Spazio dati per la sicurezza e le forze dell'ordine

Data space for security and law enforcement

TOPIC ID: DIGITAL-2022-DATA-SEC-LAW-03-ENFORCE

Ente finanziatore: Commissione europea, Programma Digital Europe

Obiettivi ed impatto attesi: L'obiettivo è quello di implementare uno spazio comune europeo di dati sulla sicurezza per l'innovazione che consenta la ricerca, lo sviluppo, il test, l'addestramento e la convalida di algoritmi per sistemi basati sull'IA per la sicurezza (law enforcement) basati su vari tipi di dataset, compresi dataset operativi pseudonimizzati e anonimizzati, seguendo il principio della minimizzazione dei dati (Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 - GDPR e Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016 - LED). Occorre prestare particolare attenzione alla riduzione dei potenziali pregiudizi negli algoritmi da utilizzare per le forze dell'ordine.

La sovranità tecnologica degli Stati membri e dell'UE nel campo della lotta al crimine e al terrorismo nell'era digitale è un interesse pubblico fondamentale, oltre che una questione di sicurezza nazionale, e può essere rafforzata creando serie di dati di alta qualità e affidabili che consentano alle forze dell'ordine degli Stati membri di sviluppare e convalidare i propri strumenti digitali.

Uno spazio comune di dati dedicato alla sicurezza e all'applicazione della legge soddisferà entrambi i principi stabiliti nella "Strategia europea per i dati", secondo cui le azioni nell'ambito degli spazi di dati per le pubbliche amministrazioni si concentreranno anche sull'uso dei dati per migliorare l'applicazione della legge nell'UE in linea con il diritto dell'UE, e che i dati per il bene pubblico possono servire a garantire una lotta più efficiente contro la criminalità.

In particolare, questo spazio dati servirebbe gli interessi di tutte le parti interessate che si occupano di sicurezza pubblica o interna e, in particolare, delle autorità di contrasto degli Stati membri, delle autorità responsabili della sicurezza delle frontiere e delle agenzie europee competenti, come Europol, l'Agenzia europea della guardia di frontiera e costiera ed eu-LISA (in conformità con le basi giuridiche ad esse applicabili). In questo modo, l'autonomia strategica aperta dell'UE nel campo delle applicazioni dell'IA per l'applicazione della legge sarà rafforzata.

L'obiettivo dello spazio dati per la sicurezza e l'applicazione della legge è esclusivamente quello di facilitare l'innovazione, e non dovrebbe riguardare la condivisione dei dati a fini investigativi.

Ambito di applicazione:
Questa azione getterà le basi economiche, organizzative e tecniche di un'infrastruttura di dati federata. In particolare, si prevede che alla fine del progetto saranno disponibili un sistema e un modello di governance dei dati, pertanto il progetto comprenderà i seguenti compiti:

• sviluppare un'architettura di riferimento, definire gli standard dei dati e determinare i criteri per le certificazioni e la qualità del prodotto, affrontando al contempo le preoccupazioni etiche e rispettando i requisiti di protezione dei dati. Dovrebbe essere proposta la standardizzazione dei dati e il quadro potrebbe essere definito sulla base del progetto UMF (uniform message format) che definisce modelli di dati in una serie di aree, come i dati su persone, armi da fuoco e veicoli;
• generare, raccogliere, annotare e rendere interoperabili i dati adatti a testare, addestrare e convalidare gli algoritmi, che dovrebbero essere disponibili per l'addestramento, la convalida e il test degli strumenti che utilizzano le tecnologie di intelligenza artificiale e, quando possibile, proporzionati e dove previsto dalla legge, condivisibili per scopi di ricerca sulla sicurezza. Dovrebbe essere previsto un processo di monitoraggio per garantire la qualità dei dati e la convalida dei risultati. In particolare, si tratterà di verificare lo standard tecnico e il contenuto, ossia che i dati non siano distorti rispetto all'etnia, al genere, alla nazionalità o ad altre categorie sociali.
I progetti dovranno implementare meccanismi di fiducia (sicurezza e privacy by design), servizi di dati che garantiscano l'identità della fonte e del destinatario dei dati e che assicurino i diritti di accesso e di utilizzo dei dati. I progetti sono incoraggiati a studiare e analizzare alternative per la raccolta dei dati con la massima efficienza, al fine di fornire interoperabilità all'interno del dominio. Attraverso questo concetto di infrastruttura di dati federata, consentiamo agli stakeholder europei della sicurezza di sviluppare il loro potenziale in un ecosistema dinamico della sicurezza. I progetti nell'ambito di questa azione devono prestare particolare attenzione alle sfide relative ai diritti fondamentali, in particolare proponendo adeguati meccanismi di attenuazione dei pregiudizi e di non discriminazione e fornendo una migliore qualità dei dati. Dovranno inoltre dimostrare di rispettare rigorosamente il quadro giuridico dell'UE sul trattamento dei dati per finalità di polizia, come stabilito dalla direttiva 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016 e dal GDPR.
I progetti garantiranno un adeguato coordinamento con i progetti pertinenti finanziati nell'ambito dei programmi quadro di ricerca e, ove applicabile, con i programmi spaziali dell'UE che gestiscono i servizi di sicurezza (Copernicus, Galileo).

I progetti selezionati per l'implementazione di questo spazio dati dovranno prendere provvedimenti per diventare gradualmente pienamente conformi al quadro tecnico degli spazi dati europei. Dovranno inoltre coordinarsi e collaborare con altri progetti che partecipano alla realizzazione dello spazio dati e con il Centro di supporto per gli spazi dati, al fine di basarsi su standard comuni.

Risultati e risultati

La creazione di una piattaforma di dati comune, comprendente le componenti nazionali e un'infrastruttura di comunicazione, con set di dati affidabili per addestrare, testare e convalidare gli algoritmi, mira a creare una quantità di dati sufficiente per la ricerca, l'innovazione e lo sviluppo di tecnologie di intelligenza artificiale, con l'obiettivo di raccogliere e analizzare automaticamente un gran numero di informazioni di vario tipo (immagini, rapporti, video, ecc.). Lo spazio dati per

la sicurezza e l'applicazione della legge creerà un ecosistema di dati specifico per le esigenze delle parti interessate alla sicurezza e all'immigrazione, comprese le autorità nazionali, le agenzie dell'UE responsabili della sicurezza europea e i rappresentanti della giustizia. I rappresentanti del settore privato possono beneficiare di una sezione dedicata dello spazio dati per la sicurezza e l'applicazione della legge contenente insiemi di dati anonimi, a condizione che svolgano ricerche sulla sicurezza nell'ambito dei programmi quadro europei per la ricerca.

Uno spazio comune di dati per la sicurezza e l'applicazione della legge promuoverà in modo sostanziale lo sviluppo delle tecnologie di intelligenza artificiale, che costituiranno un contributo molto importante per combattere la criminalità, migliorare la sicurezza delle frontiere e facilitare la migrazione legale.

Inoltre, migliorerà l'autonomia strategica europea consentendo alle autorità di contrasto nazionali ed europee di sviluppare e convalidare i propri strumenti digitali in modo da (i) eliminare la minaccia di interferenze dannose da parte di Paesi terzi/parti; (ii) consentire la definizione di standard di qualità a livello UE e (iii) aumentare le capacità tecnologiche degli Stati membri LEA. Su questa base, i soggetti controllati dall'estero che partecipano all'azione devono svolgere solo compiti specifici e chiaramente definiti e non devono essere coinvolti nella progettazione dell'architettura tecnica o dei componenti di sicurezza del prodotto.

Criteri di eleggibilità: Per essere ammissibili, i richiedenti (beneficiari ed enti affiliati) devono: essere persone giuridiche (enti pubblici o privati) avere sede in uno dei Paesi ammissibili, ovvero: Stati membri dell'UE (compresi i Paesi e i territori d'oltremare (PTOM)) Paesi non UE: Paesi SEE elencati Paesi associati al Programma Europa Digitale o Paesi che hanno in corso negoziati per un accordo di associazione e in cui l'accordo entra in vigore prima della firma della sovvenzione.

I beneficiari e gli enti affiliati devono registrarsi nel Registro dei partecipanti - prima di presentare la proposta - e dovranno essere convalidati dal Servizio centrale di convalida (REA Validation). Per la convalida, sarà richiesto loro di caricare documenti che dimostrino lo status giuridico e l'origine. Si ricorda che questo bando è soggetto a restrizioni per motivi di sicurezza, pertanto i soggetti non devono essere controllati direttamente o indirettamente da un Paese non ammissibile. Tutti i soggetti devono compilare e presentare una dichiarazione sulla proprietà intellettuale e il controllo. Inoltre: la partecipazione a qualsiasi titolo (come beneficiario, entità affiliata, partner associato, subappaltatore o destinatario di sostegno finanziario a terzi) è limitata a soggetti provenienti da Paesi ammissibili le attività del progetto (incluso il lavoro in subappalto) devono svolgersi in Paesi ammissibili
l'Accordo di sovvenzione può prevedere restrizioni in materia di Diritto di proprietà intellettuale

Composizione del Consorzio
Le proposte devono essere presentate da almeno 2 autorità preposte all'applicazione della legge (beneficiari; non entità affiliate) da almeno 2 diversi Stati membri dell'UE

Durata del progetto: 36 mesi
Sono possibili estensioni, se debitamente giustificate e attraverso un emendamento del grant agreement.

Contributo finanziario: Il budget disponibile per la call è di 8 000 000 EUR
Bilancio del progetto (importo massimo della sovvenzione):
8 000 000 EUR per progetto
Tipo di azione
Sovvenzioni semplici - tasso di finanziamento del 50%.

Scadenza: 16 marzo 2023 - 17:00:00 CET
(ora di Bruxelles)

Ulteriori informazioni:
call-fiche_digital-2022-sec-law-03_en.pdf (europa.eu)