutto nel perseguire l'obiettivo di evolvere il Data Center regionale - che sarà realizzato nel centro direzionale ex ASI di Palermo appena acquisito e per il quale sono già disponibili le risorse finanziarie a valere sul PON legalità e sicurezza appena stipulato con il Ministero dell'Interno - in un Polo strategico a livello Nazionale.

A questo scopo l'approccio classico basato su procedure gestionali complete e consolidate va coniugato, a livello strategico ed operativo, con l'attenzione ai nuovi contesti tecnologici e di processo a supporto della protezione dei dati, in accordo con quanto previsto dal governo e dalla normativa nazionale e comunitaria riguardo la protezione cibernetica e la sicurezza informatica.

Dal punto di vista operativo, per supportare il Management nelle attività di realizzazione progettuale, coordinamento, indirizzo e monitoraggio continuo della sicurezza informatica, la Regione ha definito i seguenti obiettivi, da realizzare in un'ottica di gestione dei rischi di cyber security, protezione dei dati e di resilienza delle infrastrutture tecnologiche a supporto dei servizi erogati con una specifica focalizzazione sulla sicurezza dei sistemi critici (ad es. quelli a supporto dei servizi con dati sanitari):

- Definizione e focalizzazione del perimetro di intervento operativo e dei piani di realizzazione progettuali della Sicurezza ICT della Regione in ottica Cyber Security;
- Sistema di conservazione dati sensibili (archiviazione dati sensibili)
- servizi di sicurezza applicativa per la prevenzione e gestione degli incidenti informatici e nell'analisi delle vulnerabilità dei sistemi informativi (vulnerability assessment e penetration testing);

- Sistemi di riconoscimento identità digitale (accesso in sicurezza tramite SPID, registrazione ai CUP)

- Creazione a livello regionale di un Centro Territoriale di Competenza sulla CyberSecurity con la realizzazione di un SOC - Security Operation Center - e di un CERT – Computer Emergency Response Team / CSIRT – Computer Security Incident Response Team – in grado di operare nel contesto dell'architettura delineata a livello nazionale per la cybersecurity (DPCM del 17 febbraio 2017 recante "indirizzi per la protezione cibernetica e la sicurezza informatica nazionale"), adottando i modelli operativi più evoluti in termini di Cyber Intelligence, al fine di massimizzare la capacità preventiva e reattiva per la gestione efficace degli incidenti, attacchi e minacce cyber alle infrastrutture della Regione;

- Attivazione degli interventi progettuali per la piena conformità alle normative - di cui meglio tratterete nel corso del Convegno - con particolare riferimento a: regolamento nazionale sulla privacy e comunitario GDPR (D.lgs. 196/03 e regolamento UE 2016/679 del 27/4/2016), direttiva europea NIS sulla cybersecurity (direttiva UE 2016/1148 del 6/7/2016), Codice dell'Amministrazione Digitale (D.lgs. 82/2005) e alle misure minime di sicurezza ICT per la Pubblica Amministrazione del 2017 (Dir. PCM 1/8/2015);

- Implementazione di un modello di Governance e Risk Management della IT Security adeguato al nuovo scenario delle minacce, che riguardi anche il coinvolgimento dei decisori nei criteri di accettazione del rischio e nella integrazione del IT Risk management nel processo di Risk Management complessivo dell'Amministrazione Regionale;

- Attivazione di programmi per l'implementazione delle misure e delle soluzioni tecnologiche di sicurezza allo stato dell'arte più adeguate in relazione all'estensione della superficie di attacco (postazioni di lavoro, sistemi accessibili e potenzialmente vulnerabili) e tecniche di attacco, con un approfondimento verticale sul fenomeno Ransomware e recenti attacchi correlati;

- Elaborazione di un programma per la Formazione / Awareness a tutti i livelli dell'Organizzazione regionale e personalizzato per le diverse tipologie di utenti (funzionari / amministrativi / tecnici / manager amministrativi e di governo / personale ICT / personale Direzioni e Assessorati).

Queste alcune delle iniziative avviate in un contesto che impone velocità, efficienza, sicurezza, ma anche garanzie e tutele per i cittadini, ma questo é compito del Convegno di oggi metterle meglio a fuoco e del Vostro lavoro del quale raccogliendo le relazioni, Ve lo assicuro, faremo tesoro.

Grazie dell'attenzione e buon lavoro.