BIT

BOLLETTINO
DELL'INNOVAZIONE
TECNOLOGICA
Anno 25 - 05 / 2019

Il tema del nostro tempo

COME AFFRONTARE LA SFIDA DIGITALE

SVILUPPUMBRIA
INNETWORK
Regione Umbria

BIT

B.I.T.
Bollettino dell'Innovazione Tecnologica
Periodico bimestrale
di informazione aziendale
Anno 25 numero 05 - 2019

Edito da:
Sviluppumbria S.p.a.
Sede legale:
Via Don Bosco 11 - Perugia
Tel.: 075.56811 - Fax: 075.5722454

Registrazione n. 7/96 del 16/03/1996
del Tribunale di Perugia

Direttore Editoriale
MAURO AGOSTINI

Direttore responsabile
TIBERIO GRAZIANI

Progetto grafico
LABBIT Srl

A questo numero
hanno collaborato:
Elisabetta Boncio
Annarita Martelli
Susanna Paoni
Valeria Tudisco

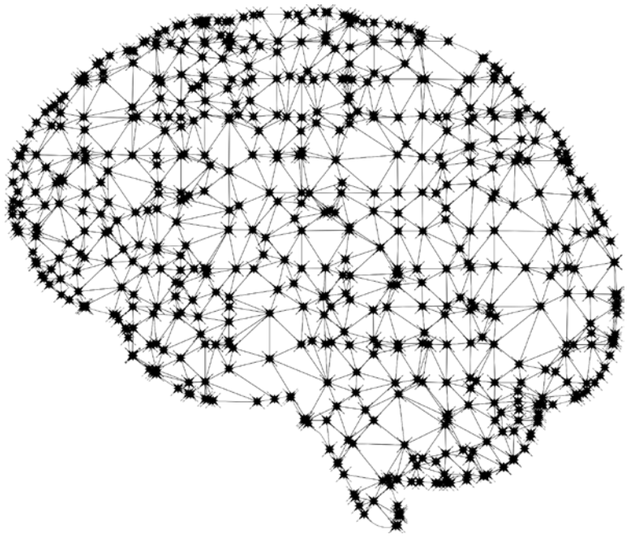
#05
2019

www.sviluppumbria.it

INTELLIGENZA ARTIFICIALE: LA DISPUTA TRA CINA, UE E STATI UNITI

Un rapporto pubblicato lo scorso agosto dal **Center for Data Innovation** intitolato "Who Is Winning the AI Race: China, the EU or the United States? "mette a confronto Cina, Unione Europea e Stati Uniti in termini di posizione relativa nell'economia dell'intelligenza artificiale analizzando sei diverse categorie: talento, ricerca, sviluppo, adozione, dati e hardware.

Gli Stati Uniti risultano guidare la classifica di quattro delle sei categorie esaminate dal rapporto, vale a dire talento, ricerca, sviluppo e hardware; La Cina guida le categorie adozione e accesso ai dati, mentre l'Unione europea non primeggia in nessuna categoria.



Tra le molte ragioni che possono spiegare gli Stati Uniti alla guida del settore, il rapporto ne individua alcune, tra cui:

- gli Stati Uniti hanno diverse startup di IA e il suo ecosistema di start-up di IA ha ricevuto il finanziamento di private equity e venture capital;
- guidano lo sviluppo sia dei semiconduttori tradizionali sia dei chip per computer che alimentano i sistemi di intelligenza artificiale;
- producono meno articoli accademici sull'intelligenza artificiale rispetto all'UE o alla Cina, ma in media la loro qualità è superiore.

La Cina è davanti all'Unione europea nell'IA e sta rapidamente riducendo il divario con gli Stati Uniti. Ha più accesso ai dati rispetto all'Unione Europea e agli Stati Uniti, il che è importante perché molti dei sistemi di IA di oggi usano grandi set di dati per addestrare i loro modelli in modo accurato. Nel finanziamento del capitale di rischio e del private equity, le start-up cinesi di AI hanno ricevuto più finanziamenti rispetto a quelle statunitensi nel 2017, ma non nel 2016 o nel 2018.

Per quanto riguarda il talento, la Cina è in ritardo rispetto agli Stati Uniti e all'UE.

L'Unione europea ha il talento per competere con gli Stati Uniti e la Cina: il punto cruciale è che esiste una disconnessione tra la quantità di talenti di intelligenza artificiale nell'UE, la sua adozione e il finanziamento commerciale dell'IA. Ad esempio, le start-up di IA negli Stati Uniti e in Cina hanno ricevuto più fondi di venture capital e fondi di private equity nel solo 2017 rispetto alle start-up di IA dell'UE ricevute tra il 2016 e il 2018.

Fonte Unione Europea e Center for Data Innovation

5G
LA COMMISSIONE RACCOMANDA UN APPROCCIO COMUNE

PERCHÉ IL LANCIO DI RETI 5G È CRUCIALE PER L'EUROPA?

Le reti di quinta generazione (5G) costituiranno la futura spina dorsale delle nostre società ed economie, collegando miliardi di oggetti e sistemi, anche in settori critici come l'energia, i trasporti, le banche e la salute, nonché i sistemi di controllo industriale che trasportano informazioni sensibili e supporto sistemi di sicurezza.

Il 5G è anche una risorsa fondamentale per l'Europa per competere nel mercato globale. Le entrate mondiali del 5G dovrebbero raggiungere l'equivalente di 225 miliardi di euro nel 2025. I vantaggi dell'introduzione del 5G in quattro settori industriali chiave, vale a dire automobilistico, sanitario, trasporti ed energia, possono raggiungere i 114 miliardi di euro all'anno.

La distribuzione del 5G è sotto la responsabilità degli Stati membri. Insieme agli operatori, i paesi dell'UE stanno attualmente adottando misure importanti per prepararla, in particolare attraverso l'organizzazione di aste nazionali per le bande di spettro pertinenti.

A livello dell'UE, il piano d'azione per il 5G fissa il 2020 per il lancio commerciale in tutti gli Stati membri e il 2025 per il lancio globale nelle città e lungo le principali vie di trasporto. L'ultimo rapporto dell'Osservatorio 5G (05/06/2019) della Commissione mostra che gli operatori europei sono in concorrenza con altre importanti regioni del mondo mentre si preparano per il lancio commerciale del 5G. L'Europa è leader mondiale nelle attività di prova del 5G, principalmente grazie al partenariato pubblico-privato 5G della Commissione, principalmente in settori verticali chiave.

Il codice europeo delle comunicazioni elettroniche sosterrà la diffusione e l'adozione delle reti 5G, in particolare per quanto riguarda l'assegnazione dello spettro radio, gli incentivi agli investimenti e le condizioni quadro favorevoli, mentre le norme recentemente adottate sull'Internet aperta forniscono certezza giuridica per quanto riguarda la diffusione di applicazioni 5G. Sul lato privato, gli attori del mercato stanno pianificando i loro investimenti in infrastrutture e creando partnership per portare le soluzioni tecnologiche dalla fase di prova all'implementazione commerciale.

QUALI SONO LE PRINCIPALI SFIDE ALLA SICUREZZA IDENTIFICATE NELLA VALUTAZIONE COORDINATA DEL RISCHIO?

Il rapporto identifica una serie di importanti sfide alla sicurezza, che potrebbero apparire o diventare più importanti nelle reti 5G, rispetto alla situazione nelle reti esistenti:

Queste sfide alla sicurezza sono principalmente legate a:

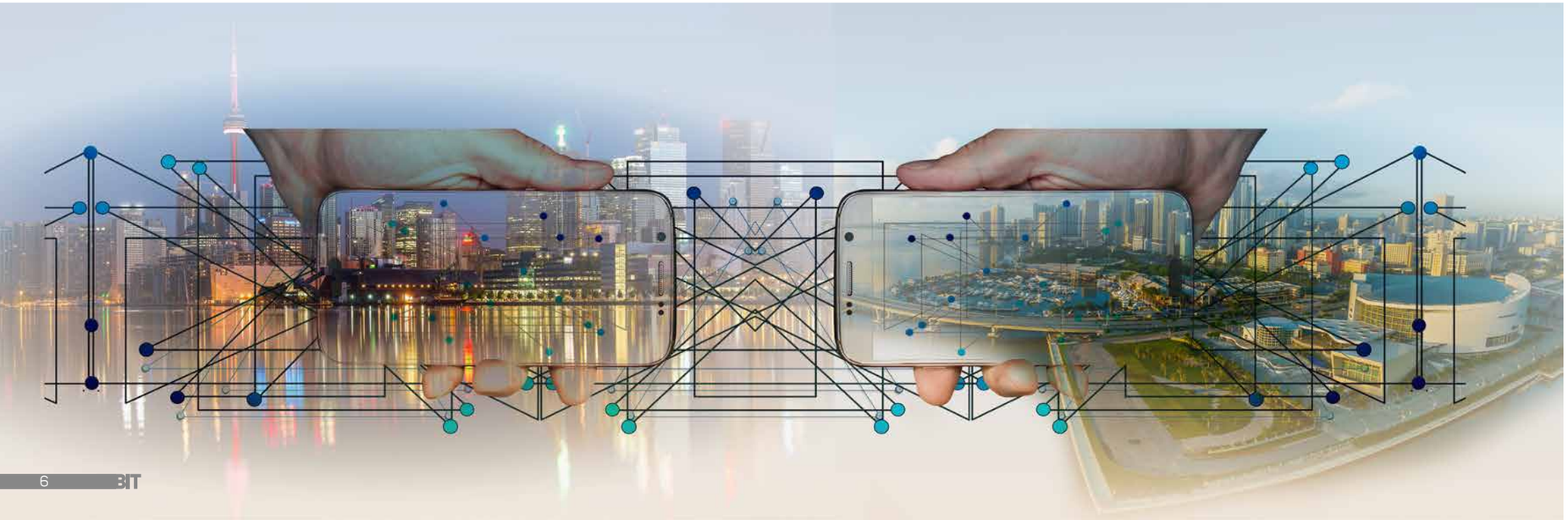
- innovazioni chiave nella tecnologia 5G
- il ruolo dei fornitori nella costruzione e gestione delle reti 5G e il grado di dipendenza dai singoli fornitori.

In particolare, il lancio di reti 5G porterà a:

Una maggiore esposizione agli attacchi e più potenziali punti di ingresso per gli aggressori: con le reti 5G sempre più basate sul software, stanno acquisendo importanza i rischi relativi ai principali difetti di sicurezza, come quelli derivanti da scarsi processi di sviluppo del software all'interno dei fornitori.

A causa delle nuove caratteristiche dell'architettura di rete 5G e delle nuove funzionalità, alcune apparecchiature o funzioni di rete stanno diventando più sensibili, come le stazioni base o le principali funzioni di gestione tecnica delle reti.

Una maggiore esposizione ai rischi legati alla dipendenza degli operatori di rete mobile dai fornitori porterà anche a un numero maggiore di percorsi di attacco ed al conseguente aumento della gravità potenziale dell'impatto di tali attacchi.



In questo contesto di maggiore esposizione agli attacchi facilitati dai fornitori, il profilo di rischio dei singoli fornitori diventerà particolarmente importante, inclusa la probabilità che il fornitore sia soggetto a interferenze da parte di un paese extra UE.

Maggiori rischi derivanti dalle principali dipendenze dai fornitori: una dipendenza maggiore da un singolo fornitore aumenta l'esposizione a una potenziale interruzione dell'offerta, derivante ad esempio da un fallimento commerciale e dalle sue conseguenze. Inoltre aggrava il potenziale impatto delle debolezze o delle vulnerabilità e del loro possibile sfruttamento da parte degli attori delle minacce, in particolare quando la dipendenza riguarda un fornitore che presenta un alto grado di rischio.

Le minacce alla disponibilità e all'integrità delle reti diventeranno i principali problemi di sicurezza: oltre alle minacce alla riservatezza e alla privacy, con le reti 5G che dovrebbero diventare la spina dorsale di molte applicazioni IT critiche, l'integrità e la disponibilità di tali reti diventeranno i principali problemi di sicurezza nazionale e un grande sfida alla sicurezza dal punto di vista dell'UE.

PERCHÉ I RISCHI RELATIVI ALLE FUTURE RETI 5G DEVONO ESSERE VALUTATI?

Una volta realizzate, le reti 5G costituiranno la struttura portante di una vasta gamma di servizi essenziali per il funzionamento del mercato interno e il mantenimento e il funzionamento delle funzioni sociali ed economiche vitali - come l'energia, i trasporti, le banche e la salute, nonché sistemi di controllo industriale. L'organizzazione di processi democratici, come le elezioni, dipenderà sempre di più dalle infrastrutture digitali e dalle reti 5G.

Qualsiasi vulnerabilità nelle reti 5G potrebbe essere sfruttata al fine di compromettere tali sistemi e infrastrutture digitali - potenzialmente causando danni molto gravi o al fine di condurre furti o spionaggio di dati su larga scala. La dipendenza di molti servizi critici dalle reti 5G renderebbe particolarmente gravi le conseguenze di interruzioni sistemiche e diffuse. Ciò giustifica la necessità di un solido approccio basato sul rischio, piuttosto che basarsi principalmente su misure di mitigazione ex post.

Gli Stati membri hanno espresso preoccupazione per i potenziali rischi per la sicurezza connessi alle reti 5G e hanno esplorato o adottato misure per affrontare tali rischi, oltre a dichiarare che non vedevano l'ora di adottare un approccio comune a livello dell'UE nelle conclusioni del Consiglio europeo del 22 Marzo 2019.

Questo è il motivo per cui il 26 marzo 2019 la Commissione ha pubblicato una raccomandazione per gli Stati membri affinché intraprendessero azioni concrete per valutare i rischi di cibersicurezza delle reti 5G e rafforzare le misure di attenuazione dei rischi.

La raccomandazione terrà conto della vasta gamma di strumenti già in atto per rafforzare la cooperazione contro gli attacchi informatici e consentire all'UE di agire collettivamente per proteggere la sua economia e la sua società.

PERCHÉ DOBBIAMO AGIRE A LIVELLO EUROPEO PER PROTEGGERE LE RETI 5G?

Garantire la sicurezza informatica delle reti 5G è una questione di importanza strategica per l'UE, in un momento in cui gli attacchi informatici sono in aumento e più sofisticati che mai.
La natura interconnessa e transnazionale delle infrastrutture digitali e la natura transfrontaliera delle minacce coinvolte significano che qualsiasi vulnerabilità nelle reti 5G o un attacco informatico contro le reti future in uno Stato membro interesserebbe l'Unione nel suo insieme. Ecco perché le misure concertate e adottate a livello nazionale ed europeo devono garantire un elevato livello di sicurezza informatica.

Inoltre, la sicurezza informatica delle reti 5G è fondamentale per garantire l'autonomia strategica dell'Unione, come riconosciuto nella comunicazione congiunta "UE-Cina, una prospettiva strategica". Gli investimenti esteri in settori strategici, le acquisizioni di risorse, tecnologie e infrastrutture critiche nell'UE, il coinvolgimento nella definizione di standard UE e la fornitura di attrezzature essenziali possono comportare rischi per la sicurezza dell'UE. Ciò è particolarmente rilevante per le infrastrutture critiche, come le reti 5G che saranno essenziali per il nostro futuro e dovranno essere completamente sicure.

COME FUNZIONA IL COORDINAMENTO DELL'UE? QUALI SONO I PASSAGGI NECESSARI?

1. A livello nazionale

Tutti gli Stati membri hanno completato una valutazione del rischio nazionale delle infrastrutture di rete 5G. Su questa base, gli Stati membri sono incoraggiati ad aggiornare i requisiti di sicurezza esistenti per i fornitori di rete e includono le condizioni per garantire la sicurezza delle reti pubbliche, in particolare al momento della concessione dei diritti d'uso per le frequenze radio nelle bande 5G. Tali misure dovrebbero includere obblighi rafforzati nei confronti di fornitori e operatori per garantire la sicurezza delle reti. Le valutazioni e misure di rischio nazionali dovrebbero prendere in considerazione vari fattori di rischio, come i rischi tecnici e i rischi legati al comportamento di fornitori o operatori, compresi quelli di paesi terzi. Le valutazioni dei rischi nazionali sono un elemento centrale nella costruzione di una valutazione coordinata dei rischi dell'UE.

Inoltre, gli Stati membri dell'UE hanno il diritto di escludere le società dai loro mercati per motivi di sicurezza nazionale, se non rispettano le norme e il quadro giuridico del paese.

2. A livello dell'UE

Gli Stati membri si sono scambiati informazioni tra loro e, con il sostegno della Commissione e dell'Agenzia europea per la sicurezza informatica (Enisa), hanno ora completato una valutazione coordinata del rischio. Su tale base, gli Stati membri concorderanno una serie di misure di mitigazione che possono essere utilizzate per contenere i rischi di cibersicurezza identificati a livello nazionale e dell'UE. Questi possono includere, ad esempio, requisiti di certificazione, test, controlli, nonché l'identificazione di prodotti o fornitori considerati potenzialmente non sicuri. Tali misure saranno identificate dal gruppo di cooperazione delle autorità competenti come stabilito dalla direttiva sulla sicurezza delle reti e dei sistemi di informazione, con l'aiuto della Commissione e dell'Agenzia europea per la sicurezza informatica. Questo lavoro coordinato dovrebbe sostenere le azioni degli Stati membri a livello nazionale e fornire orientamenti alla Commissione per eventuali ulteriori passi a livello dell'UE. Inoltre, gli Stati membri dovrebbero sviluppare requisiti di sicurezza specifici che potrebbero applicarsi nel contesto degli appalti pubblici relativi alle reti 5G, compresi i requisiti obbligatori per attuare i sistemi di certificazione della cibersicurezza.

QUALE LEGISLAZIONE DELL'UE È GIÀ IN ATTO O È IN FASE DI ATTUAZIONE PER PROTEGGERE LE FUTURE RETI 5G?

L'UE dispone di una serie di strumenti per proteggere le reti di comunicazione elettronica, tra cui la prima normativa dell'UE in materia di cibersicurezza (direttiva sulla sicurezza delle reti e dei sistemi di informazione), la legge sulla cibersicurezza recentemente approvata dal Parlamento europeo e le nuove norme dell'UE in materia di telecomunicazioni.

Inoltre, gli Stati membri dell'UE possono escludere le società dai loro mercati per motivi di sicurezza nazionale, se non rispettano le norme e il quadro giuridico del paese.

Norme nel settore delle telecomunicazioni: gli Stati membri devono garantire il mantenimento dell'integrità e della sicurezza delle reti pubbliche di comunicazione, con l'obbligo di garantire che gli operatori adottino misure tecniche e organizzative per gestire adeguatamente i rischi per la sicurezza delle reti e dei servizi. Il nuovo codice delle telecomunicazioni prevede inoltre che le autorità nazionali di regolamentazione competenti dispongano di poteri, compreso il potere di emettere istruzioni vincolanti e garantire la loro conformità. Inoltre, gli Stati membri sono autorizzati ad applicare condizioni relative alla sicurezza delle reti pubbliche contro l'accesso non autorizzato all'autorizzazione generale, al fine di proteggere la riservatezza delle comunicazioni.

Strumenti nel campo della sicurezza informatica: il quadro europeo di certificazione della sicurezza informatica per prodotti, processi e servizi digitali fornisce uno strumento di supporto essenziale per promuovere livelli coerenti di sicurezza. Dovrebbe consentire lo sviluppo di schemi di certificazione della sicurezza informatica per rispondere alle esigenze degli utenti di apparecchiature e software relativi al 5G.

Per sostenere l'attuazione di tali obblighi e strumenti, l'Unione ha istituito una serie di organismi di cooperazione. L'Agenzia europea per la sicurezza informatica (Enisa), la Commissione, gli Stati

membri e le autorità nazionali di regolamentazione hanno sviluppato linee guida tecniche per le autorità nazionali di regolamentazione in materia di segnalazione di incidenti, misure di sicurezza e minacce e beni. Il gruppo di cooperazione istituito dalla direttiva sulla sicurezza della rete e dei sistemi di informazione riunisce le autorità competenti al fine di sostenere e facilitare la cooperazione, in particolare fornendo orientamenti strategici.

Garantire la sicurezza informatica richiede anche il mantenimento di un'autonomia strategica di livello sufficiente, attraverso il raggiungimento di una massa critica di investimenti nella sicurezza informatica e tecnologie digitali avanzate nell'UE. La Commissione ha pertanto proposto di rendere prioritario questo obiettivo nel prossimo periodo di bilancio dell'UE, in particolare attraverso la sua proposta per un programma Europa digitale, e ha proposto un nuovo centro europeo di competenza in materia di cibersicurezza e una rete per attuare progetti pertinenti nel settore della cibersicurezza.

Norme in materia di appalti pubblici: le norme dell'UE in materia di appalti pubblici contribuiscono a ottenere un migliore valore per i soldi dei contribuenti garantendo che gli appalti pubblici siano aggiudicati attraverso procedure di gara competitive, aperte, trasparenti e ben regolamentate.

Le direttive UE in materia di appalti pubblici non distinguono tra operatori economici dell'UE e di paesi terzi, ma includono una serie di garanzie. Ad esempio, consentono alle amministrazioni aggiudicatrici di respingere a determinate condizioni gare d'appalto ingiustificatamente basse o che non rispettano le norme in materia di sicurezza, lavoro e ambiente. Consentono inoltre alle autorità di contatto di proteggere i loro interessi essenziali in materia di sicurezza e difesa.

Norme per lo screening degli investimenti diretti esteri: il nuovo regolamento è entrato in vigore nell'aprile 2019 e si applicherà integralmente a partire da novembre 2020. Fornirà un potente strumento per rilevare e sensibilizzare sugli investimenti esteri in attività, tecnologie e infrastrutture essenziali. Consentirà inoltre di identificare e affrontare collettivamente le minacce alla sicurezza e all'ordine pubblico poste da acquisizioni in settori sensibili. Gli Stati membri dovrebbero utilizzare il periodo tra l'entrata in vigore e l'inizio dell'applicazione del regolamento per apportare le modifiche necessarie alle rispettive prassi e legislazioni nazionali e istituire strutture amministrative per garantire un'efficace cooperazione a livello dell'UE con la Commissione conformemente i meccanismi stabiliti.

Regime sanzionatorio orizzontale per contrastare gli attacchi informatici: il nuovo regime concordato dagli Stati membri nel maggio 2019 avrà una copertura mondiale e consentirà una risposta flessibile dell'UE a prescindere dal luogo da cui sono stati lanciati gli attacchi informatici e indipendentemente dal fatto che siano effettuati da attori statali o non statali. Questo regime sanzionatorio, una volta adottato, consentirebbe all'Unione di rispondere agli attacchi informatici con un "effetto significativo" che minaccia l'integrità e la sicurezza dell'UE, dei suoi Stati membri e dei nostri cittadini.

QUAL È IL RUOLO DELL'AGENZIA EUROPEA PER LA SICUREZZA INFORMATICA IN QUESTO COORDINAMENTO?

La legge sulla cibersicurezza conferisce un mandato permanente e più forte all'Agenzia europea per la cibersicurezza.

L'Agenzia europea per la sicurezza informatica sta già fornendo sostegno alla Commissione nel settore della sicurezza delle reti di telecomunicazioni. Insieme agli Stati membri e alle autorità nazionali di regolamentazione, l'Enisa ha sviluppato linee guida tecniche per le autorità nazionali di regolamentazione in materia di segnalazione di incidenti, misure di sicurezza, minacce e risorse.

Inoltre, l'Agenzia europea per la sicurezza informatica ha preparato un'apposita mappatura del panorama delle minacce delle reti 5G, che considera più in dettaglio alcuni aspetti tecnici trattati nella relazione di alto livello. L'Agenzia europea per la sicurezza informatica lavorerà anche allo sviluppo di schemi di certificazione a livello europeo, come previsto dalla legge sulla sicurezza informatica.

Fonte UE

ECONOMIA DIGITALE
LO STATO DELL'ARTE

Il Rapporto sull'economia digitale (Digital Economy Report 2019) recentemente pubblicato dall'UNCTAD - la Conferenza delle Nazioni Unite per il commercio e lo sviluppo - evidenzia come la rapida espansione dell'economia digitale stia offrendo opportunità economiche uniche ma anche sfide che devono essere gestiti implementando nuove politiche a livello locale, nazionale e internazionale, in particolare focalizzate sulla gestione e la sicurezza dei dati.

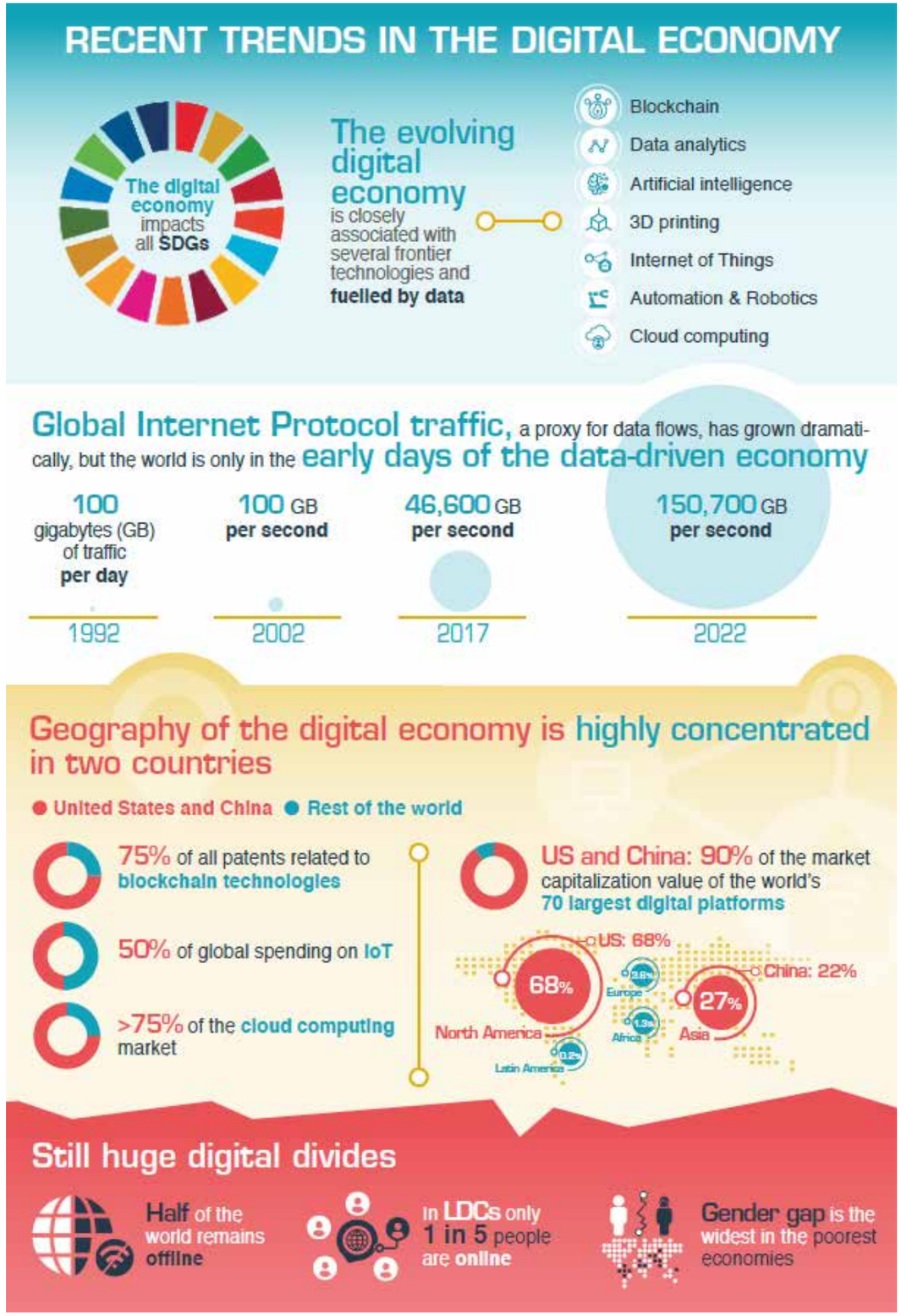
L'economia digitale si sta evolvendo a una velocità molto rapida ed è guidata dalla capacità di raccogliere, utilizzare e analizzare enormi quantità di dati digitali. Il traffico IP (Global Internet Protocol) è cresciuto da circa 100 gigabyte (GB) al giorno nel 1992 a oltre 45.000 GB al secondo nel 2017 e si prevede che raggiungerà i 150.700 GB al secondo nel 2020.

Oltre ai dati c'è un altro fattore chiave dell'economia digitale che è la "platformizzazione". Negli ultimi dieci anni sono apparse diverse piattaforme digitali e il loro potere si riflette nel fatto che sette delle prime otto società al mondo per capitalizzazione di mercato utilizzano modelli di business basati su piattaforma.

Nella geografia economica del divario digitale possiamo osservare che due paesi stanno guidando questa rivoluzione: gli Stati Uniti e la Cina. Usa e Cina rappresentano il 75% di tutti i brevetti relativi alle tecnologie blockchain, il 50% della spesa globale per l'IoT e oltre il 75% del mercato mondiale per il cloud computing pubblico. In questo contesto, la quota dell'Europa è solo del 4%, mentre Africa e America Latina insieme rappresentano solo l'1%.

È innegabile che l'economia digitale stia crescendo, ma misurare la relativa creazione di valore può essere difficile in quanto non esiste una definizione ampiamente accettata di economia digitale e anche perché mancano statistiche affidabili su di essa, soprattutto nei paesi in via di sviluppo. Tuttavia, si stima che le dimensioni dell'economia digitale siano comprese tra 4,5 e 15,5 del PIL mondiale.

Fonte UNCTAD - United Nations Conference on Trade and Development



IL “GIUSTO” METODO PER SCEGLIERE LA “GIUSTA” TECNOLOGIA

I progressi della tecnologia e quelli, più in generale, della scienza sono certamente tra i fattori chiave per assicurare benefici alla società e all’economia. Tuttavia, va riscontrato che la pervasività delle tecnologie più recenti, dovuta anche al fenomeno della globalizzazione, pone nuove sfide e rischi per la società. Tra i rischi maggiormente percepiti dall’opinione pubblica ci sono principalmente quelli connessi alla salute, all’ambiente e alla sicurezza.

Partendo dal queste premesse, la statunitense Rand Corporation, uno dei più prestigiosi e accreditati pensatoi mondiali, ritiene che sia necessaria una infrastruttura per la gestione e il controllo delle tecnologie e dei progressi scientifici o un processo di supervisione degli stessi, al fine sia di capitalizzare i benefici e le opportunità generate dallo sviluppo della ricerca scientifica e dall’introduzione delle nuove tecnologie nella vita quotidiana sia di minimizzarne i potenziali fattori di rischio.

Questo processo di gestione, per indirizzare lo sviluppo di nuove scienze o tecnologie nel tempo, è noto come “supervisione” o “sorveglianza”.

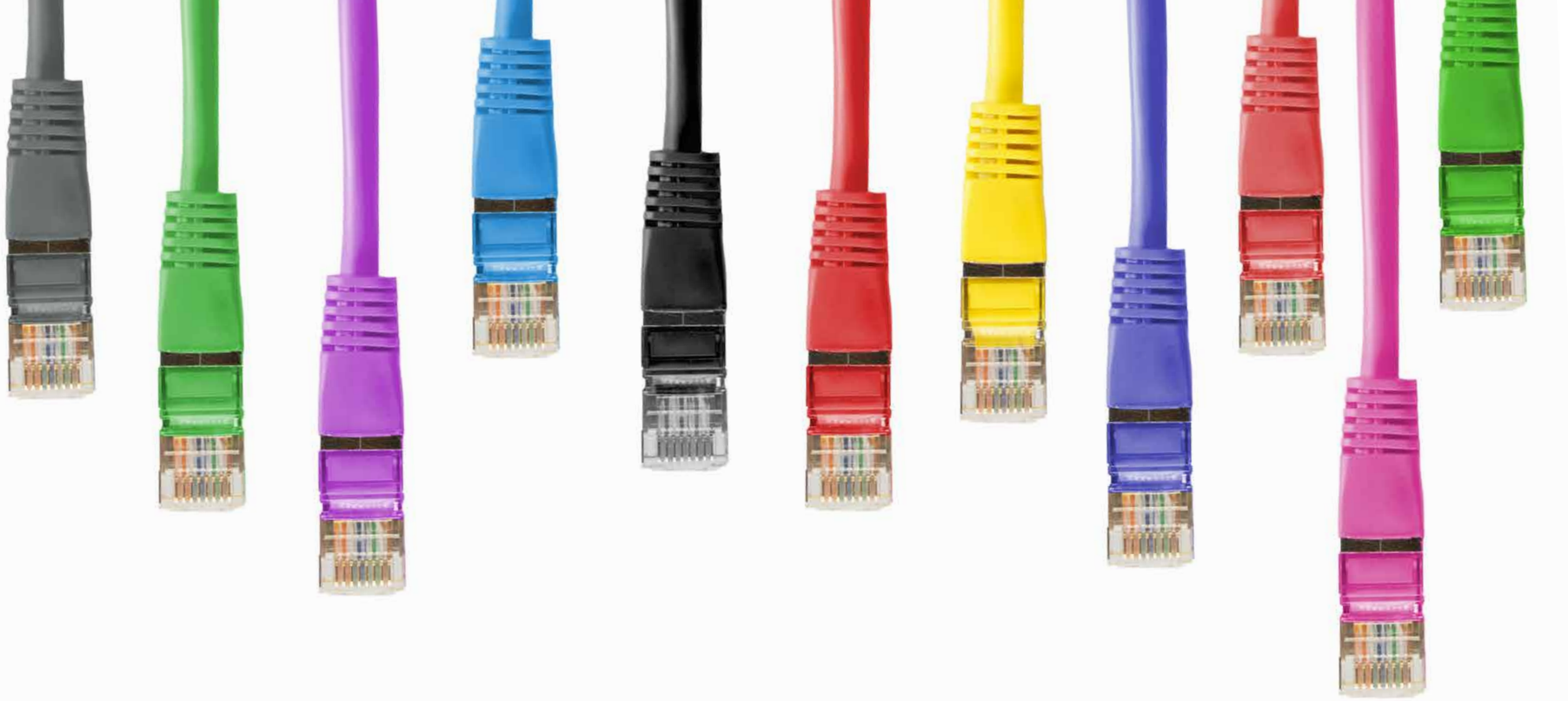
Nell’ambito di uno studio (*Oversight of emerging science and technology. Learning from past and present efforts around the world*), commissionato dalla Wellcome Trust, la Rand Corporation ha “supervisionato” alcuni risultati scientifici e tecnologie emergenti in casi storici e contemporanei che coprono diversi paesi ed abbracciano differenti settori e aree scientifico-tecnologiche, e ne ha estratto temi e lezioni comuni. I ricercatori della Rand Corporation hanno individuato 10 casi studio per esplorare l’efficacia dei metodi di supervisione e identificare i principi guida. La ricerca fa parte di un più ampio progetto della Wellcome Trust per stabilire i passi necessari per posizionare il Regno Unito come leader globale nella supervisione efficace, efficiente ed etica della scienza e della tecnologia emergenti.

I principi guida del processo di supervisione

L’analisi ha identificato una serie di lezioni comuni - o principi guida - che sono abbastanza ampi da poter essere utilmente considerati in altri contesti di supervisione scientifica e tecnologica emergente.

La supervisione scientifico-tecnologica deve essere:

- Equilibrata: è importante che gli approcci di supervisione mirino a bilanciare i vantaggi e i rischi contrastanti associati alla scienza o alla tecnologia emergenti, nonché alle esigenze dei diversi stakeholder.
- Diversa e contestuale: non esiste un approccio “unico per tutti” nei confronti della sorveglianza scientifica e tecnologica emergente - è fondamentale tenere conto del contesto in cui la scienza o la tecnologia si sta sviluppando.
- Proattiva: le parti interessate che prendono l’iniziativa per creare tempestivamente strutture di supervisione possono trarre vantaggio dalle opportunità offerte dalla scienza o dalla tecnologia emergenti e anche aiutare a identificare i rischi.
- Anticipatoria: è utile anticipare i diversi percorsi potenziali che una scienza o una tecnologia emergente potrebbe seguire man mano che si evolve nel tempo, nonché i conseguenti impatti.
- Adattabile: affinché un approccio di supervisione sia efficace, deve aiutare a costruire flessibilità in modo che possa rispondere ai cambiamenti e adattarsi nel tempo con l’evoluzione della scienza o della tecnologia.
- Collaborativa: l’adozione di un approccio inclusivo e partecipativo alla sorveglianza scientifica e tecnologica aiuta a costruire responsabilità e fiducia.
- Comunicativa: una comunicazione efficace tra i principali attori coinvolti nel processo di supervisione facilita la trasparenza e la chiarezza di ruoli e responsabilità.
- Impegnata con il pubblico: sfruttare il ruolo del pubblico può aiutare a costruire responsabilità e fiducia e anche impegnarsi



I casi studio analizzati

• Il protocollo di Cartagena sulla biosicurezza

L'uso crescente di organismi geneticamente modificati (OGM) negli anni '90, in particolare nel settore della biotecnologia agricola, ha portato con sé una crescente preoccupazione pubblica per i possibili rischi ambientali e per la salute umana associati agli OGM. Ciò è stato riscontrato in particolare nei paesi in via di sviluppo che non partecipavano ancora al commercio di OGM ed erano preoccupati per i rischi di ingresso di questi organismi nei loro paesi anche a loro insaputa. Per far fronte a queste preoccupazioni, è stato concepito il Protocollo di Cartagena del 2003 sulla biosicurezza come un accordo internazionale giuridicamente vincolante per governare il movimento di organismi geneticamente modificati attraverso i confini.

• E-government e società digitale in Estonia

Dalla metà degli anni '90 in poi, l'Estonia è emersa come uno dei primi promotori delle attività relative all'e-government e alla più ampia società digitale. Il governo estone ha adottato misure per sostenere l'integrazione della tecnologia dell'informazione e delle comunicazioni (TIC) nei servizi governativi e gettare le basi per una società digitale in senso lato. La sua supervisione comprendeva meccanismi di ampia portata (e collaborazione con le parti interessate del settore privato), tra cui: documenti strategici; legislazione; incentivi fiscali; standardizzazione; infrastruttura tecnologica e sviluppo delle capacità; e programmi educativi progettati per sviluppare competenze TIC.

• Sandbox regolamentari Fintech

L'emergere di nuove tecnologie finanziarie (fintech – financial technology) potenzialmente dirompenti genera opportunità ma comporta anche nuovi rischi, sia per i sistemi bancari che per i consumatori. Prendendo a prestito da approcci di "sandbox" implementati in altri contesti, la Financial Conduct Authority (FCA) del Regno Unito nel 2015 ha sviluppato il concetto di "sandbox normativo" fintech; uno "spazio sicuro" regolamentare in cui le imprese ammissibili possono effettuare prove limitate su prodotti innovativi fintech pur essendo esenti da determinati requisiti normativi. Il concetto si è rivelato popolare con altri governi, in particolare nella regione Asia-Pacifico.

• La rivoluzione verde: il caso della tecnologia agricola in India

Alla fine degli anni '50, gli istituti internazionali di ricerca agricola avevano sviluppato nuove varietà ad alto rendimento (HYV) di grano che potevano essere coltivate su vasta scala in una ampia gamma di ambienti. In combinazione con un pacchetto di altre innovazioni agricole - tra cui fertilizzanti, pesticidi e metodi di irrigazione - gli HYV promettevano una resa agricola significativamente più elevata rispetto alla maggior parte delle colture tradizionali. Dalla metà degli anni '60 in poi, insieme alle parti interessate internazionali, il governo indiano ha costruito una vasta infrastruttura pubblica focalizzata sulla promozione di queste nuove tecnologie agricole.

• M-Pesa: mobile banking senza filiali in Kenya

Il servizio M-Pesa, fornito dall'operatore di rete mobile keniota, Safaricom, e dalla società di telecomunicazioni Vodacom, nel 2007, ha aperto la strada all'uso dei telefoni cellulari per estendere i servizi bancari di base alle popolazioni precedentemente senza accesso. Lo sviluppo di M-Pesa ha spinto gli sforzi della Banca centrale del Kenya a creare un ambiente favorevole alla crescita del servizio. La banca ha lavorato a stretto contatto con gli sviluppatori di servizi e i cittadini per aiutare l'espansione del mobile banking senza filiali, cercando anche di limitare i potenziali rischi finanziari associati alla tecnologia.

• DAMD: la banca dati di medicina generale della Danimarca

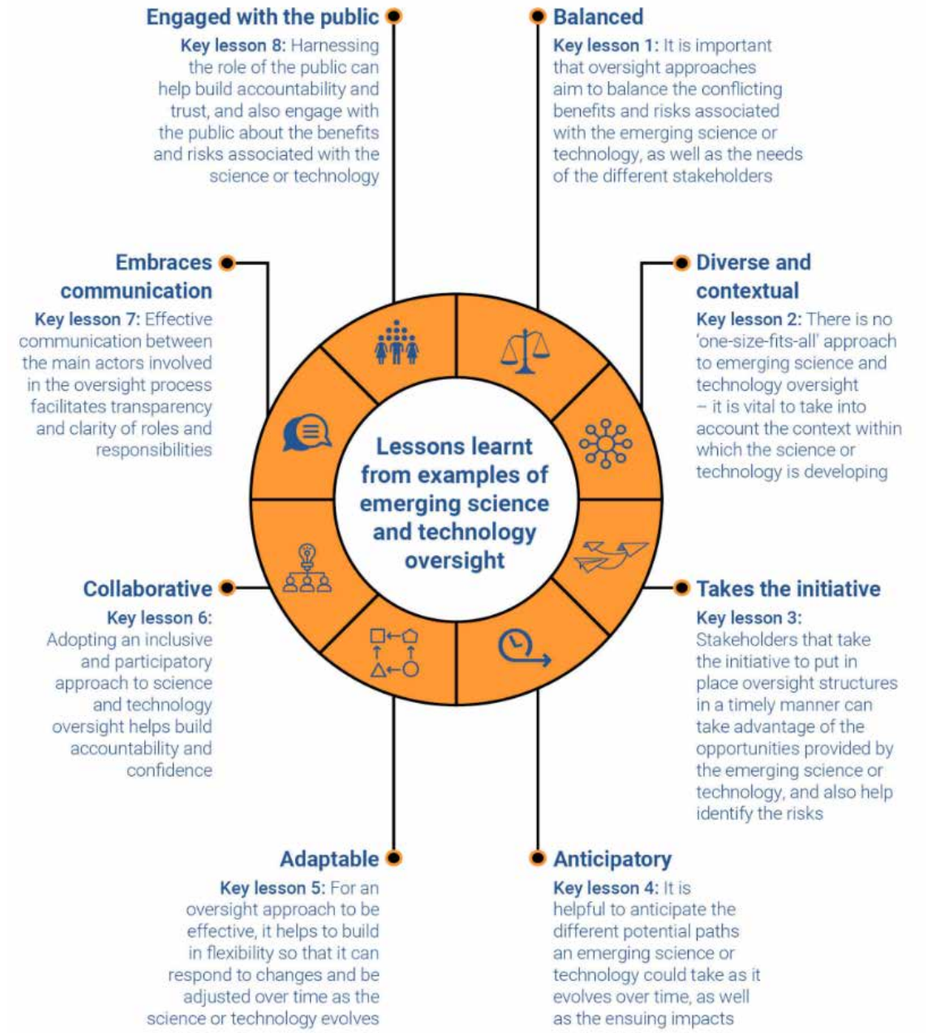
Dalla fine degli anni '90 in poi, i Paesi europei hanno iniziato a promuovere la digitalizzazione nei sistemi sanitari. Come parte di questo programma, la digitalizzazione dei dati dei pazienti ha permesso di migliorare notevolmente l'offerta di assistenza sanitaria e l'analisi dei sistemi sanitari. In questo contesto, dal 2003 in poi, i medici generici danesi

hanno collaborato con le autorità sanitarie regionali per sviluppare un sistema (DAMD - Dansk AlmenMedicinsk Database)in grado di acquisire e archiviare automaticamente e continuamente i dati raccolti dai sistemi ICT.

• Il comitato consultivo del DNA ricombinante dell'NIH negli Stati Uniti
La tecnologia del DNA ricombinante (rDNA) iniziò ad emergere alla fine degli anni '60 con lo sviluppo di tecniche per la giunzione di molecole di DNA. La tecnologia del DNA ricombinante offriva una serie di possibilità per la ricerca biologica molecolare, compresa la terapia genica e le modificazioni genetiche. Riconoscendo sia le potenziali applicazioni dell'rDNA, sia i suoi molteplici rischi, la comunità scientifica ha cercato di sviluppare forum in cui discutere degli usi dell'rDNA. Negli Stati Uniti, questi sforzi hanno portato alla formazione, nel 1973, del Comitato consultivo per il DNA ricombinante del National Institutes of Health (NIH).

• Human Fertilization and Embryology Act nel Regno Unito
Nel 1990, per rispondere alle preoccupazioni pubbliche e parlamentari relative alle questioni legali, sociali ed etiche associate agli sviluppi nella ricerca e nel trattamento della fertilità umana, il Regno Unito ha adottato lo Human Fertilization and Embryology Act. La legge regolava le licenze delle cliniche per garantire la protezione dei pazienti e stabiliva misure che consentivano alla ricerca scientifica di progredire in modo responsabile. Un componente chiave è stata la creazione di un ente normativo indipendente - la Human Fertilization and Embryology Authority (HFEA) - per supervisionare le tecnologie di riproduzione assistita.

• La prima crittografia pubblica negli Stati Uniti
L'invenzione, a metà degli anni '70, della "crittografia a chiave pubblica" ha permesso lo scambio di messaggi crittografati tra le persone. Il suo sviluppo ha in seguito consentito di integrare la crittografia complessa nei formati di comunicazione di tutti i giorni, come le reti telefoniche e di posta elettronica, aiutando questi mercati a crescere. Le agenzie governative degli Stati Uniti, preoccupate per l'impatto della crittografia pubblica sulla loro capacità di monitorare le comunicazioni, hanno cercato di limitare l'accesso del pubblico a questa tecnologia. E dall'inizio degli anni '90 in poi hanno promosso i programmi che avrebbero fornito "backdoor" nei sistemi di crittografia. Nel frattempo, un'ampia coalizione di attori non statali - compresi crittografi, sostenitori della privacy e interessi industriali - ha combattuto contro l'agenda del governo. Sollecitati da una serie di interessi, dalla protezione delle libertà civili alle preoccupazioni sulla competitività industriale, questi gruppi hanno cercato di proteggere un accesso diffuso e non mediato ai sistemi di crittografia.



Fonte: RAND Europe analysis

SOCIAL IMPACT BANKING

60 milioni di euro per le microimprese italiane

Il FEI (Fondo europeo per gli investimenti, facente parte del gruppo BEI Banca europea per gli investimenti) e UniCredit hanno firmato un accordo di 60 milioni di euro a sostegno delle microimprese italiane. Il sostegno assume la forma di microfinanza, fornita con una garanzia sostenuta dall'UE nell'ambito del programma EaSI (Occupazione e innovazione sociale) della Commissione europea. I prestiti sono disponibili per singoli imprenditori e microimprese con meno di 10 dipendenti e un massimo di 2 milioni di euro di fatturato annuo o totale attivo. L'obiettivo è sostenere quelle imprese con prestiti fino a un massimo di 25000 euro, nonché fornire loro sostegno allo sviluppo delle loro attività e all'accesso a una rete di partner del settore pertinente.

UniCredit è una banca commerciale paneuropea, che fornisce una articolata rete europea al suo vasto franchising di clienti. UniCredit offre ai suoi clienti competenze sia locali che internazionali, offrendo loro un accesso alle principali banche nei suoi 14 mercati principali attraverso la rete bancaria europea: Italia, Germania, Austria, Bosnia ed Erzegovina, Bulgaria, Croazia, Repubblica Ceca, Ungheria, Romania, Russia, Serbia, Slovacchia, Slovenia e Turchia. Facendo leva su una rete internazionale di uffici di rappresentanza e filiali, UniCredit serve clienti in altri 18 paesi.

Questo accordo fa seguito a quello firmato nel marzo 2018, per una garanzia di portafoglio di 50 milioni di euro, a beneficio di circa 2.500 microimprese italiane. Arriva anche sulla scia dei recenti accordi del Gruppo BEI a sostegno delle PMI italiane con particolare attenzione alle donne imprenditrici e all'innovazione (400 milioni di euro), alla lotta ai cambiamenti climatici (100 milioni di euro), nonché all'accordo di 50 milioni di euro a sostegno dei servizi sociali imprese. Questo secondo accordo di microfinanza EaSi copre un portafoglio più ampio per classi di rischio più elevate rispetto al primo accordo del 2018, aprendolo a più microimprese rispetto a prima.

Il Fondo europeo per gli investimenti (FEI) è un istituto finanziario che fa parte del gruppo BEI (Banca europea per gli investimenti). Il suo compito principale è quello di sostenere le micro, piccole e medie imprese (PMI) in Europa, facilitando il loro accesso al credito. Il FEI definisce e sviluppa strumenti azionari, garanzie e strutture di microcredito su misura per le esigenze di questa categoria di imprese. Nello svolgimento di questo ruolo, il FEI persegue gli obiettivi dell'UE in materia di innovazione, ricerca e sviluppo, imprenditorialità, crescita e occupazione.

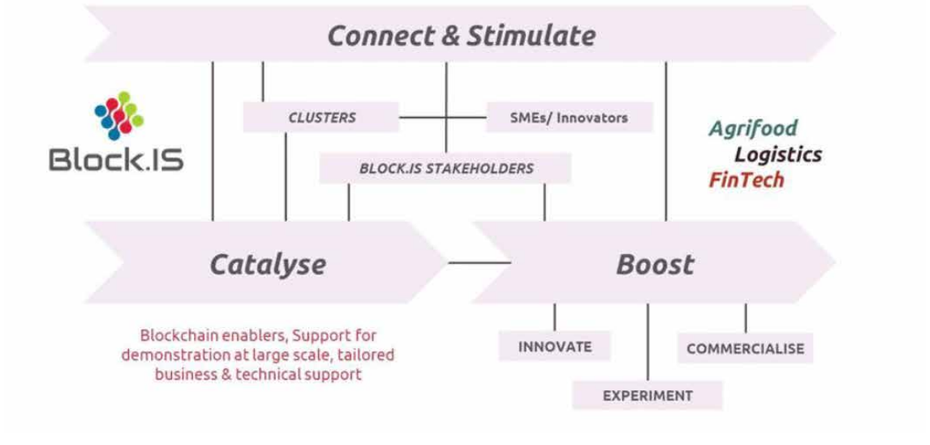
Il programma dell'UE per l'occupazione e l'innovazione sociale (EaSI) mira a sostenere l'obiettivo dell'UE di un'occupazione di alto livello, un'adeguata protezione sociale, la lotta contro l'esclusione sociale e la povertà e il miglioramento delle condizioni di lavoro. L'asse di microfinanza e imprenditoria sociale del programma EaSI fornisce sostegno agli intermediari finanziari che offrono microcrediti agli imprenditori o finanziamenti alle imprese sociali. L'obiettivo è aumentare l'accesso alla microfinanza, che comprende il microcredito, vale a dire prestiti fino a 25.000 EUR, in particolare per le persone vulnerabili e le microimprese. Inoltre, per la prima volta, l'UE sostiene le imprese sociali attraverso investimenti fino a 500.000 EUR. Il sostegno alla microfinanza e all'imprenditoria sociale è attualmente in fase di attuazione attraverso la garanzia EaSI, che consente agli intermediari finanziari di raggiungere (potenziali) imprenditori che non sarebbero stati in grado di ottenere finanziamenti altrimenti a causa di considerazioni di rischio. Viene inoltre implementato attraverso la "Finestra degli investimenti EaSI" per rafforzare la capacità degli intermediari finanziari nei settori della microfinanza e della finanza sociale attraverso investimenti azionari. La Commissione europea ha selezionato il FEI per attuare la garanzia EaSI e la Finestra per gli investimenti nello sviluppo delle capacità dell'EaSI.

BLOKCHAIN
fondi per i settori Agrifood, Logistica e finanziario

Block.IS organizzerà due inviti aperti per attrarre, selezionare e finanziare il meglio delle migliori PMI per generare prodotti, processi e modelli di business basati su blockchain con un forte potenziale di mercato nei settori agroalimentare, logistico e finanziario.

Affinché l'economia dell'UE cresca in modo sostenibile, deve essere reindustrializzata, sfruttando l'innovazione e l'intelligenza digitale. Tra i settori più importanti dell'economia dell'UE si possono trovare i settori agroalimentare, logistico e finanziario. Il settore agroalimentare dell'UE ha una forte posizione competitiva globale in quanto principale esportatore di alimenti e bevande con una quota di mercato del 18%. Il settore della logistica ammonta al 14% del PIL dell'UE e il settore dovrebbe crescere del 40% entro il 2040. Il settore finanziario rappresenta fino al 20-30% delle entrate totali del mercato dei servizi e circa il 20% del prodotto interno lordo totale nell'UE economie.

La tecnologia Blockchain è stata riconosciuta da persone e istituzioni influenti, tra cui EC e WEF, come una delle tecnologie più promettenti e dirompenti di questo secolo. La tecnologia presenta una combinazione unica di funzionalità che la rendono ideale per risolvere le sfide sopra menzionate - provenienza, trasparenza, tracciabilità, efficienza, fiducia, condivisione dei dati - nei tre settori. La tecnologia Blockchain consente un modo decentralizzato, affidabile e programmabile per trasferire valore e informazioni.
Il bando è articolato in tre fasi:
Innovazione: 45 PMI saranno invitate a elaborare un primo prototipo della soluzione proposta;
Sperimentazione: 23 PMI delle prime 45 verranno invitate a sviluppare la soluzione proposta;
Commercializzazione: 10 PMI verranno invitate a sviluppare attività legate alla promozione dei propri progetti;
Ogni impresa potrà ricevere al **massimo 60.000€** Le imprese interessate possono candidarsi entro il **6 novembre 2019**.
Maggiori informazioni presso il sito: Block:Is e la pagina



L'approccio Block.IS Block.IS mira a fornire alle PMI europee competitive e orientate al mercato l'accesso a conoscenze, tecnologia, capitali e mercati allo scopo di collocare nuovi prodotti e servizi nel mercato mirando alla tecnologia blockchaint. Il progetto ha tre dimensioni principali:

I. Connect & Stimulate: mira a costituite sinergie tra cluster per condividere le migliori pratiche sull'innovazione stimolando le PMI e gli innovatori a superare le sfide poste dalle esigenze del mercato.
II. Catalyse: ha lo scopo di creare un solido quadro di supporto tecnico e commerciale per lo sviluppo di strumenti per la blockchain al fine di catalizzare il potenziale e il raggio d'azione dell'applicazione della tecnologia Blockchain nei diversi settori. In questa fase, oltre al supporto tecnico e alla formazione, Block.IS offre ai beneficiari selezionati abilitatori software basati su blockchain che implementano funzionalità comunemente utilizzate in varie applicazioni per accelerare lo sviluppo di nuove applicazioni e il lancio di nuovi prodotti / servizi sul mercato.
III. Boost: un ambizioso programma di accelerazione in 3 fasi (innovazione, sperimentazione, commercializzazione) che mira a sostenere l'adozione e l'impatto sul mercato delle innovazioni / soluzioni proposte

SPACE ECONOMY
100 milioni di euro in favore di progetti di ricerca e sviluppo presentati dalle imprese

A partire dal 15 ottobre le imprese in possesso dei requisiti previsti dal **Programma Mirror GovSatCom** potranno presentare domanda per il sostegno a progetti di ricerca industriale e di sviluppo sperimentale. Si tratta di progetti che rientrano nell'ambito del Piano Strategico Nazionale e degli Accordi di innovazione per la **Space Economy**. È stato, infatti, pubblicato oggi il decreto del MiSE che disciplina le modalità e i termini per la presentazione delle domande di agevolazione.

Le risorse finanziare disponibili sono pari a **100 milioni di euro**, di cui circa 42 milioni di euro messi a disposizione dal Ministero dello Sviluppo economico. I restanti 58 milioni di euro sono a valere sulle risorse messe a disposizione da Regioni e Province autonome.

L'agevolazione verrà concessa sulla base di una procedura negoziale, secondo quanto previsto dagli Accordi per l'innovazione.

Per maggiori informazioni

- Decreto 26 settembre 2019 – Accordi di innovazione per la Space Economy. Modalità e termini di attuazione dell'intervento agevolativo
- Programma "Mirror GovSatCom" (Accordi di innovazione per la Space Economy)

Ufficio competente del Mise: Divisione VII - Interventi per ricerca e sviluppo

Fonte MiSE

PRE-ANNUNCIO
di AAL Call Challenge 2020

AAL Call 2020 fa parte del programma Active & Assisted Living (Programma AAL) che è stato approvato nel maggio 2014 dal Parlamento europeo e dal Consiglio dell'Unione europea. Nell'ambito del programma di lavoro, AAL intende lanciare un nuovo invito per la presentazione di proposte relative a "**Healthy Ageing through Digital Solutions and Ecosystems**".

L'obiettivo dell'invito è sostenere progetti di collaborazione innovativi, transnazionali e multidisciplinari. La Call 2020 è caratterizzata dal seguente approccio:

1. L'AAL Call 2020 sta promuovendo un approccio al corso di vita per la salute e il benessere ed è aperto allo sviluppo di nuovi prodotti ICT, servizi associati e loro implementazione finale, rivolti a qualsiasi area di applicazione all'interno del dominio AAL. Oltre a concentrarsi sugli adulti più anziani, le proposte dovrebbero considerare l'applicabilità delle soluzioni proposte ad altri gruppi di popolazione. Le soluzioni proposte devono essere integrate nelle strategie delle organizzazioni degli utenti finali, dei fornitori di servizi e dei partner commerciali partecipanti.

2. L'invito AAL 2020 consente flessibilità riguardo alla portata, alle dimensioni e alla durata dei progetti proposti (compresi i piccoli progetti collaborativi). I desideri e le esigenze degli utenti finali coinvolti in combinazione con le richieste delle altre parti interessate (fornitori e finanziatori) svolgeranno un ruolo fondamentale nella definizione di soluzioni AAL utili e attraenti con un elevato potenziale di mercato, nonché nella promozione e nel rafforzamento degli ecosistemi a supporto dell' "invecchiamento in buona salute". Sia i "Progetti collaborativi" che i "Piccoli progetti collaborativi" saranno ancora finanziati attraverso questo invito.

Progetti collaborativi - Principali caratteristiche e obiettivi
I progetti collaborativi mirano a sviluppare e portare sul mercato soluzioni TIC nel settore AAL. Le proposte di AAL Call 2020 dovrebbero essere guidate dagli utenti attraverso la co-creazione e affrontare una sfida specifica. L'invito sottolinea un forte coinvolgimento degli utenti finali, in particolare secondari e terziari, e di altre parti interessate nella definizione delle soluzioni e nella creazione dei rispettivi mercati. Inoltre, la strada per il mercato deve essere chiaramente descritta e allineata con le strategie commerciali dei partner responsabili della commercializzazione. Le soluzioni proposte devono rispondere a requisiti diversi, a seconda del tipo di mercato.

Piccoli progetti collaborativi - Principali caratteristiche e obiettivi
Questo tipo di strumento sarà disponibile nell'invito 2020. I piccoli progetti di collaborazione hanno una durata di 9 mesi, un budget massimo di cofinanziamento di € 300.000 e procedure di presentazione e comunicazione più snelle. L'obiettivo principale dei piccoli progetti collaborativi è l'esplorazione di nuove idee, concetti e approcci per soluzioni basate sulle TIC per gli anziani. Dovrebbero raggiungere i nuovi stakeholder per l'inclusione nello sviluppo (futuro) delle soluzioni AAL, costruire forti collaborazioni con organizzazioni di utenti finali, supportare la costruzione di comunità con nuovi clienti e creare programmi condivisi.

Notare che:
Le informazioni sull'invito finale sono destinate a essere pubblicate con il lancio dell'invito sul sito web AAL all'inizio di febbraio 2020, la scadenza per la presentazione di una proposta di progetto è prevista per la fine di maggio 2020. Sono previste giornate informative prima del lancio del Bando. I potenziali candidati sono invitati a registrarsi alla newsletter del programma AAL o a monitorare il sito Web del programma.

IL "BIOMATTONE" CHE TAGLIA LA CLIMATIZZAZIONE

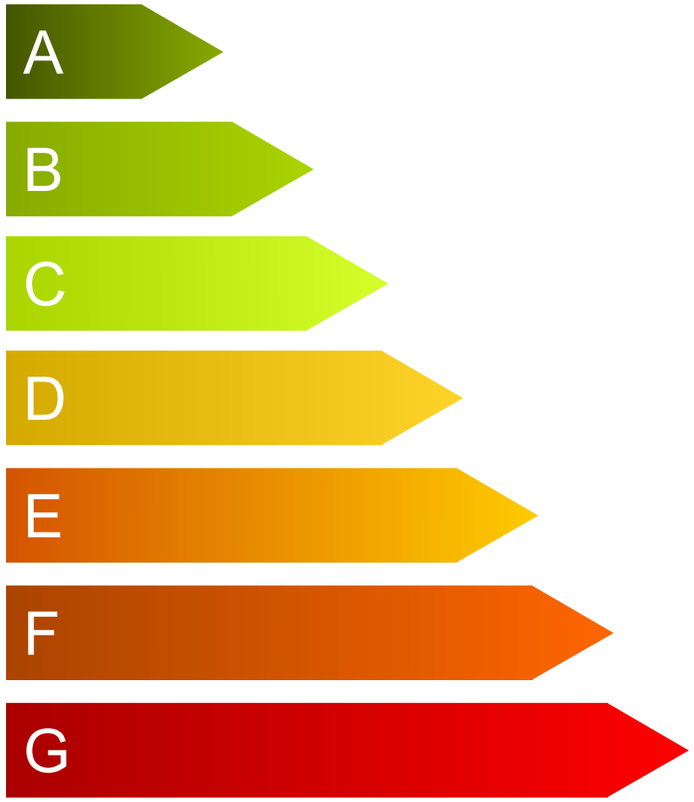
Un "biomattone" in materiale composito ideale per un clima come il nostro, in grado di mantenere in casa nei periodi di grande caldo una temperatura media di 26 gradi, senza necessariamente ricorrere alla climatizzazione. È uno dei risultati dello studio condotto da ENEA e Politecnico di Milano nell'ambito del progetto "Riqualificazione energetica degli edifici pubblici esistenti: direzione nZEB", finanziato dalla Ricerca di Sistema Elettrico del Ministero dello Sviluppo Economico.

Ricavato da una miscela di calce e canapulo, lo 'scarto' legnoso della canapa, il materiale abbina basso impatto ambientale, alte prestazioni energetiche, traspirabilità, ottime capacità isolanti, protezione dall'umidità e comfort. Oltre alla valutazione delle prestazioni ambientali del "calcecanapulo" mediante l'analisi del ciclo di vita (LCA), i ricercatori hanno effettuato dapprima prove in laboratorio in camera climatica a 23° e a 35° e successivamente anche una campagna di misure "in situ", in Sicilia e in Veneto, su edifici realizzati con le stesse tecnologie.

Costruire e riqualificare il patrimonio edilizio nazionale in un'ottica green potrebbe migliorare l'efficienza energetica nell'edilizia dei paesi a clima caldo-temperato, caratterizzati dall'elevato fabbisogno di energia nei periodi estivi, e far risparmiare il 50% di energia: in questo contesto gli edifici svolgono un ruolo chiave in quanto sono responsabili di buona parte del consumo energetico

nazionale. secondo studi ENEA, infatti, i consumi energetici delle abitazioni in Italia sono responsabili del 45% delle emissioni di CO_2.

"Lo studio ha evidenziato nel complesso un bilancio ambientale molto positivo per quanto riguarda l'impronta di carbonio: in pratica la parete in blocchi in calcecanapulo funziona come un sistema in grado di sottrarre CO_2 dall'atmosfera e tenerla bloccata per un tempo sufficientemente lungo", sottolinea Giovanni Dotelli del Politecnico di Milano. "Inoltre dai primi dati sperimentali emerge la buona performance termoigrometrica della parete che, indipendentemente dalle oscillazioni di umidità e temperatura esterne, si assesta su valori interni constanti, senza l'utilizzo di condizionatori e per l'intero periodo di misura effettuato nei mesi più caldi", aggiunge Patrizia Aversa, del Centro Ricerche ENEA di Brindisi.



Per definire e calibrare modelli matematici in grado di prevedere il comportamento termoigrometrico di edifici in condizioni climatiche reali, i risultati della sperimentazione sono stati poi confrontati con quelli ottenuti attraverso le simulazioni numeriche.

"Per il mercato italiano dell'edilizia, l'introduzione delle normative in ambito energetico ha rappresentato un forte stimolo a innovare materiali e componenti per garantire prestazioni più elevate in linea con i nuovi standard", spiega Vincenza Luprano, ricercatrice del Centro Ricerche ENEA di Brindisi. "La canapa, come materiale naturale, e i suoi sottoprodotti agricoli, hanno un ruolo importante per la nascita di nuove filiere, incentivate anche da leggi nazionali, per l'ampia disponibilità sul territorio e per il basso impatto del ciclo produttivo sull'ambiente, in un'ottica di economia circolare", aggiunge Luprano.

I risultati di questa ricerca sono stati recentemente presentati al convegno internazionale Resilient Built Environment for Sustainable Mediterranean Countries (SBE 2019) organizzato dal Politecnico di Milano in collaborazione con le organizzazioni internazionali International Council for Research and Innovation in Building and Construction (CIB), International Initiative for a Sustainable Built Environment (IISBE), United Nations Environment Programme (UNEnvironment) e International Federation of Consulting Engineers (FIDIC).

Per maggiori informazioni:

Vincenza Luprano – ENEA, Centro Ricerche di Brindisi - Laboratorio Materiali funzionali e Tecnologie per applicazioni sostenibili

Fonte: Enea

EVENTI

Conferenza SET-Plan 2019 - R&I nel settore energetico, per rafforzare la leadership industriale europea

13 novembre 2019, Helsinki, Finlandia

La 13a conferenza sul Piano strategico per le tecnologie energetiche (piano SET) si svolgerà dal 13 al 15 novembre 2019 a Helsinki, in Finlandia.

L'evento avrà inizio il pomeriggio del 13 novembre con visite tecniche. Il programma ufficiale inizia il 14 novembre alle 9.00 presso la Finlandia Hall e terminerà il 15 novembre alle 14.00.

Le sessioni affronteranno, tra l'altro, la decarbonizzazione dell'industria, l'accoppiamento settoriale e gli sviluppi nelle energie rinnovabili. Saranno inoltre discussi il finanziamento di tecnologie a basse emissioni di carbonio, piccoli reattori nucleari modulari e il ruolo delle donne nella transizione verso l'energia pulita.

Ulteriori informazioni sono disponibili nel sito SET-Plan 2019.

The future of science advice in Europe

13 novembre 2019, National Museum of Finland, Helsinki Finlandia

Il mondo di oggi deve affrontare un ambiente politico sempre più complesso e interconnesso. Ciò ha spinto l'UE e i governi nazionali a ripensare gli strumenti e le strutture esistenti per l'elaborazione delle politiche e a cercare modi innovativi di governare.

Questo ripensamento si estende anche alla consulenza scientifica. Molte sfide politiche chiave del ventunesimo secolo dipendono da campi scientifici in cui le prove sono complesse, incerte o in rapida evoluzione o in cui vi sono controversie sia all'interno che all'esterno della comunità scientifica.

L'attenzione si concentrerà sulla consulenza scientifica a livello sia UE che nazionale.

Ulteriori informazioni sono reperibili nel sito SAPEA.

Economia circolare: il ruolo delle imprese sociali

6 – 8 November 2019, Berriozar (Pamplona) - Spagna

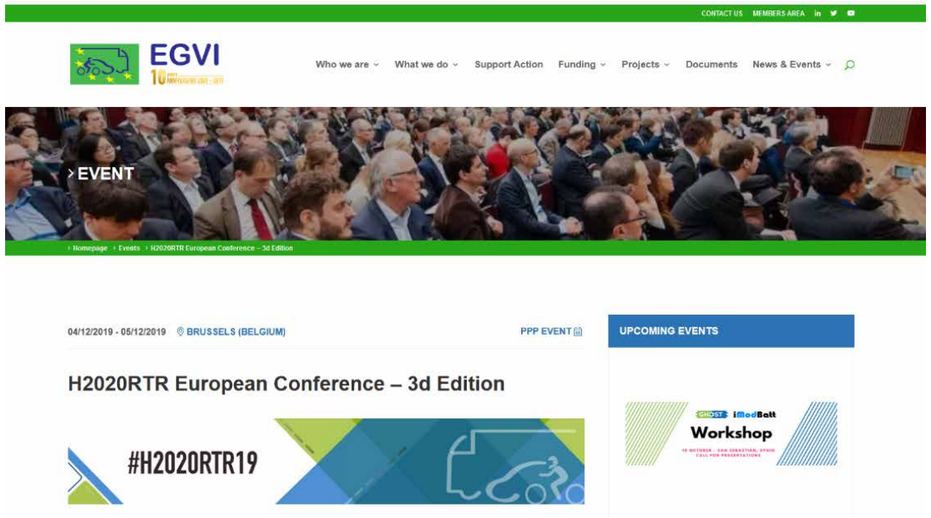
3rd International Conference on the Role of Social & Solidarity Enterprises in the Circular Economy

RREUSE, la rete europea di imprese sociali attive nel riutilizzo, riparazione e riciclaggio, in collaborazione rete spagnola di imprese sociali AERESS e Traperos de Emaús Navarra, organizza la terza edizione della conferenza annuale dedicata al ruolo delle imprese sociali nella promozione e nello sviluppo dell'economia circolare.

L'evento si concentrerà sulle strategie a supporto di prodotti più duraturi attraverso il riutilizzo e la riparazione che creano posti di lavoro inclusivi locali, forniscono prodotti e servizi ecologici e contribuiscono positivamente al benessere nella nostra società.

I punti salienti di quest'anno includeranno discussioni approfondite sul riutilizzo di prodotti tessili e dei rifiuti elettronici, nonché sugli sviluppi giuridici a livello dell'UE relativi all'economia circolare e alla misurazione dell'impatto sociale. Riunendo imprenditori sociali, responsabili politici locali, regionali e internazionali, comuni e rappresentanti del settore privato, l'evento offrirà, inoltre, opportunità di networking.

Ulteriori informazioni sono reperibili nel sito Rreuse



Conferenza europea H2020RTR – Terza Edizione

4 e 5 dicembre 2019, Albert Borschette Conference Center (CCAB) - Rue Froissart 36, 1040 Bruxelles

Dal 4 al 5 dicembre saranno presentati i risultati progetti di Orizzonte 2020 dedicati ai trasporti stradali ed alla logistica.

Come nelle precedenti edizioni, i progetti sono stati selezionati in vari settori: veicoli verdi, mobilità urbana, logistica, sistemi di trasporto intelligenti, sicurezza, trasporto stradale automatizzato. Lo scopo della conferenza è fornire una visione globale del settore dei trasporti e di come l'Unione Europea solleciti fattivamente lo sviluppo del settore a beneficio dell'ambiente, dell'economia e della società in generale.

L'evento è anche un'opportunità unica per fare rete e incontrare colleghi interessati nel settore della ricerca nel settore dei trasporti su strada.

Ulteriori informazioni sono reperibili nel sito EGVIA - H2020RTR19

www.sviluppumbria.it

BIT

Sede legale
Via Don Bosco, 11
06121 - Perugia (PG)
Tel. 075 56811
Fax. 075 5722454
email: svilpg@sviluppumbria.it
email certificata: sviluppumbria@legalmail.it

Unità locale di Terni
Strada delle Campore, 13
05100 Terni (TR)
Tel. 0744 58542
Fax. 0744 58544

Unità locale di Foligno
Via Andrea Vici 28
06034 Foligno (PG)
Tel: 0742 / 32681
Fax: 0742 / 32682