

KA210-ADU Small-Scale Partnership in Adult Education

Empowering Adults: Digital Safety and Fraud Prevention in the Age of Technology | digiSAFE



**Project Number:
2025-1-IT02-KA210-ADU-000359787**

Transnational Report

Acronimo progetto	digiSAFE
Titolo progetto	Empowering Adults: Digital Safety and Fraud Prevention in the Age of Technology
Numero progetto	2025-1-IT02-KA210-ADU-000359787



Durata	Data inizio: 01-09-2025 Data fine: 31-08-2027
Sottoprogramma	Small-Scale Partnership in Adult Education
Sito web	www.digisafeproject.eu
Data di consegna	
Stato	Versione 1.0
Autore	DC
Responsabile autore	DC

Sommario

1. Introduzione	3
2. Metodologia	5
3. Contesto nazionale	7
4. Buone pratiche	16
5. Analisi dei risultati del questionario	43
6. Analisi transnazionale	52
7. Principali risultati	55
8. Gap individuati e fabbisogni formativi	56
9. Raccomandazioni per lo sviluppo del curriculum	59
10. Conclusione	61
Bibliografia	62

1. Introduzione

Il progetto digiSAFE – “Empowering Adults: Digital Safety and Fraud Prevention in the Age of Technology” – è un Partenariato su piccola scala Erasmus+ nell’Educazione degli Adulti (KA210-ADU, Grant Agreement No. 2025-1-IT02-KA210-ADU-000359787), realizzato da un consorzio transnazionale composto da tre organizzazioni partner: Associazione Italiana Socio-Educatori per la Cooperazione – AISEC APS (Italia, coordinatore del progetto),

Asociación UNO (Spagna) e IKREON (Slovacchia). Il progetto si svolge dal 1° settembre 2025 al 31 agosto 2027.

La trasformazione digitale sta ridefinendo praticamente ogni aspetto della vita quotidiana in Europa: dal modo in cui i cittadini accedono ai servizi pubblici e gestiscono le proprie finanze personali, fino alle modalità di comunicazione e di fruizione delle informazioni. Sebbene la digitalizzazione offra opportunità indiscutibili, essa genera anche rischi nuovi e in rapida evoluzione, in particolare frodi online, criminalità informatica, disinformazione e violazioni dei dati. Gli adulti di età pari o superiore a 45 anni sono colpiti in modo sproporzionato da tali rischi, poiché spesso combinano un elevato livello di utilizzo degli strumenti digitali con una limitata consapevolezza in materia di cybersecurity e un accesso insufficiente a percorsi formativi mirati sulla sicurezza digitale.

Il progetto digiSAFE è stato ideato per rispondere direttamente a questo divario. I suoi principali output sono un Curriculum di educazione non formale (NFE) incentrato sulla sicurezza digitale e sulla prevenzione delle frodi, e un Toolkit pratico per la prevenzione delle frodi digitali, entrambi specificamente progettati per adulti di età pari o superiore a 45 anni. Per fondare tali output su evidenze concrete, la prima fase del progetto ha previsto una ricerca nazionale approfondita in tutti e tre i Paesi partner. Il presente Report transnazionale sintetizza e confronta i risultati emersi dalle ricerche nazionali e rappresenta il principale output dell'Attività A1 (fase di analisi dei bisogni), fornendo la base conoscitiva per lo sviluppo del curriculum e del toolkit.

Il presente documento mira a consolidare e analizzare i risultati delle ricerche nazionali condotte in Italia, Spagna e Slovacchia, e a confrontare le evidenze emerse nei tre Paesi al fine di individuare tendenze comuni, differenze significative e modelli transnazionali. Inoltre, il report intende identificare gli specifici gap di apprendimento e i fabbisogni formativi degli adulti di età pari o superiore a 45 anni in relazione alla sicurezza digitale, alla prevenzione delle frodi online e alla consapevolezza in materia di cybersecurity, fornendo al contempo raccomandazioni basate su evidenze per orientare la progettazione del Curriculum NFE e del Toolkit per la prevenzione delle frodi digitali di digiSAFE.

Il gruppo target principale considerato nel presente report è costituito da adulti di età pari o superiore a 45 anni, con particolare attenzione alle persone con livelli bassi o medi di competenze digitali, maggiormente vulnerabili ai rischi online. Questo gruppo è sempre più attivo negli ambienti digitali, ma spesso non dispone delle competenze, della fiducia e della consapevolezza necessarie per muoversi in tali ambienti in modo sicuro e autonomo.

In questo contesto, il report si allinea alle priorità chiave di Erasmus+ e, più in generale, dell'Unione europea, in particolare quelle relative alla trasformazione digitale,

all'inclusione sociale e all'apprendimento permanente, sostenendo lo sviluppo di approcci educativi inclusivi e accessibili per gli adulti in apprendimento.

2. Metodologia

La ricerca alla base del presente Report transnazionale è stata condotta simultaneamente nei tre Paesi partner durante la prima fase del progetto digiSAFE (fine 2025 – inizio 2026). È stata adottata una metodologia condivisa e armonizzata, al fine di garantire la comparabilità dei dati e dei risultati nei diversi contesti nazionali. Tale metodologia si è basata su un quadro di ricerca comune sviluppato a livello di progetto, con il partner responsabile dell'Attività A1 (Asociación UNO) incaricato di predisporre le linee guida di ricerca, applicate in modo coerente da tutti i partner nei tre Paesi. La ricerca ha combinato due approcci complementari: la ricerca documentale e un questionario quantitativo di autovalutazione.

2.1 Ricerca documentale

Ciascun partner nazionale ha condotto un'ampia analisi di fonti secondarie, tra cui dati statistici ufficiali, documenti di policy nazionali, strumenti legislativi, report della Commissione europea e letteratura accademica e grigia, selezionati sulla base della loro pertinenza e affidabilità in conformità con le linee guida di ricerca. Oltre a mappare il contesto nazionale a livello macro, i partner hanno individuato anche una serie di buone pratiche nazionali utili a orientare lo sviluppo degli output di progetto. La ricerca documentale mirava a fornire una panoramica completa di ciascun Paese, includendo lo stato attuale dell'alfabetizzazione digitale tra gli adulti di età pari o superiore a 45 anni, i quadri normativi esistenti in materia di protezione dei dati e cybersecurity, nonché i programmi o le iniziative attive a supporto dell'educazione digitale degli adulti e della sicurezza online. Le fonti utilizzate sono documentate nei report nazionali e consolidate nella sezione bibliografica del presente documento.

2.2 Questionario di autovalutazione

Un questionario quantitativo standardizzato di autovalutazione è stato somministrato ad adulti di età pari o superiore a 45 anni in ciascun Paese partner. Lo stesso questionario è stato utilizzato in tutti i Paesi per garantire la comparabilità dei risultati. Lo strumento ha utilizzato una combinazione di scale a 5 punti e domande a scelta multipla per valutare le abitudini digitali quotidiane dei partecipanti, la fiducia percepita negli ambienti online, specifiche competenze di sicurezza digitale, la consapevolezza rispetto a diversi tipi di minacce online, l'esperienza diretta di frodi digitali e i fabbisogni formativi percepiti. Lo scopo principale del questionario era individuare competenze digitali, livelli di

consapevolezza del rischio e bisogni formativi tra gli adulti di età pari o superiore a 45 anni.

Il questionario è stato distribuito online attraverso le reti di ciascun partner, utilizzando canali di comunicazione adattati per raggiungere il gruppo target. La raccolta dei dati è avvenuta su base volontaria e completamente anonima, in conformità con il Regolamento generale sulla protezione dei dati (GDPR). È stato stabilito un obiettivo minimo di almeno 50 risposte valide per Paese, come definito nella proposta progettuale, al fine di garantire l'affidabilità dei dati e la comparabilità dei risultati nei tre contesti nazionali.

2.3 Partecipanti

I dati del questionario sono stati raccolti nei tre Paesi partner, con un campione comparabile per ciascun Paese, assicurando una base equilibrata per l'analisi transnazionale. In tutti e tre i campioni, le donne hanno costituito la maggioranza dei rispondenti. La distribuzione per età si è concentrata prevalentemente nelle fasce 45–54 e 55–64 anni, con una rappresentanza più contenuta di persone di età pari o superiore a 65 anni. I partecipanti provenivano da contesti urbani, semi-urbani e rurali, e presentavano background educativi e occupazionali diversificati, comprendendo lavoratori dipendenti, lavoratori autonomi e pensionati. Nel complesso, il campione riflette un gruppo eterogeneo di adulti di età pari o superiore a 45 anni, rafforzando la rilevanza e la rappresentatività dei risultati.

2.4 Analisi dei dati

I dataset nazionali sono stati analizzati indipendentemente da ciascun partner attraverso metodi statistici descrittivi. L'analisi si è concentrata su frequenze, distribuzioni delle risposte e identificazione di pattern ricorrenti all'interno di ciascun campione nazionale. In particolare, i partner hanno esaminato variabili chiave quali i livelli di utilizzo del digitale, la fiducia percepita, la consapevolezza dei rischi online, le esperienze di frode digitale e i fabbisogni formativi espressi.

Per garantire coerenza, è stato seguito un approccio analitico comune nei tre Paesi, consentendo un confronto strutturato dei risultati. Le evidenze sono state poi analizzate a livello transnazionale attraverso confronti tra Paesi, evidenziando sia somiglianze sia differenze nei comportamenti, nelle percezioni e nelle vulnerabilità dei partecipanti. Particolare attenzione è stata dedicata all'individuazione di pattern rilevanti per la progettazione di interventi educativi, includendo sia aree di bisogno condivise sia sfide specifiche dei singoli Paesi.

Il presente report sintetizza tali analisi e trae conclusioni transnazionali sulla base delle evidenze combinate, fornendo una base coerente per lo sviluppo del curriculum e del toolkit digiSAFE.

3. Contesto nazionale

Questa sezione fornisce una panoramica comparativa del panorama digitale per gli adulti di età pari o superiore a 45 anni in ciascun Paese partner. Per ogni Paese, l'analisi affronta lo stato attuale dell'alfabetizzazione digitale, le principali sfide affrontate dal gruppo target, le normative e le politiche nazionali rilevanti, nonché i programmi e le iniziative esistenti.

3.1 Italia

Alfabetizzazione digitale e principali sfide

L'Italia presenta un paradosso significativo: sebbene siano stati compiuti progressi importanti nelle infrastrutture digitali e nella diffusione dei servizi pubblici digitali, persistono lacune strutturali nelle competenze digitali dei cittadini, in particolare tra gli adulti più anziani. Secondo il Digital Decade Country Report 2025 della Commissione europea, l'Italia ha registrato progressi nella connettività e nell'e-government; tuttavia, permangono criticità rilevanti nella capacità dei cittadini di utilizzare le tecnologie digitali in modo efficace e sicuro.

I dati ISTAT confermano questa doppia tendenza. Nel 2024, l'86,2% delle famiglie italiane disponeva di accesso a Internet; tuttavia, tale percentuale scende al 60,6% tra le famiglie composte esclusivamente da persone anziane. L'uso di Internet varia significativamente in base all'età: mentre l'81,9% della popolazione totale di età pari o superiore a 6 anni ha utilizzato Internet nei tre mesi precedenti, solo il 68,1% delle persone di età compresa tra 65 e 74 anni lo ha fatto. Le disparità regionali aggravano ulteriormente questo quadro, con le regioni meridionali in ritardo rispetto al Centro e al Nord Italia sia in termini di accesso sia di utilizzo.

I livelli di competenze digitali tra gli adulti più anziani rappresentano una criticità rilevante. Nel 2023, solo il 45,9% delle persone di età compresa tra 16 e 74 anni che utilizzavano Internet possedeva almeno competenze digitali di base. La percentuale scende al 48,7% tra le persone di età compresa tra 45 e 54 anni, al 38,5% tra quelle di età compresa tra 55 e 64 anni, e ad appena il 19,3% tra le persone di età compresa tra 65 e 74 anni. Di conseguenza, molte persone appartenenti al gruppo 45+ incontrano difficoltà nell'accesso autonomo ai servizi digitali, nella valutazione delle informazioni online e nella protezione dai rischi digitali.

Le frodi online e la criminalità informatica rappresentano una preoccupazione crescente e concreta. L'ISTAT stima che circa 1,7 milioni di persone – pari al 3,3% degli utenti Internet

– abbiano subito frodi o truffe online nei 12 mesi precedenti l'indagine 2022–2023. I casi di frodi finanziarie tramite online banking sono aumentati del 74% rispetto al periodo 2015–2016. Nel 2024, la piattaforma del Commissariato di PS Online ha registrato circa 3 milioni di visite, oltre 82.000 segnalazioni e circa 23.000 richieste di assistenza relative a phishing e truffe online.

Questi dati indicano che, per gli adulti di età pari o superiore a 45 anni, il problema non riguarda più soltanto l'accesso, ma la qualità e l'autonomia nell'uso del digitale.

Normative e politiche nazionali

L'Italia ha sviluppato un quadro normativo e di policy articolato in materia di sicurezza digitale. La protezione dei dati è disciplinata dal GDPR (UE 2016/679), attuato a livello nazionale attraverso il D.lgs. n. 196/2003, come modificato, con la supervisione del Garante per la protezione dei dati personali. Il Codice dell'Amministrazione Digitale stabilisce i diritti digitali dei cittadini nelle interazioni con le pubbliche amministrazioni, mentre l'Agenzia per l'Italia Digitale (AgID) promuove la cittadinanza digitale e strumenti di segnalazione delle violazioni. La cybersecurity è coordinata attraverso la Strategia nazionale di cybersicurezza 2022–2026, gestita dall'Agenzia per la Cybersicurezza Nazionale (ACN). L'Italia ha inoltre recepito la Direttiva NIS2 tramite il D.lgs. n. 138/2024 e ha attuato il Digital Operational Resilience Act (DORA) nel settore finanziario.

Programmi e iniziative esistenti

Accanto alle misure normative, l'Italia ha sviluppato un'ampia gamma di programmi e iniziative a supporto dell'inclusione e dell'educazione digitale degli adulti. Un ruolo centrale è svolto da Repubblica Digitale, iniziativa nazionale guidata dal Dipartimento per la Trasformazione Digitale, che coordina la Strategia nazionale per le competenze digitali e promuove la collaborazione tra istituzioni pubbliche, attori del settore privato e organizzazioni della società civile. All'interno di questo quadro, la Rete dei servizi di facilitazione digitale mira a raggiungere due milioni di cittadini entro il 2026 attraverso 4.000 punti fisici di accesso (Punti Digitale Facile), fornendo supporto nell'accesso ai servizi digitali e nel miglioramento della sicurezza online.

Ulteriori iniziative includono il Servizio Civile Digitale e programmi di finanziamento mirati come Dritti al Punto, che supportano attività formative incentrate sulla consapevolezza in materia di cybersecurity, sull'uso critico delle informazioni e sull'accesso sicuro ai servizi pubblici digitali. Parallelamente, politiche del mercato del lavoro come il Programma GOL (Garanzia di Occupabilità dei Lavoratori) mirano a coinvolgere tre milioni di beneficiari, con una forte enfasi sullo sviluppo delle competenze digitali.

L'educazione degli adulti è inoltre supportata dai Centri Provinciali per l'Istruzione degli Adulti (CPIA), che rappresentano presidi territoriali fondamentali per l'apprendimento

permanente. Tali centri offrono opportunità di istruzione formale e non formale e svolgono un ruolo cruciale nel raggiungere gruppi vulnerabili, compresi gli adulti più anziani con bassi livelli di istruzione o di competenze digitali. La loro funzione è inserita in politiche più ampie di promozione dell'apprendimento permanente e dello sviluppo delle competenze nella popolazione.

Infine, una vasta gamma di attori istituzionali e settoriali contribuisce alla sensibilizzazione e alla promozione di comportamenti sicuri online. L'Agenzia per l'Italia Digitale (AgID) e l'Agenzia per la Cybersicurezza Nazionale (ACN) sostengono la diffusione delle competenze digitali e di cybersecurity, mentre la Polizia Postale fornisce servizi di prevenzione e assistenza. Il Garante per la protezione dei dati personali promuove la consapevolezza dei diritti in materia di privacy, e istituzioni finanziarie come la Banca d'Italia, insieme a iniziative come I Navigati, contribuiscono a educare i cittadini rispetto alle frodi online e ai rischi di cybersecurity finanziaria.

Nel complesso, il contesto italiano evidenzia un divario significativo tra la rapida digitalizzazione dei servizi e l'effettiva capacità degli adulti – in particolare quelli di età pari o superiore a 45 anni – di utilizzare tali strumenti in modo sicuro ed efficace. Sebbene il quadro normativo e istituzionale sia ben sviluppato, la sfida principale resta garantire che tutti i cittadini, soprattutto gli adulti più anziani, acquisiscano le competenze necessarie per partecipare pienamente e in sicurezza alla società digitale.

3.2 Spagna

Alfabetizzazione digitale e principali sfide

La Spagna ha vissuto una rapida trasformazione digitale nell'ultimo decennio, ridefinendo le modalità con cui i cittadini interagiscono con i servizi pubblici, le istituzioni finanziarie, i sistemi sanitari e le piattaforme di comunicazione. La diffusione dell'online banking, delle piattaforme di e-government, dei servizi sanitari digitali e dei social media ha aumentato in modo significativo la connettività digitale della popolazione, migliorando sia l'accessibilità sia l'efficienza amministrativa.

Tuttavia, nonostante questo progresso complessivo, in Spagna persiste un divario digitale significativo. Tale divario è fortemente associato all'età, al livello di istruzione e alle condizioni socio-economiche. Gli adulti di età pari o superiore a 45 anni, e in particolare quelli sopra i 55 anni, tendono a riportare livelli più bassi di fiducia digitale e una familiarità più limitata con le pratiche di sicurezza digitale. Molte persone appartenenti a questa fascia d'età non hanno acquisito competenze digitali durante il percorso di istruzione formale o la carriera professionale, il che rende l'adattamento ad ambienti digitali in rapida evoluzione più complesso e spesso più lento.

Questo divario generazionale si riflette inoltre nei modelli di utilizzo digitale e nell'esposizione ai rischi online. Le frodi online e la criminalità informatica rappresentano

una preoccupazione sempre più rilevante nel contesto spagnolo. Le minacce comuni includono email di phishing, SMS fraudolenti, furto d'identità, falsi servizi online e truffe finanziarie. Gli adulti di età pari o superiore a 45 anni risultano particolarmente vulnerabili, poiché spesso combinano un uso regolare dei servizi digitali – come online banking, applicazioni di messaggistica ed e-commerce – con una minore consapevolezza dei rischi di cybersecurity e delle pratiche preventive. Inoltre, la crescente sofisticazione delle tecniche di social engineering, compreso l'uso di meccanismi fraudolenti supportati dall'intelligenza artificiale, accentua ulteriormente tali vulnerabilità e rende più difficile l'individuazione delle truffe per gli utenti meno esperti.

A livello istituzionale, la Spagna ha sviluppato una serie di strategie nazionali in materia di trasformazione digitale, cybersecurity e inclusione digitale. Tali quadri di policy mirano a rafforzare le competenze digitali dei cittadini, migliorare i meccanismi di protezione dei dati e promuovere un coinvolgimento più sicuro e responsabile con le tecnologie digitali. Accanto a queste strategie nazionali, istituzioni pubbliche, governi regionali e organizzazioni della società civile hanno attuato vari programmi di formazione e iniziative di sensibilizzazione rivolte all'alfabetizzazione digitale degli adulti e alla sicurezza online.

Tuttavia, le iniziative esistenti restano frammentate e distribuite in modo non uniforme tra le regioni. Inoltre, molti programmi tendono a privilegiare l'acquisizione di competenze digitali di base, dedicando minore attenzione alla sicurezza digitale, alla prevenzione delle frodi e alla consapevolezza critica dei rischi online. Questo divario evidenzia la necessità di interventi educativi più strutturati, accessibili e mirati, specificamente progettati per rafforzare la resilienza digitale degli adulti di età pari o superiore a 45 anni.

In questo contesto, il progetto digiSAFE risponde direttamente a tali sfide, combinando ricerca, educazione non formale e strumenti pratici finalizzati a rafforzare le competenze di sicurezza online e a sostenere una partecipazione più sicura alla società digitale.

Normative e politiche nazionali

La risposta della Spagna alla sicurezza digitale e alla prevenzione delle frodi si inserisce in un sistema di governance multilivello che combina la legislazione nazionale con più ampi quadri strategici di policy, finalizzati a promuovere la trasformazione e l'inclusione digitale. Negli ultimi anni, il governo spagnolo ha progressivamente affiancato agli approcci regolatori strategie nazionali complessive volte a ridurre le disuguaglianze digitali e a rafforzare le capacità digitali dei cittadini, in particolare tra i gruppi vulnerabili come gli adulti di età pari o superiore a 45 anni.

Un pilastro fondamentale di questo approccio è la strategia nazionale Digital Spain 2026, che rappresenta la principale roadmap per la trasformazione digitale del Paese. Tale strategia promuove la crescita economica, la coesione sociale e l'inclusione territoriale attraverso la digitalizzazione, affrontando esplicitamente i divari digitali legati all'età, al

genere e alla geografia. Tra le sue priorità figurano l'ampliamento delle infrastrutture digitali, la promozione delle tecnologie emergenti e il rafforzamento delle competenze digitali dei cittadini, come strumento per garantire che nessun gruppo sia lasciato indietro nella transizione digitale.

All'interno di questo quadro, il National Digital Skills Plan (Plan Nacional de Competencias Digitales) svolge un ruolo centrale nella promozione dell'inclusione digitale. Esso mira a dotare cittadini, lavoratori e pubbliche amministrazioni delle competenze necessarie per operare in una società sempre più digitale. Il piano affronta specificamente i gap strutturali nell'alfabetizzazione digitale, che interessano ancora una quota significativa della popolazione, in particolare gli adulti più anziani e altri gruppi vulnerabili. Le sue misure includono programmi formativi su larga scala, iniziative di riqualificazione e azioni per ridurre le disuguaglianze di genere e territoriali nell'accesso alle competenze digitali. Inoltre, programmi come l'iniziativa UNICO Broadband mirano a estendere l'accesso a Internet ad alta velocità nelle aree rurali e meno servite, riducendo le disparità territoriali e garantendo un accesso più equo ai servizi digitali in tutto il Paese. Queste iniziative evidenziano l'importanza di affrontare non solo le competenze individuali, ma anche le condizioni strutturali di accesso, come la connettività.

Tali iniziative strategiche sono inserite nel più ampio Piano di ripresa, trasformazione e resilienza, che integra la digitalizzazione come pilastro centrale dello sviluppo economico e sociale. Attraverso investimenti e riforme coordinati, la Spagna intende non solo modernizzare la propria economia, ma anche garantire un accesso inclusivo alle tecnologie e ai servizi digitali per l'intera popolazione.

Accanto a questi quadri strategici, la Spagna ha sviluppato una solida struttura giuridica in materia di sicurezza digitale. Il quadro normativo di base è stabilito dalla Legge organica 3/2018 sulla protezione dei dati personali e la garanzia dei diritti digitali (LOPDGDD), che recepisce il Regolamento generale sulla protezione dei dati (GDPR) nell'ordinamento spagnolo. Tali strumenti regolano il trattamento e la protezione dei dati personali, riconoscendo al contempo i diritti digitali come diritti fondamentali. Tuttavia, la consapevolezza e l'effettiva comprensione di tali diritti restano disomogenee, in particolare tra gli utenti più anziani che fanno sempre maggiore affidamento sui servizi digitali.

Nel campo della cybersecurity, il Real Decreto-Ley 12/2018 e il Real Decreto 43/2021 recepiscono i requisiti europei di cybersecurity nel diritto nazionale, rafforzando la capacità istituzionale della Spagna nella gestione dei rischi digitali. Analogamente, le frodi online sono affrontate attraverso il Codice penale spagnolo (Legge organica 10/1995), che criminalizza un'ampia gamma di reati informatici, compresi phishing e furto d'identità. Tuttavia, la crescente sofisticazione delle frodi digitali evidenzia la necessità di misure complementari incentrate sulla prevenzione e sulla consapevolezza degli utenti.

La protezione dei consumatori e la regolazione delle piattaforme rafforzano ulteriormente questo quadro attraverso strumenti quali il Real Decreto Legislativo 1/2007 e la Legge 34/2002 (LSSI), allineati agli sviluppi europei come il Digital Services Act. Tali regolamenti rafforzano la trasparenza, la responsabilità e la protezione degli utenti negli ambienti digitali.

Infine, la rapida espansione dei servizi pubblici digitali è stata accompagnata da iniziative come il Piano di digitalizzazione delle pubbliche amministrazioni, che mira a migliorare l'accessibilità, l'efficienza e l'esperienza utente nelle interazioni con le istituzioni pubbliche. Tuttavia, sebbene tali sviluppi rappresentino un progresso significativo, essi possono anche rafforzare involontariamente le disuguaglianze esistenti se non accompagnati da adeguate misure di alfabetizzazione digitale. In particolare, gli adulti più anziani con competenze digitali limitate possono incontrare ulteriori barriere nell'accesso a servizi essenziali sempre più disponibili prevalentemente online.

Nel complesso, la Spagna combina un quadro giuridico completo con un insieme sempre più robusto di strategie nazionali orientate alla trasformazione e all'inclusione digitale. Tuttavia, permane un divario significativo tra l'esistenza di tali politiche e il loro impatto effettivo sulle pratiche digitali quotidiane dei cittadini. In particolare, gli adulti di età pari o superiore a 45 anni spesso non dispongono delle conoscenze e delle competenze necessarie per beneficiare pienamente di tali misure. Questo gap evidenzia l'importanza di iniziative educative e di sensibilizzazione come digiSAFE, che traducono i quadri normativi e strategici in conoscenze pratiche e competenze quotidiane.

Programmi e iniziative esistenti

In Spagna, diverse iniziative affrontano l'inclusione digitale degli adulti più anziani, in particolare nell'ambito di programmi nazionali finalizzati a migliorare le competenze digitali della popolazione. Iniziative pubbliche promosse dal governo spagnolo, così come programmi locali attuati da municipalità, ONG e centri di educazione degli adulti, offrono percorsi di alfabetizzazione digitale di base per i cittadini più anziani, concentrandosi sull'uso degli smartphone, sulla navigazione in Internet e sull'accesso ai servizi pubblici digitali. Ad esempio, programmi quali laboratori di formazione digitale offerti presso biblioteche pubbliche e centri di comunità forniscono supporto pratico agli adulti più anziani nell'apprendimento dell'uso delle applicazioni mobili e nell'accesso alle piattaforme di e-government. Inoltre, le iniziative promosse nell'ambito del National Digital Skills Plan includono corsi di base finalizzati a migliorare l'autonomia digitale dei cittadini più anziani. Analogamente, le organizzazioni non governative organizzano spesso sessioni introduttive incentrate su attività digitali quotidiane, come l'online banking o la prenotazione di visite mediche, rafforzando il coinvolgimento pratico con gli strumenti digitali.

Tuttavia, tali iniziative tendono a privilegiare l'inclusione digitale generale piuttosto che la sicurezza digitale. Le attività formative si concentrano spesso su come utilizzare gli strumenti digitali, dedicando un'attenzione limitata ai rischi associati agli ambienti online, come frodi, phishing o truffe emergenti basate sull'intelligenza artificiale. In Spagna, un ruolo chiave è svolto dall'Istituto Nacional de Ciberseguridad (INCIBE), che rappresenta un punto di riferimento nazionale **per la cybersecurity. Questa istituzione pubblica fornisce campagne di sensibilizzazione, risorse educative e servizi di supporto** finalizzati alla prevenzione delle minacce informatiche e all'assistenza dei cittadini nella risposta ai rischi digitali. Tuttavia, nonostante il ruolo importante svolto da INCIBE, tali iniziative sono generalmente rivolte alla popolazione nel suo complesso e non mirano specificamente agli adulti di età pari o superiore a 45 anni attraverso percorsi di apprendimento strutturati e continuativi.

Nel complesso, sebbene la Spagna abbia sviluppato un quadro nazionale completo per l'inclusione digitale e la cybersecurity, come illustrato nella sezione 1.2, la sua attuazione pratica resta disomogenea. Le differenze nell'accesso alla formazione, nei livelli di alfabetizzazione digitale e la mancanza di programmi mirati per specifiche fasce d'età limitano l'efficacia di tali politiche. Questo divario tra quadri normativi e risultati pratici evidenzia la necessità di approcci più inclusivi e personalizzati. Di conseguenza, permane un gap significativo tra gli sforzi di inclusione digitale e lo sviluppo di competenze pratiche per la prevenzione delle frodi tra gli adulti più anziani. Ciò sottolinea la necessità di approcci educativi mirati che combinino alfabetizzazione digitale e formazione pratica nel riconoscimento e nella risposta alle minacce online. In questo contesto, digiSAFE affronta direttamente tale divario offrendo un modello di apprendimento personalizzato e basato su scenari, specificamente progettato per adulti di età pari o superiore a 45 anni.

3.3 Slovacchia

Alfabetizzazione digitale e principali sfide

La Repubblica Slovacca affronta una sfida specifica: mentre le infrastrutture digitali e la connettività sono migliorate considerevolmente, il capitale umano necessario per muoversi in sicurezza negli ambienti digitali resta significativamente sottosviluppato, in particolare tra la popolazione più anziana. Secondo il Digital Decade Country Report 2024 della Commissione europea, la Slovacchia ha raggiunto una copertura delle competenze digitali di base pari al 51,3% – un lieve calo rispetto alle rilevazioni precedenti e un valore inferiore alla media UE del 55,6%.

Le disparità sono particolarmente gravi tra le fasce demografiche più anziane. Tra i senior slovacchi di età compresa tra 65 e 74 anni, solo l'11% possiede competenze digitali di base o superiori – meno della metà della media UE del 24% per la stessa fascia d'età. Inoltre, il 27% dei senior in questa fascia d'età non ha mai utilizzato Internet e solo il 39% ha utilizzato un computer nei dodici mesi precedenti. Per gli adulti di età compresa tra 45 e

64 anni, le competenze digitali sono spesso limitate ad operazioni di routine, senza la profondità critica e gli strumenti analitici necessari per affrontare minacce di cybersecurity in continua evoluzione.

La Slovacchia presenta tipologie di frode specifiche e gravi. Una tecnica molto diffusa prevede che i truffatori si fingano agenti di polizia, dipendenti della sicurezza bancaria o rappresentanti della Banca nazionale slovacca, sfruttando tecnologie di spoofing del numero telefonico per manipolare l'identificativo chiamante e utilizzando tattiche basate sulla paura per ottenere credenziali bancarie o indurre le vittime a trasferire denaro su conti fraudolenti. Inoltre, lo spazio digitale slovacco è fortemente esposto a campagne di disinformazione e disinformazione collegate al posizionamento geopolitico e alla polarizzazione politica interna.

Normative e politiche nazionali

Per proteggere i diritti digitali dei cittadini e contrastare le minacce informatiche, la Repubblica Slovacca ha sviluppato un quadro normativo strettamente allineato alle direttive dell'Unione europea. La base della protezione dei dati in Slovacchia è costituita dal Regolamento generale sulla protezione dei dati (GDPR), integrato nel diritto nazionale attraverso la Legge n. 18/2018 Coll. sulla protezione dei dati personali. In vigore da maggio 2018, tale normativa stabilisce linee guida chiare per il trattamento lecito dei dati personali, imponendo trasparenza, minimizzazione dei dati e limitazione delle finalità. Essa garantisce ai cittadini il diritto di accesso, rettifica e cancellazione dei propri dati, nonché la protezione contro decisioni automatizzate non autorizzate.

L'Ufficio per la protezione dei dati personali della Repubblica Slovacca (ÚOOÚ) supervisiona tali normative. In qualità di autorità di controllo indipendente, l'ÚOOÚ assicura il rispetto della disciplina nei settori pubblico e privato. Fornisce inoltre orientamenti vincolanti su questioni complesse di protezione dei dati, come la conduzione delle valutazioni d'impatto sulla protezione dei dati. In particolare, la legge slovacca disciplina in modo rigoroso l'utilizzo del numero di nascita nazionale (rodné číslo). La divulgazione pubblica di tale identificativo è vietata, salvo autorizzazione esplicita dell'interessato o previsione di legge specifica, rappresentando una misura essenziale per prevenire il furto d'identità.

In materia di cybersecurity, il principale strumento legislativo è la Legge n. 69/2018 Coll. sulla cybersicurezza, che originariamente ha recepito la Direttiva europea NIS. Tale legge ha stabilito la base della governance nazionale della cybersecurity, definendo gli obblighi giuridici degli operatori di servizi essenziali, i requisiti di segnalazione degli incidenti e le procedure di audit. Per rispondere all'evoluzione delle minacce, la Slovacchia ha aggiornato tale quadro per soddisfare i requisiti avanzati della Direttiva NIS2 (Direttiva (UE) 2022/2555). Con la Legge n. 366/2024 Coll., in vigore dal 1° gennaio 2025, la Slovacchia ha ampliato significativamente l'ambito di applicazione della regolazione in

materia di cybersecurity. La modifica introduce un meccanismo preciso per l'identificazione dei soggetti obbligati, includendo un numero più ampio di settori critici e imponendo misure di sicurezza più stringenti.

L'Autorità nazionale per la sicurezza (NBÚ) coordina questi interventi legislativi attraverso la Strategia nazionale di cybersicurezza 2021–2025. La strategia delinea priorità quali garantire la preparazione dello Stato, individuare la criminalità informatica, costruire un settore privato resiliente, integrare la cybersecurity nella pubblica amministrazione e promuovere le competenze digitali sia dei professionisti sia della popolazione generale. Questa enfasi sull'educazione pubblica evidenzia che le difese tecniche devono essere direttamente supportate dalla consapevolezza dei cittadini e dalla resilienza digitale individuale.

Programmi e iniziative esistenti

L'attuazione della strategia digitale slovacca si basa sulla collaborazione tra istituzioni pubbliche, ONG, forze dell'ordine e settore privato, al fine di colmare il divario digitale e rafforzare la sicurezza online degli adulti.

Il Ministero degli Investimenti, dello Sviluppo Regionale e dell'Informatizzazione (MIRRI) guida tali sforzi, gestendo componenti chiave del Piano nazionale di ripresa e resilienza. La sua iniziativa principale, "Digitálni seniori" (Senior digitali), mira a fornire formazione sulle competenze digitali a oltre 100.000 senior (di età pari o superiore a 65 anni) e persone svantaggiate entro il 2026. Il programma eroga sessioni formative localizzate e fornisce ai partecipanti che completano il percorso un tablet configurato e un pacchetto dati mobili, affrontando direttamente sia le barriere educative sia quelle legate all'accesso ai dispositivi.

Nel campo della sicurezza, l'Autorità nazionale per la sicurezza (NBÚ) e il Centro nazionale per la sicurezza informatica (SK-CERT) gestiscono la cybersecurity tecnica e la risposta nazionale agli incidenti, contribuendo al contempo alle campagne di sensibilizzazione pubblica. Inoltre, le Forze di Polizia della Repubblica Slovacca contrastano attivamente le frodi digitali e la disinformazione. Attraverso il proprio canale pubblico di comunicazione dedicato, "Hoaxy a podvody – Polícia SR" (Bufale e truffe – Polizia SR), la polizia monitora lo spazio digitale, smentisce bufale virali, segnala ai cittadini truffe finanziarie emergenti ed educa il pubblico all'identificazione delle comunicazioni fraudolente.

La collaborazione intersettoriale è formalizzata attraverso la Digital Coalition (Digitálna koalícia), una partnership che riunisce governo, industria IT, mondo accademico e società civile. Questa piattaforma conduce valutazioni nazionali, come l'IT Fitness Test, per misurare le competenze digitali della popolazione e individuare i gruppi demografici che necessitano di interventi educativi. La coalizione collabora inoltre con il MIRRI per progettare percorsi formativi su misura per senior e dipendenti pubblici più anziani.

Le ONG e il settore privato forniscono un supporto specialistico essenziale. Iniziative indipendenti come Konšpirátori.sk mettono a disposizione del pubblico banche dati trasparenti di siti web noti per diffondere disinformazione o contenuti fraudolenti, fungendo da strumenti pratici per la verifica delle fonti. Nel settore finanziario, l'Associazione bancaria slovacca e le singole banche realizzano regolarmente campagne di sensibilizzazione mirate per prevenire le frodi nell'online banking. Tali campagne insegnano ai clienti come riconoscere i tentativi di phishing, utilizzare l'autenticazione multifattore e navigare in sicurezza nei servizi bancari elettronici.

Sebbene la Slovacchia abbia istituito una solida base istituzionale, il raggiungimento di una resilienza digitale diffusa tra gli adulti di età pari o superiore a 45 anni richiede uno sforzo costante. Il successo dipende dalla continua espansione di programmi di educazione non formale accessibili e dall'efficace diffusione di strumenti pratici di cybersecurity.

4. Buone pratiche

La ricerca documentale nazionale ha individuato un totale di quindici buone pratiche nei tre Paesi partner — cinque per ciascun Paese — rappresentative di una varietà di attori, metodologie e approcci rivolti ai diversi gruppi target. Queste iniziative dimostrano come le sfide legate alla sicurezza digitale vengano affrontate attraverso prevenzione, educazione ed empowerment a diversi livelli di governance e della società civile. Le pratiche sono presentate di seguito per Paese, utilizzando un formato coerente.

4.1 Italia

Durante la fase di ricerca documentale sono state individuate cinque buone pratiche nazionali rilevanti, che riflettono un ecosistema diversificato di iniziative volte a rafforzare l'alfabetizzazione digitale, la sicurezza online e la prevenzione delle frodi tra gli adulti. Tali iniziative includono programmi istituzionali, campagne di sensibilizzazione, iniziative regionali, progetti europei e azioni promosse dal terzo settore.

A livello nazionale, Repubblica Digitale rappresenta un quadro strategico per la promozione dello sviluppo delle competenze digitali e dell'inclusione, attraverso azioni coordinate come la Rete dei servizi di facilitazione digitale, a supporto dei cittadini — in particolare degli adulti — nell'uso sicuro dei servizi digitali.

Analogamente, la campagna I Navigati, promossa da istituzioni finanziarie e pubbliche, si concentra specificamente sulla sensibilizzazione rispetto alle frodi online e ai rischi di cybersecurity, in particolare nell'ambito dei servizi finanziari digitali.

A livello regionale, il programma Pane e Internet, sviluppato dalla Regione Emilia-Romagna, offre opportunità formative strutturate per gli adulti, con una forte attenzione alle competenze pratiche, incluse la sicurezza online e l'uso responsabile degli strumenti digitali.

Dal punto di vista europeo, il progetto Erasmus+ DIGITOL rappresenta un esempio rilevante di educazione non formale rivolta agli adulti più anziani, con l'obiettivo di migliorare le competenze digitali e promuovere un coinvolgimento sicuro con le tecnologie digitali.

Infine, Fondazione Mondo Digitale svolge un ruolo importante nel contesto italiano, realizzando programmi educativi inclusivi che supportano gruppi vulnerabili, compresi gli adulti, nello sviluppo di consapevolezza digitale e competenze in materia di cybersecurity. Nel loro insieme, queste iniziative dimostrano un approccio multilivello e multi-attore all'educazione alla sicurezza digitale, combinando policy, formazione, sensibilizzazione e innovazione.

Di seguito sono riportate le buone pratiche individuate:

1. **Repubblica Digitale (Digital Republic)**

<i>Titolo della buona pratica</i>	Repubblica Digitale
<i>Tipologia di buona pratica</i>	Iniziativa nazionale
<i>Organizzazione attuatrice</i>	Comitato Tecnico Guida, coordinato dal Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei Ministri, Italia. https://innovazione.gov.it/
<i>Obiettivi principali</i>	Colmare il divario digitale, contrastare tutte le forme di analfabetismo digitale e promuovere l'educazione alle tecnologie del futuro, sostenendo così lo sviluppo del Paese. Garantire una transizione graduale e inclusiva verso una società pienamente digitale.
<i>Gruppo/i target</i>	L'iniziativa si concentra principalmente su: • cittadini a rischio di esclusione digitale, come persone anziane o residenti in aree remote; • lavoratori che necessitano di aggiornare le proprie competenze tecnologiche; • studenti impegnati nello sviluppo dell'alfabetizzazione digitale; • pubbliche amministrazioni, per modernizzare i servizi pubblici; • organizzazioni del terzo settore, per creare una rete diffusa di facilitatori digitali.
<i>Risultati educativi e impatto</i>	Nel 2024, 272.270 dipendenti pubblici si sono iscritti a percorsi di apprendimento personalizzati per migliorare le proprie competenze digitali attraverso la piattaforma Syllabus. Inoltre, è stata introdotta una nuova direttiva che, a partire dal 2025, prevede almeno 40 ore annuali di formazione per ogni dipendente pubblico, con uno specifico focus sulla digitalizzazione, segnando un significativo cambiamento di tendenza rispetto al passato.

	Il Fondo per Repubblica Digitale ha finanziato 73 progetti che, nel 2024, hanno formato oltre 13.000 persone, tra cui NEET, disoccupati e lavoratori a rischio, contribuendo a colmare il divario di professionisti ICT nel mercato del lavoro italiano. Gli Hub di Educazione Digitale sono stati finanziati con 60 milioni di euro del PNRR, rappresentando uno sforzo volto a rafforzare il sistema universitario nei settori del trasferimento tecnologico e della formazione avanzata, a supporto della preparazione di specialisti altamente qualificati. I “Punti Digitale Facile” hanno coinvolto oltre 1,8 milioni di cittadini entro ottobre 2025, contribuendo a ridurre il divario digitale e a promuovere l’accesso ai servizi digitali per la popolazione generale. Gli interventi di formazione e digitalizzazione coinvolgono attivamente enti pubblici, imprese e terzo settore. Questa strategia orienta gli interventi sia nella sfera pubblica sia in quella privata, favorendo una continuità di lungo periodo oltre gli investimenti straordinari.
<i>Descrizione dell’attività e approccio metodologico</i>	Un pilastro chiave di questa attività è il Servizio Civile Digitale, un programma in cui giovani volontari di età compresa tra 18 e 28 anni operano per 12 mesi come mentor, accompagnando i cittadini attraverso un processo di “learning by doing”. Questo apprendimento peer-to-peer e intergenerazionale si fonda ulteriormente sui Punti Digitale Facile: con oltre 4.000 hub fisici istituiti in tutto il Paese, tali centri rappresentano spazi comunitari accessibili in cui i cittadini possono attivare la propria identità digitale, come SPID o CIE. Oltre alla semplice attivazione, i facilitatori forniscono la formazione necessaria per utilizzare questi strumenti, insegnando agli utenti come accedere al fascicolo sanitario elettronico, pagare tasse online o firmare documenti digitali. Inoltre, Repubblica Digitale ha lanciato la Coalizione Italiana per le competenze digitali e il lavoro, un’alleanza aperta che mira a individuare e coinvolgere il maggior numero possibile di stakeholder — imprese, enti pubblici, ONG, ecc. — per creare

	una rete digitale e umana di soggetti disponibili a cooperare e a sviluppare una cultura scientifico-tecnologica nazionale. Ad oggi, più di 180 organizzazioni hanno aderito alla Coalizione Italiana e avviato oltre 220 progetti. Per aderire alla coalizione, un'organizzazione deve formalmente sottoscrivere il Manifesto di Repubblica Digitale, garantendo che tutti i membri siano impegnati nei medesimi valori di inclusione, etica e sovranità digitale.
<i>Caratteristiche innovative</i>	L'iniziativa utilizza sia l'educazione formale sia quella non formale, integrate nelle diverse attività e nei vari progetti, e valorizza fortemente la cooperazione multisettoriale tra settore pubblico, settore privato e società civile. Un tratto distintivo del modello di intervento è l'utilizzo di un approccio peer-to-peer e dell'apprendimento intergenerazionale. Questi elementi, insieme all'impegno per una ampia inclusione e all'attenzione ai gruppi vulnerabili, la rendono una base strategica e integrata per l'alfabetizzazione e la formazione digitale a livello nazionale.
<i>Link / riferimento</i>	https://repubblicadigitale.gov.it/portale/
<i>Materiali visivi</i>	https://repubblicadigitale.gov.it/portale/-/l-italia-delle-competenze-digitali-si-fa-rete-i-risultati-raggiunti-e-le-sfide-del-futuro-martedì%3AC3%AC31-marzo-a-roma The graphic consists of two parts. The top part is an orange banner with the text 'È online il nuovo programma formativo "Pratiche digitali di partecipazione per il Governo Aperto"'. Below this, it says 'Scopri i moduli.' and shows icons for a laptop, a smartphone, and a person. The bottom part is a grid of 12 small images showing various people, likely participants or organizers, with the text 'REPUBBLICA DIGITALE' and 'Martedì, 31 marzo 2016'.

Valutazione dell'adattabilità di Repubblica Digitale

Criterio	Completamente	In certa misura	Per nulla	Commenti (opzionale)
a) Diversi gruppi target (es. giovani, senior, professionisti)	☒	☐	☐	
b) Diverse organizzazioni (es. ONG, scuole, autorità pubbliche)	☒	☐	☐	
c) Diversi temi o sfide (es. privacy, disinformazione, cybersecurity)	☐	☒	☐	

2. I Navigati

Titolo della buona pratica	I Navigati
Tipologia di buona pratica	Campagna, strumento online
Organizzazione attuatrice	CERTFin — Computer Emergency Response Team del settore finanziario italiano. https://www.certfin.it/en/
Obiettivi principali	Promuovere l'alfabetizzazione digitale, sensibilizzare ed educare le persone a un uso consapevole e sicuro degli strumenti e delle piattaforme digitali, al fine di evitare che cadano nelle trappole predisposte dai criminali informatici.
Gruppo/i target	Il pubblico target è ampio: dai giovani agli adulti. Il target principale è costituito da persone che utilizzano regolarmente canali digitali — online banking, app di pagamento, trading online — per gestire le proprie finanze, nonché da persone con competenze digitali

	limitate che incontrano difficoltà nel distinguere una truffa da una procedura legittima.
<i>Risultati educativi e impatto</i>	Gli utenti imparano a fermarsi e verificare le richieste attraverso canali ufficiali prima di agire. I partecipanti acquisiscono competenze per identificare truffe sofisticate che possono aggirare i filtri tradizionali. Intervenendo sul “fattore umano”, la campagna riduce significativamente la vulnerabilità dei partecipanti. Gli utenti imparano a riconoscere deepfake vocali o video generati dall’intelligenza artificiale, prevenendo il rischio di cadere vittima di truffe emotive che imitano familiari o persone conosciute.
<i>Descrizione dell’attività e approccio metodologico</i>	La campagna si svolge generalmente in “ondate” annuali, spesso con un picco nel mese di ottobre in coincidenza con il Mese europeo della cybersecurity. La campagna è promossa attraverso i principali canali televisivi, radiofonici, il sito ufficiale e i social media. La campagna utilizza lo storytelling per rendere più semplice la comprensione di temi complessi: • una web serie di brevi video in cui i membri della famiglia Navigati affrontano diversi rischi legati al mondo digitale; • il podcast “Al Sicuro”, condotto dall’esperta tech Fjona Cakalli, che affronta diverse tipologie di frodi online, trasformando tali lezioni audio in uno strumento per offrire consigli pratici su come riconoscere le strategie psicologiche dei truffatori.
<i>Caratteristiche innovative</i>	Ciò che distingue realmente I Navigati è l’uso innovativo dello storytelling e di una strategia mediatica multicanale, pensata per trasformare temi complessi di cybersecurity in scenari quotidiani facilmente riconoscibili. La campagna ruota attorno alla “famiglia Navigati”,

	esperta di sicurezza digitale, le cui avventure domestiche fungono da modelli educativi per il pubblico. Attraverso una serie di brevi episodi video — di circa 3 minuti ciascuno — la famiglia mostra come difendersi e riconoscere i primi segnali di una truffa. Questo tono familiare e leggero rende i consigli tecnici accessibili e meno intimidatori per i non esperti. Per garantire che il messaggio raggiunga anche i cittadini in mobilità, la campagna include anche una breve serie podcast, offrendo lezioni audio flessibili sulla sicurezza digitale.
<i>Link / riferimento</i>	https://inavigati.certfin.it/index.html
<i>Materiali visivi</i>	Copertura mediatica: https://www.bancaditalia.it/media/notizia/i-navigati-al-via-la-nuova-campagna-sulla-sicurezza-informatica/?dotcache=refresh

Valutazione dell'adattabilità de I Navigati

<i>Criterio</i>	<i>Completamente</i>	<i>In certa misura</i>	<i>Per nulla</i>	<i>Commenti (opzionale)</i>
a) <i>Diversi gruppi target (es. giovani, senior, professionisti)</i>	☒	☐	☐	
b) <i>Diverse organizzazioni (es. ONG, scuole, autorità pubbliche)</i>	☒	☐	☐	
c) <i>Diversi temi o sfide (es. privacy, misinformation e, cybersecurity)</i>	☒	☐	☐	

3. **Pane e Internet**

<i>Titolo della buona pratica</i>	Pane e Internet
<i>Tipologia di buona pratica</i>	Progetto / Formazione
<i>Organizzazione attuatrice</i>	Regione Emilia-Romagna, Italia pei@paneeinternet.it
<i>Obiettivi principali</i>	Promuovere lo sviluppo delle competenze digitali, rafforzare la rete regionale sia a livello locale sia regionale e accrescere la consapevolezza digitale dei cittadini rispetto alle questioni globali.
<i>Gruppo/i target</i>	Cittadini di qualsiasi età che utilizzano la tecnologia per accedere alle informazioni, usare servizi online e beneficiare delle opportunità digitali disponibili nella propria comunità.
<i>Risultati educativi e impatto</i>	I programmi formativi di Pane e Internet sono stati progettati e realizzati in conformità con il modello europeo DigComp, il quadro di riferimento per le competenze digitali dei cittadini. Le sue attività formative sono state riconosciute dalla Commissione europea come una delle migliori pratiche europee nel campo dell'educazione all'alfabetizzazione digitale. I partecipanti possono essere gradualmente introdotti al mondo digitale attraverso webinar e corsi adattati ai loro bisogni e al loro livello di conoscenza. I partecipanti non solo migliorano la propria consapevolezza digitale, ma diventano anche contributori attivi alla trasformazione dell'Emilia-Romagna in una regione più avanzata e tecnologicamente inclusiva, favorendo un cambiamento collettivo verso una comunità più connessa e pronta al futuro.
<i>Descrizione dell'attività e approccio</i>	L'iniziativa opera offrendo numerosi workshop e corsi online. Durante tutto l'anno propone decine di corsi

<i>metodologico</i>	gratuiti e webinar, con durata variabile a seconda del tema. Un'azione permanente è il mantenimento dei Punti Pane e Internet (Pel) in tutta la regione, grazie alla collaborazione con Comuni e municipalità, assicurando che il supporto digitale sia sempre fisicamente raggiungibile all'interno della comunità. Pane e Internet offre corsi di alfabetizzazione digitale personalizzati, che spaziano dalle competenze informatiche di base e dall'uso dell'hardware fino alla consapevolezza avanzata in materia di cybersecurity. Questo approccio per livelli consente agli utenti di progredire dalle operazioni tecniche di base fino all'identificazione e alla difesa da rischi online complessi. Nella progettazione dei corsi viene dedicata una particolare attenzione anche ai gruppi vulnerabili, al fine di garantire massima diffusione e accessibilità.
<i>Caratteristiche innovative</i>	La Commissione europea ha riconosciuto il programma educativo Pel come una delle migliori pratiche europee nel campo dell'alfabetizzazione digitale. Gli eventi formativi e i webinar si svolgono online per garantire la massima accessibilità, raggiungendo anche le aree più remote della regione. Al tempo stesso, il progetto mantiene una forte presenza territoriale attraverso hub fisici strategicamente distribuiti sul territorio regionale. Questi centri locali sono essenziali per favorire la cooperazione comunitaria e garantire una diffusione ampia degli strumenti digitali.
<i>Link / riferimento</i>	https://www.paneeinternet.it/
<i>Materiali visivi</i>	https://www.paneeinternet.it/public/elenco-news

Valutazione dell'adattabilità di Pane e Internet

Criterio	Completament	In certa	Per nulla	Commenti
----------	--------------	----------	-----------	----------

	<i>e</i>	<i>misura</i>		<i>(opzionale)</i>
<i>a) Diversi gruppi target (es. giovani, senior, professionisti)</i>	☒	☐	☐	
<i>b) Diverse organizzazioni (es. ONG, scuole, autorità pubbliche)</i>	☒	☐	☐	
<i>c) Diversi temi o sfide (es. privacy, disinformazione e, cybersecurity)</i>	☒	☐	☐	

4. **Progetto Erasmus+ DIGITOL**

<i>Titolo della buona pratica</i>	Progetto Erasmus+ DIGITOL
<i>Tipologia di buona pratica</i>	Progetto
<i>Organizzazione attuatrice</i>	Partenariato composto da sei organizzazioni provenienti da sei diversi Paesi europei: Consorzio Comunità Brianza (Italia), Pro Arbeit (Germania), 50PLUS Hellas (Grecia), Znanie (Bulgaria), Tree Agency (Estonia), AGE Platform Europe (Belgio).
<i>Obiettivi principali</i>	DIGITOL promuove valori dell'Unione europea come solidarietà e diversità attraverso programmi innovativi di alfabetizzazione digitale. Il progetto mira a creare un Internet più rispettoso, contrastando discriminazione e xenofobia attraverso il coinvolgimento di diverse generazioni nell'identificazione e nel contenimento delle fake news e dell'odio online.
<i>Gruppo/i target</i>	Adulti europei più anziani, di età superiore a 55 anni.
<i>Risultati educativi e impatto</i>	Dieci giovani, di età compresa tra 18 e 30 anni, provenienti dai Paesi partner, sono stati formati attraverso un percorso di training for trainers della

	durata di 30 ore, focalizzato sul contrasto alle fake news e alla polarizzazione. Venticinque senior, di età superiore a 55 anni, hanno partecipato al programma DIGITOL di capacity building della durata di 60 ore, guidato da giovani ed esperti esterni, finalizzato a fornire ai partecipanti strumenti teorici e pratici per comprendere meglio l'evoluzione della società contemporanea in linea con i valori europei.
<i>Descrizione dell'attività e approccio metodologico</i>	Training of Trainers (ToT): i "Young Ambassadors", giovani di età compresa tra 18 e 30 anni, hanno imparato a diventare mentor intergenerazionali. Hanno acquisito non solo competenze digitali, ma anche tecniche pedagogiche per insegnare ai senior. Capacity Building Programme (CBP): la fase educativa centrale, in cui gli Young Ambassadors hanno condotto workshop per senior di età superiore a 55 anni su media literacy, identificazione delle fake news e contrasto all'odio online. Azioni pilota e attività di follow-up: i partecipanti sono passati dalla formazione in aula all'azione concreta, organizzando "Human Libraries" e "Digitol Festivals" per promuovere coesione sociale e valori europei nelle comunità locali.
<i>Caratteristiche innovative</i>	La caratteristica più innovativa del progetto è l'approccio intergenerazionale: giovani formati come mentor supportano gli adulti più anziani nello sviluppo di competenze digitali e critiche, creando un ambiente di apprendimento basato su fiducia, scambio e cooperazione. Il progetto combina educazione non formale, media literacy e promozione dei valori europei, affrontando in modo integrato fake news, polarizzazione e odio online. Inoltre, il passaggio dalle attività formative alle azioni

	pubbliche locali rafforza l'impatto comunitario e la trasferibilità del modello.
<i>Link / riferimento</i>	https://digitol.eu/it/
<i>Materiali visivi</i>	Brochure del progetto: https://digitol.eu/wp-content/uploads/2020/07/DIGITOL-Project-Brochure-English.pdf Toolkit: https://digitol.eu/wp-content/uploads/2022/01/toolkit-ITA-DEF.pdf

Valutazione dell'adattabilità del progetto Erasmus+ DIGITOL

<i>Criterio</i>	<i>Completamente</i>	<i>In certa misura</i>	<i>Per nulla</i>	<i>Commenti (opzionale)</i>
<i>a) Diversi gruppi target (es. giovani, senior, professionisti)</i>	☒	☐	☐	
<i>b) Diverse organizzazioni (es. ONG, scuole, autorità pubbliche)</i>	☒	☐	☐	
<i>c) Diversi temi o sfide (es. privacy, disinformazione, cybersecurity)</i>	☒	☐	☐	

5. Fondazione Mondo Digitale

<i>Titolo della buona pratica</i>	Fondazione Mondo Digitale
<i>Tipologia di buona pratica</i>	Formazione

<i>Organizzazione attuatrice</i>	Fondazione Mondo Digitale ETS, Italia info@mondodigitale.org https://www.mondodigitale.org/
<i>Obiettivi principali</i>	Promuovere una cultura dell'innovazione e favorire una nuova economia basata sulla conoscenza come leva di sviluppo del Paese. Utilizzare le tecnologie digitali per il progresso sociale, al fine di alimentare crescita, benessere, produttività e competitività.
<i>Gruppo/i target</i>	Persone di ogni età e background lavorativo: il sito consente agli utenti di selezionare il termine che meglio li rappresenta, ad esempio donne, disoccupati, dirigenti, artisti, ecc.
<i>Risultati educativi e impatto</i>	Le persone che partecipano ai progetti e agli eventi della Fondazione Mondo Digitale acquisiscono competenze in ambito STEAM, creando al contempo una rete di relazioni nel proprio contesto di riferimento. Grazie alla struttura dei progetti, le competenze digitali sono integrate con competenze sociali e di cittadinanza attiva. Ciò avviene incoraggiando la partecipazione a eventi, competizioni locali e webinar.
<i>Descrizione dell'attività e approccio metodologico</i>	Fondazione Mondo Digitale si concentra sull'offerta di laboratori STEAM in diversi ambiti. Inoltre, workshop e seminari sono direttamente integrati con contest locali e nazionali, offrendo ai partecipanti opportunità immediate di applicare concetti teorici attraverso competizioni pratiche, come RomeCup e Digital Made. I progetti possono variare da workshop brevi e intensivi di 3 ore fino a percorsi curricolari annuali integrati nel calendario scolastico. La metodologia del learning by doing è utilizzata in ogni progetto, e la sua principale rappresentazione è costituita dalle Palestre dell'Innovazione, spazi ibridi fisici e virtuali diffusi in tutta Italia, nei quali persone di ogni età possono apprendere sia competenze tecniche sia soft skills.
<i>Caratteristiche innovative</i>	Ciò che distingue realmente questo progetto è la pagina web personalizzata, che organizza le opportunità in specifici gruppi target — da donne e giovani, a persone anziane, migranti, artisti,

	ecc. — consentendo agli utenti di individuare immediatamente corsi e iniziative più adatti alla propria crescita personale o professionale. Questa accessibilità è accompagnata da una filosofia di “learning by doing”, in cui le attività educative pratiche sono direttamente intrecciate con contest nazionali e locali. Partecipando a tali competizioni, i discenti possono applicare immediatamente le conoscenze teoriche a sfide reali.
<i>Link / riferimento</i>	https://www.mondodigitale.org/
<i>Materiali visivi</i>	https://youtu.be/m-Jd6NR31uk?si=DBQRTWNVSPVP4Ycx https://www.repubblica.it/tecnologia/sicurezza/2020/02/04/news/google_premia_4_progetti_italiani_su_sicurezza_online-247591358/

Valutazione dell'adattabilità di Fondazione Mondo Digitale

Criterio	Completamente	In certa misura	Per nulla	Commenti (opzionale)
a) Diversi gruppi target (es. giovani, senior, professionisti)	☒	☐	☐	
b) Diverse organizzazioni (es. ONG, scuole, autorità pubbliche)	☒	☐	☐	
c) Diversi temi o sfide (es. privacy, disinformazione, cybersecurity)	☒	☐	☐	

4.2 Spagna

Nell'ambito della fase di ricerca del progetto digiSAFE, è stata realizzata una mappatura delle buone pratiche nazionali al fine di individuare iniziative efficaci in Spagna che promuovano la sicurezza digitale, la prevenzione delle frodi e l'alfabetizzazione digitale tra gli adulti, con particolare rilevanza per le persone di età pari o superiore a 45 anni.

L'obiettivo di questa analisi è stato evidenziare approcci esistenti in grado di orientare lo sviluppo del Curriculum di educazione non formale di digiSAFE e del Toolkit per la prevenzione delle frodi digitali.

Le buone pratiche selezionate rappresentano una varietà di attori e metodologie, tra cui istituzioni pubbliche, forze dell'ordine, organizzazioni non governative, campagne nazionali di sensibilizzazione e iniziative formative basate sulla comunità.

Nel loro insieme, esse dimostrano come le sfide legate alla sicurezza digitale siano affrontate in Spagna attraverso prevenzione, educazione ed empowerment, piuttosto che facendo affidamento esclusivamente su misure tecniche o regolatorie.

Particolare attenzione è stata dedicata alle iniziative che adottano approcci di apprendimento non formale e accessibili, riconoscendo che gli adulti di età pari o superiore a 45 anni traggono spesso maggiore beneficio da metodi educativi pratici, basati sull'esperienza e facili da utilizzare.

Le pratiche individuate si concentrano sul rafforzamento della fiducia digitale, sulla sensibilizzazione rispetto ai rischi online, sul miglioramento della capacità di riconoscere frodi e truffe e sulla promozione di un uso responsabile delle tecnologie digitali nella vita quotidiana.

Inoltre, le buone pratiche selezionate mostrano un elevato grado di adattabilità e trasferibilità ad altri contesti nazionali ed europei. Molte di esse sono scalabili, inclusive e progettate per essere attuate da diverse tipologie di organizzazioni, risultando quindi particolarmente adatte alla replicazione nell'ambito del quadro progettuale di digiSAFE.

Di seguito sono riportate le 5 buone pratiche individuate in Spagna:

1. **Fundación Cibervoluntarios – Digital Inclusion and Digital Skills for Adults**

<i>Titolo della buona pratica</i>	Fundación Cibervoluntarios – Inclusione digitale e competenze digitali per adulti
<i>Tipologia di buona pratica</i>	Progetto / Formazione / Workshop
<i>Organizzazione attuatrice</i>	Fundación Cibervoluntarios, Spagna https://www.cibervoluntarios.org
<i>Obiettivi principali</i>	Ridurre il divario digitale, rafforzando negli adulti e nei senior competenze digitali, fiducia e consapevolezza, affinché possano partecipare in modo sicuro alla società digitale.
<i>Gruppo/i target</i>	Adulti, senior, gruppi vulnerabili, adulti di età pari o superiore a 45 anni.
<i>Risultati educativi e impatto</i>	I partecipanti migliorano le competenze digitali di base e intermedie, aumentano la fiducia nell'uso degli strumenti

	digitali e sviluppano una maggiore consapevolezza dei rischi online, delle frodi e della disinformazione.
<i>Descrizione dell'attività e approccio metodologico</i>	Attività gratuite di formazione digitale erogate online e in presenza attraverso centri comunitari, associazioni e istituzioni pubbliche. La metodologia si basa sull'educazione non formale, su esercitazioni pratiche, apprendimento tra pari e scenari digitali tratti dalla vita reale.
<i>Caratteristiche innovative</i>	Mentoring digitale guidato da volontari, approccio basato sulla comunità e percorsi di apprendimento personalizzati per adulti e senior.
<i>Link / riferimento</i>	https://www.cibervoluntarios.org
<i>Materiali visivi</i>	Materiali formativi, video, infografiche, report di progetto e risorse online disponibili sul sito dell'organizzazione.

Valutazione dell'adattabilità del Fundación Cibervoluntarios – Digital Inclusion and Digital Skills for Adults

<i>Criterio</i>	<i>Completamente</i>	<i>In certa misura</i>	<i>Per nulla</i>	<i>Commenti</i>
<i>a) Diversi gruppi target (es. giovani, senior, professionisti)</i>	☒	☐	☐	
<i>b) Diverse organizzazioni (es. ONG, scuole, autorità pubbliche)</i>	☒	☐	☐	
<i>c) Diversi temi o sfide (es. privacy, disinformazione, cybersecurity)</i>	☒	☐	☐	

2. Aula Mentor – Adult Education and Digital Skills Programme

<i>Titolo della buona pratica</i>	Aula Mentor – Programma di educazione degli adulti e competenze digitali
<i>Tipologia di buona pratica</i>	Formazione / Programma di apprendimento online
<i>Organizzazione attuatrice</i>	Ministero dell'Istruzione e della Formazione Professionale, Spagna https://www.aulamentor.es
<i>Obiettivi principali</i>	Promuovere l'apprendimento permanente offrendo agli adulti un accesso flessibile alla formazione sulle competenze digitali e ICT.

<i>Gruppo/i target</i>	Adulti (18+), compresi adulti di età pari o superiore a 45 anni.
<i>Risultati educativi e impatto</i>	I discenti acquisiscono competenze digitali di base, migliorano la propria autonomia nell'uso degli strumenti online e aumentano la fiducia negli ambienti digitali.
<i>Descrizione dell'attività e approccio metodologico</i>	Corsi online supportati da mentor formati, che consentono agli adulti di apprendere secondo i propri tempi attraverso un modello flessibile di apprendimento non formale, adattato ai bisogni degli adulti in apprendimento.
<i>Caratteristiche innovative</i>	Copertura nazionale, apprendimento supportato da mentor e accesso flessibile per gli adulti.
<i>Link / riferimento</i>	https://www.aulamentor.es
<i>Materiali visivi</i>	Cataloghi dei corsi online, screenshot della piattaforma e materiali informativi disponibili sul sito ufficiale.

Valutazione dell'adattabilità di Aula Mentor – Adult Education and Digital Skills Programme

<i>Criterio</i>	<i>Completamente</i>	<i>In certa misura</i>	<i>Per nulla</i>	<i>Commenti</i>
<i>a) Diversi gruppi target (es. giovani, senior, professionisti)</i>	☒	☐	☐	
<i>b) Diverse organizzazioni (es. ONG, scuole, autorità pubbliche)</i>	☐	☒	☐	
<i>c) Diversi temi o sfide (es. privacy, disinformazione, cybersecurity)</i>	☒	☐	☐	

3. Policía Nacional – Plan Mayor Seguridad

<i>Titolo della buona pratica</i>	Policía Nacional – Plan Mayor Seguridad
<i>Tipologia di buona pratica</i>	Campagna / Iniziativa di sensibilizzazione

<i>Organizzazione attuatrice</i>	Policía Nacional, Spagna https://www.policia.es
<i>Obiettivi principali</i>	Prevenire crimini e frodi che colpiscono gli adulti più anziani, aumentando la consapevolezza dei rischi digitali e offline e promuovendo comportamenti sicuri.
<i>Gruppo/i target</i>	Adulti più anziani, senior, associazioni per persone anziane.
<i>Risultati educativi e impatto</i>	Aumento della consapevolezza rispetto agli schemi di frode, miglioramento della capacità di riconoscere le truffe e rafforzamento della fiducia tra cittadini anziani e istituzioni pubbliche.
<i>Descrizione dell'attività e approccio metodologico</i>	Incontri informativi e workshop realizzati da agenti di polizia presso centri comunitari e associazioni, utilizzando esempi pratici e indicazioni orientate alla prevenzione.
<i>Caratteristiche innovative</i> <i>Link / riferimento</i>	Coinvolgimento diretto di professionisti delle forze dell'ordine e forte partecipazione comunitaria. https://www.policia.es/_es/colabora_plan_mayor_seguridad.php
<i>Materiali visivi</i>	Poster, brochure, materiali di presentazione e visual della campagna disponibili attraverso i canali della Policía Nacional.

Valutazione dell'adattabilità di Policía Nacional – Plan Mayor Seguridad

<i>Criterio</i>	<i>Completament e</i>	<i>In certa misura</i>	<i>Per nulla</i>	<i>Comment i</i>
<i>a) Diversi gruppi target (es. giovani, senior, professionisti)</i>	☐	☒	☐	
<i>b) Diverse organizzazioni (es. ONG, scuole, autorità pubbliche)</i>	☐	☒	☐	
<i>c) Diversi temi o sfide (es. privacy, disinformazione, cybersecurity)</i>	☒	☐	☐	

4. INCIBE – 017 Cybersecurity Helpline and Awareness Programme

<i>Titolo della buona pratica</i>	INCIBE – Linea 017 di assistenza cybersecurity e programma di sensibilizzazione
<i>Tipologia di buona pratica</i>	Servizio pubblico / Campagna di sensibilizzazione / Strumento online
<i>Organizzazione attuatrice</i>	Instituto Nacional de Ciberseguridad (INCIBE), Spagna https://www.incibe.es
<i>Obiettivi principali</i>	Migliorare la consapevolezza dei cittadini sui rischi di cybersecurity e fornire orientamento sulla prevenzione delle frodi e sui comportamenti digitali sicuri.
<i>Gruppo/i target</i>	Popolazione generale, adulti, senior, utenti vulnerabili.
<i>Risultati educativi e impatto</i>	Gli utenti migliorano la consapevolezza delle minacce digitali, aumentano la capacità di riconoscere frodi e truffe e adottano pratiche online più sicure.
<i>Descrizione dell'attività e approccio metodologico</i>	Linea pubblica gratuita di assistenza che offre supporto personalizzato tramite telefono, chat e app di messaggistica, combinata con campagne di sensibilizzazione e risorse educative online.
<i>Caratteristiche innovative</i>	Accesso multicanale, supporto personalizzato in tempo reale e integrazione tra educazione e risposta agli incidenti.
<i>Link / riferimento</i>	https://www.incibe.es/linea-017
<i>Materiali visivi</i>	N/D

Valutazione dell'adattabilità di INCIBE – 017 Cybersecurity Helpline and Awareness Programme

<i>Criterio</i>	<i>Completamente</i>	<i>In certa misura</i>	<i>Per nulla</i>	<i>Commenti</i>
<i>a) Diversi gruppi target (es. giovani, senior, professionisti)</i>	☒	☐	☐	
<i>b) Diverse organizzazioni (es. ONG, scuole, autorità pubbliche)</i>	☐	☒	☐	
<i>c) Diversi temi o sfide (es. privacy, disinformazione, cybersecurity)</i>	☒	☐	☐	

5. Regional Digital Skills Programmes for Seniors (Spain)

<i>Titolo della buona pratica</i>	Programmi regionali di competenze digitali per senior (Spagna)
<i>Tipologia di buona pratica</i>	Formazione / Workshop / Iniziativa pubblica

<i>pratica</i>	
<i>Organizzazione attuatrice</i>	Autorità pubbliche regionali e locali, Spagna
<i>Obiettivi principali</i>	Promuovere l'inclusione digitale e l'uso sicuro delle tecnologie digitali tra gli adulti più anziani a livello locale.
<i>Gruppo/i target</i>	Adulti più anziani, senior, adulti con basse competenze digitali.
<i>Risultati educativi e impatto</i>	I partecipanti migliorano le competenze digitali di base, aumentano la fiducia nell'uso dei servizi online e acquisiscono consapevolezza dei rischi online e delle strategie di prevenzione delle frodi.
<i>Descrizione dell'attività e approccio metodologico</i>	Attività formative pratiche svolte presso centri comunitari, biblioteche o centri di educazione degli adulti, attraverso sessioni in piccoli gruppi orientate alla pratica.
<i>Caratteristiche innovative</i>	Approccio localizzato, coinvolgimento diretto della comunità e adattamento ai bisogni specifici dei discenti.
<i>Link / riferimento</i>	N/D
<i>Materiali visivi</i>	N/D

Valutazione dell'adattabilità di *Regional Digital Skills Programmes for Seniors (Spain)*

<i>Criterio</i>	<i>Completamente</i>	<i>In certa misura</i>	<i>Per nulla</i>	<i>Commenti</i>
<i>a) Diversi gruppi target (es. giovani, senior, professionisti)</i>	☒	☐	☐	
<i>b) Diverse organizzazioni (es. ONG, scuole, autorità pubbliche)</i>	☒	☐	☐	
<i>c) Diversi temi o sfide (es. privacy, disinformazione, cybersecurity)</i>	☒	☐	☐	

4.3 Slovacchia

La fase di ricerca documentale ha individuato cinque buone pratiche nazionali distinte in Slovacchia, promosse dal settore privato, da organizzazioni non profit e da reti comunitarie. Queste iniziative offrono approcci altamente adattabili per contrastare l'esclusione digitale e prevenire le frodi online tra gli adulti più anziani.

Bezpečne na nete (Navigare in sicurezza)
Realizzato dalla società slovacca di cybersecurity ESET, questo portale educativo completo offre risorse gratuite e accessibili sulla sicurezza digitale. Sebbene sia rivolto alla popolazione generale, i suoi articoli, podcast e video-guide, formulati in modo

semplice e diretto, risultano particolarmente efficaci per adulti e senior. La piattaforma traduce minacce complesse di cybersecurity — come malware, phishing e privacy dei dati — in un linguaggio semplice e quotidiano. La sua principale innovazione consiste nel mettere a disposizione del pubblico competenze specialistiche provenienti dal settore privato della cybersecurity, offrendo contenuti educativi di alta qualità, costantemente aggiornati e fruibili individualmente secondo i propri tempi.

Zrelí na dobu digitánu (Maturi per l'era digitale)
 Gestito dal Fondo di dotazione Slovak Telekom, questo programma educativo e di finanziamento è specificamente rivolto all'inclusione digitale dei senior. L'iniziativa finanzia e sostiene organizzazioni locali, case di cura e centri comunitari affinché realizzino corsi di alfabetizzazione digitale su misura. La metodologia si concentra su ambienti di apprendimento pratici, in piccoli gruppi, nei quali gli adulti più anziani possono esercitarsi in sicurezza nell'uso degli smartphone, nella gestione degli account online e nel riconoscimento delle truffe più comuni. Questo approccio decentralizzato assicura che l'educazione raggiunga i senior nelle loro comunità locali, rendendo l'apprendimento accessibile e socialmente coinvolgente.

Zodpovedne.sk (Responsabilmente.sk)

Gestito dall'associazione civica eSlovensko, questo centro nazionale di sensibilizzazione si concentra sull'uso sicuro di Internet per tutte le generazioni. Per il target 45+, mette a disposizione manuali stampati mirati, video didattici e servizi di consulenza relativi alle minacce informatiche. L'iniziativa agisce come strumento educativo preventivo, insegnando agli adulti come mettere in sicurezza i propri dispositivi, proteggere i dati personali e riconoscere la manipolazione psicologica online. Il suo punto di forza è la continuità nel tempo e l'ampia raccolta di materiali localizzati e facili da comprendere, che possono essere ampiamente distribuiti da educatori e ONG.

Seminari Senior bezpečne online (Senior sicuri online)
 Organizzati attraverso le sezioni locali dell'Unione dei Pensionati in Slovacchia (JDS), in collaborazione con esperti IT regionali, questi seminari di base offrono un'educazione diretta e supportata dai pari. I workshop si svolgono in spazi comunitari familiari e si concentrano fortemente sulle minacce immediate, come truffe finanziarie locali, falsi e-shop e comunicazione sicura con i familiari. La forza metodologica risiede nel modello di fiducia peer-to-peer: apprendere all'interno di una rete di pari riduce significativamente l'ansia che gli adulti più anziani spesso provano nell'adottare nuove abitudini digitali.

Smart Senior Academies presso le biblioteche regionali
 Le biblioteche pubbliche slovacche, come le biblioteche regionali di Žilina e Bratislava, si sono trasformate in importanti hub per l'educazione digitale degli adulti. Queste istituzioni ospitano regolarmente corsi strutturati "Smart Senior". Bibliotecari e formatori IT volontari guidano i partecipanti nella navigazione digitale di base, nella valutazione delle informazioni online e nel riconoscimento delle email fraudolente. Questa pratica utilizza infrastrutture comunitarie esistenti, affidabili e accessibili, per fornire un

supporto educativo continuo, gratuito e paziente, rendendola un modello facilmente adattabile a qualsiasi municipalità.

Di seguito sono riportate le 5 buone pratiche individuate:

1. **Bezpečne na nete (Safely on the Net)**

<i>Titolo della buona pratica</i>	Bezpečne na nete (Navigare in sicurezza)
<i>Tipologia di buona pratica</i>	Strumento online / Campagna
<i>Organizzazione attuatrice</i>	ESET, Slovacchia. https://bezpecnenanete.eset.com/sk/
<i>Obiettivi principali</i>	Aumentare la consapevolezza rispetto alle minacce di cybersecurity e fornire educazione gratuita e pratica su come navigare in Internet in modo sicuro, adattata a tutti i gruppi di utenti, compresi i senior.
<i>Gruppo/i target</i>	Popolazione generale, adulti, senior, educatori e genitori.
<i>Risultati educativi e impatto</i>	Gli utenti accedono a una biblioteca costantemente aggiornata di articoli, video e podcast. I partecipanti imparano a riconoscere le minacce informatiche moderne, proteggere la propria privacy digitale e operare online in sicurezza senza timore di esclusione digitale.
<i>Descrizione dell'attività e approccio metodologico</i>	Il portale opera come hub educativo centralizzato che offre materiali di apprendimento passo dopo passo. La metodologia si basa sulla traduzione di concetti complessi di sicurezza informatica, come malware, phishing e violazioni dei dati, in un linguaggio semplice e quotidiano. I contenuti sono organizzati per diversi livelli di competenza e situazioni di vita, rendendo facile per gli adulti più anziani fruirli secondo i propri tempi.
<i>Caratteristiche innovative</i>	L'iniziativa valorizza la profonda competenza globale di cybersecurity di una società tecnologica leader del settore privato, ESET, per fornire al pubblico contenuti educativi gratuiti, di alta qualità e non commerciali.
<i>Link / riferimento</i>	https://bezpecnenanete.eset.com/sk/
<i>Materiali visivi</i>	Screenshot del portale e della biblioteca podcast disponibili su: https://bezpecnenanete.eset.com/sk/

Valutazione dell'adattabilità di Bezpečne na nete (Safely on the Net):

<i>Criterio</i>	<i>Completament</i>	<i>In certa</i>	<i>Per</i>	<i>Commenti</i>
-----------------	---------------------	-----------------	------------	-----------------

	<i>e</i>	<i>misura</i>	<i>nulla</i>	
<i>a) Diversi gruppi target (es. giovani, senior, professionisti)</i>	☒	☐	☐	I contenuti sono già segmentati per diversi gruppi di età e livelli di competenza tecnica.
<i>b) Diverse organizzazioni (es. ONG, scuole, autorità pubbliche)</i>	☒	☐	☐	Aziende del settore privato in tutta Europa potrebbero replicare questo modello di responsabilità sociale d'impresa.
<i>c) Diversi temi o sfide (es. privacy, disinformazione, cybersecurity)</i>	☒	☐	☐	Il formato della piattaforma consente facilmente l'aggiunta di nuovi temi, come le minacce legate all'IA.

2. *Zrelí na dobu digitálnu (Mature for the Digital Age)*

<i>Titolo della buona pratica</i>	Zrelí na dobu digitálnu (Maturi per l'era digitale)
<i>Tipologia di buona pratica</i>	Progetto / Finanziamento / Formazione
<i>Organizzazione attuatrice</i>	Slovak Telekom Endowment Fund (Nadačný fond Telekom pri Nadácii Pontis), Slovacchia. https://nadacnyfondtelekom.sk/
<i>Obiettivi principali</i>	Promuovere l'alfabetizzazione digitale, sensibilizzare ed educare le persone a un uso consapevole e sicuro degli strumenti e delle piattaforme digitali, così da evitare che cadano nelle trappole predisposte dai criminali informatici.
<i>Gruppo/i target</i>	Senior di età pari o superiore a 65 anni, ONG locali, case di cura e centri comunitari.
<i>Risultati educativi e impatto</i>	Il programma di finanziamento ha sostenuto decine di organizzazioni locali con oltre 200.000 euro, formando migliaia di senior. I partecipanti migliorano il pensiero critico, imparano a verificare le fonti informative e sviluppano resilienza rispetto alla manipolazione emotiva utilizzata dai truffatori.
<i>Descrizione dell'attività e</i>	Più che un singolo corso centralizzato, si tratta di un meccanismo di finanziamento che consente agli enti locali di

<i>approccio metodologico</i>	erogare formazione. I progetti sostenuti utilizzano metodologie pratiche in piccoli gruppi. I senior vengono formati in ambienti familiari per esercitarsi in sicurezza nell'uso degli smartphone, nell'identificazione delle truffe e nella comunicazione con i familiari, garantendo un accompagnamento paziente e personalizzato.
<i>Caratteristiche innovative</i>	Il modello di finanziamento decentralizzato si basa fortemente sulle reti comunitarie di base, assicurando che l'educazione digitale raggiunga anche senior isolati nelle aree rurali, che potrebbero non partecipare a corsi statali di grandi dimensioni.
<i>Link / riferimento</i>	https://nadacnyfondtelekom.sk/
<i>Materiali visivi</i>	Dettagli della campagna disponibili su: https://nadacnyfondtelekom.sk/aktualne-vyzvy/

Valutazione dell'adattabilità di Zrelí na dobu digitálnu (Mature for the Digital Age)

<i>Criterio</i>	<i>Completamente</i>	<i>In certa misura</i>	<i>Per nulla</i>	<i>Commenti</i>
<i>a) Diversi gruppi target (es. giovani, senior, professionisti)</i>	☐	☒	☐	Il modello di finanziamento è specificamente adattato ai bisogni e ai ritmi di apprendimento degli adulti più anziani.
<i>b) Diverse organizzazioni (es. ONG, scuole, autorità pubbliche)</i>	☒	☐	☐	Qualsiasi fondazione aziendale o ente pubblico può adottare questa metodologia di finanziamento decentralizzata.
<i>c) Diversi temi o sfide (es. privacy, disinformazione, cybersecurity)</i>	☒	☐	☐	I finanziamenti possono essere tematizzati annualmente per concentrarsi su questioni specifiche, come phishing o IA.

3. **Zodpovedne.sk (Responsibly.sk)**

<i>Titolo della buona pratica</i>	Zodpovedne.sk (Responsabilmente.sk)
<i>Tipologia di buona pratica</i>	Campagna / Strumento online
<i>Organizzazione attuatrice</i>	Associazione civica eSlovensko, Slovacchia. https://www.zodpovedne.sk/
<i>Obiettivi principali</i>	Aumentare la consapevolezza nazionale sulla sicurezza in Internet, prevenire la criminalità informatica e fornire risorse educative e servizi di consulenza sulle minacce informatiche per tutte le generazioni.
<i>Gruppo/i target</i>	Popolazione generale, adulti, senior, genitori ed educatori.
<i>Risultati educativi e impatto</i>	I senior imparano a cercare informazioni in modo autonomo, utilizzare account email e riconoscere comunicazioni fraudolente. L'iniziativa favorisce un senso di indipendenza e integrazione nella società digitale moderna.
<i>Descrizione dell'attività e approccio metodologico</i>	Le biblioteche ospitano corsi strutturati "Smart Senior" di più settimane o sessioni di supporto IT a sportello. Bibliotecari e formatori IT volontari guidano piccoli gruppi attraverso esercitazioni pratiche. La metodologia è molto paziente e consente ai senior di esercitarsi sui computer della biblioteca o sui propri dispositivi, affrontando temi che vanno dall'accensione del dispositivo fino alla sicurezza avanzata su Internet.
<i>Caratteristiche innovative</i>	L'iniziativa utilizza in modo intelligente l'infrastruttura esistente delle biblioteche pubbliche, percepite come affidabili e accessibili, per fornire educazione continua, gratuita e non intimidatoria agli adulti.
<i>Link / riferimento</i>	https://www.krajskakniznicazilina.sk/
<i>Materiali visivi</i>	Descrizioni dei corsi disponibili su: https://www.krajskakniznicazilina.sk/index.php/2023/10/19/digitalne-zrucni-seniori/

Valutazione dell'adattabilità di Zodpovedne.sk (Responsibly.sk)

<i>Criterio</i>	<i>Completamente</i>	<i>In certa misura</i>	<i>Per nulla</i>	<i>Commenti</i>
<i>a) Diversi gruppi target (es. giovani,</i>	☒	☐	☐	Le biblioteche servono l'intera comunità e

<i>senior, professionisti)</i>				possono adattare le classi a qualsiasi gruppo demografico.
<i>b) Diverse organizzazioni (es. ONG, scuole, autorità pubbliche)</i>	☒	☐	☐	Può essere utilizzato da scuole, centri di educazione degli adulti e autorità pubbliche.
<i>c) Diversi temi o sfide (es. privacy, disinformazione, cybersecurity)</i>	☒	☐	☐	È costantemente aggiornabile per affrontare nuovi fenomeni come gioco d'azzardo, IA e uso improprio dei dati.

4. Erasmus+ project DIGITOL

<i>Titolo della buona pratica</i>	Progetto Erasmus+ DIGITOL
<i>Tipologia di buona pratica</i>	Progetto
<i>Organizzazione attuatrice</i>	Unione dei Pensionati in Slovacchia (JDS), in collaborazione con esperti IT regionali e università. https://www.jednotadochodcov.sk
<i>Obiettivi principali</i>	Fornire un'educazione localizzata e supportata dai pari, che aiuti i senior a navigare in sicurezza in Internet, riconoscere le truffe finanziarie locali e ridurre l'ansia legata agli strumenti digitali.
<i>Gruppo/i target</i>	Senior e adulti pensionati.
<i>Risultati educativi e impatto</i>	I partecipanti passano progressivamente dall'evitare gli strumenti digitali all'utilizzarli in modo attivo e sicuro, compresi smartphone, applicazioni di chat e online banking, riducendo significativamente isolamento e vulnerabilità alle frodi di base.
<i>Descrizione dell'attività e approccio metodologico</i>	Si tratta di seminari di base organizzati direttamente dall'unione dei pensionati in spazi comunitari locali. La metodologia enfatizza l'apprendimento peer-to-peer e l'applicazione pratica immediata. I temi sono fortemente legati alla vita quotidiana: riconoscere e-shop fraudolenti, individuare fake news e imparare a ignorare o bloccare comunicazioni indesiderate.

<i>Caratteristiche innovative</i>	Il modello di fiducia peer-to-peer è particolarmente efficace. L'apprendimento all'interno di una rete di pari, cioè altri senior, riduce drasticamente la barriera psicologica e l'ansia che gli adulti più anziani spesso sperimentano nei corsi IT formali e dal ritmo veloce.
<i>Link / riferimento</i>	https://www.jednotadochodcov.sk/
<i>Materiali visivi</i>	N/D

Valutazione dell'adattabilità di Erasmus+ project DIGITOL

<i>Criterio</i>	<i>Completamente</i>	<i>In certa misura</i>	<i>Per nulla</i>	<i>Commenti</i>
<i>a) Diversi gruppi target, ad esempio giovani, senior, professionisti</i>	☐	☒	☐	Il modello di supporto tra pari funziona meglio quando i partecipanti condividono età o esperienze di vita simili.
<i>b) Diverse organizzazioni, ad esempio ONG, scuole, autorità pubbliche</i>	☒	☐	☐	Altamente adattabile a centri comunitari, ONG locali e club per senior.
<i>c) Diversi temi o sfide, ad esempio privacy, disinformazione, cybersecurity</i>	☒	☐	☐	I seminari possono facilmente integrare nella discussione nuovi scenari di minaccia.

5. Smart Senior Academies at Regional Libraries

<i>Titolo della buona pratica</i>	Smart Senior Academies presso le biblioteche regionali
<i>Tipologia di buona pratica</i>	Formazione / Progetto
<i>Organizzazione e attuatrice</i>	Biblioteche pubbliche regionali, ad esempio Krajská knižnica Žilina, Slovacchia. https://www.krajskakniznicazilina.sk/
<i>Obiettivi principali</i>	Trasformare le biblioteche pubbliche in hub essenziali per l'educazione digitale degli adulti, insegnando ai senior la navigazione di base sui dispositivi e come valutare in sicurezza le informazioni online.

<i>Gruppo/i target</i>	Senior, adulti svantaggiati e membri della comunità locale.
<i>Risultati educativi e impatto</i>	I senior imparano a cercare informazioni in modo autonomo, gestire account email e riconoscere comunicazioni fraudolente. L'iniziativa favorisce un senso di indipendenza e integrazione nella moderna società digitale.
<i>Descrizione dell'attività e approccio metodologico</i>	Le biblioteche ospitano corsi strutturati "Smart Senior" di più settimane o sessioni di supporto IT a sportello. Bibliotecari e formatori IT volontari guidano piccoli gruppi attraverso esercitazioni pratiche. La metodologia è molto paziente e consente ai senior di esercitarsi sui computer della biblioteca o sui propri dispositivi, affrontando temi che vanno dall'accensione del dispositivo fino alla sicurezza avanzata su Internet.
<i>Caratteristiche innovative</i>	L'iniziativa utilizza in modo intelligente l'infrastruttura esistente, altamente affidabile e accessibile, delle biblioteche pubbliche per fornire educazione continua, gratuita e non intimidatoria agli adulti.
<i>Link / riferimento</i>	https://www.krajskakniznicazilina.sk/
<i>Materiali visivi</i>	Descrizioni dei corsi disponibili su: https://www.krajskakniznicazilina.sk/index.php/2023/10/19/digitalne-zrucni-seniori/

Valutazione dell'adattabilità di Smart Senior Academies at Regional Libraries

<i>Criterio</i>	<i>Completamente</i>	<i>In certa misura</i>	<i>Per nulla</i>	<i>Commenti</i>
<i>a) Diversi gruppi target (es. giovani, senior, professionisti)</i>	☒	☐	☐	Le biblioteche servono l'intera comunità e possono adattare i corsi a qualsiasi gruppo demografico.
<i>b) Diverse organizzazioni (es. ONG, scuole, autorità pubbliche)</i>	☒	☐	☐	Questo modello può essere replicato da qualsiasi istituzione pubblica dotata di spazi e computer.

c) <i>Diversi temi o sfide</i> (es. <i>privacy</i> , <i>misinformazione</i> , <i>cybersecurity</i>)	☒	☐	☐ Il curriculum può spostarsi dall'uso di base dell'hardware alla formazione avanzata anti-phishing.
---	-------------------------------------	--------------------------	--

5. Analisi dei risultati del questionario

5.1 Italia

Scopo e metodologia

Il questionario italiano è stato condotto nell'ambito dell'analisi nazionale dei bisogni, con l'obiettivo di raccogliere dati quantitativi sull'alfabetizzazione digitale, sulla consapevolezza in materia di sicurezza online e sull'esposizione alle frodi online tra gli adulti di età pari o superiore a 45 anni in Italia. Il questionario è stato somministrato online tramite Google Forms e diffuso attraverso diversi canali, al fine di garantire un'ampia partecipazione.

Inizialmente, il questionario è stato condiviso all'interno della rete dell'Associazione Italiana Socio-Educatori per la Cooperazione (AISEC APS), attraverso strumenti di comunicazione interna, tra cui scambi email e presentazioni durante le assemblee annuali dell'associazione. Inoltre, il questionario è stato diffuso attraverso i canali ufficiali di comunicazione di Confcooperative Lazio Nord, a cui AISEC è affiliata, mediante newsletter, circolari ed email dirette rivolte alla rete dell'organizzazione nelle province di Rieti, Viterbo e Roma.

Ai fini dell'analisi nazionale, sono state considerate esclusivamente le risposte provenienti da partecipanti residenti in Italia. Il campione finale era composto da 63 rispondenti di età pari o superiore a 45 anni, di cui 39 donne e 24 uomini. Il gruppo di età più rappresentato era quello 45–54 anni, con 28 rispondenti, seguito dal gruppo 65–74 anni, con 19 rispondenti, dal gruppo 55–64 anni, con 14 rispondenti, e dal gruppo 75+, con 2 rispondenti.

Dal punto di vista territoriale, i rispondenti provenivano da un'ampia area della regione Lazio, comprendente sia il Lazio settentrionale sia l'area metropolitana di Roma. Il campione era eterogeneo anche in termini di contesto abitativo, includendo aree urbane, rurali e semi-urbane, nonché diverse condizioni occupazionali e diversi background educativi. Tale diversità consente di offrire una panoramica complessiva delle esperienze, delle pratiche e dei bisogni percepiti dagli adulti di età pari o superiore a 45 anni nel contesto italiano.

Risultati principali

Il dataset italiano indica che gli adulti di età pari o superiore a 45 anni sono generalmente utenti attivi delle tecnologie digitali, sebbene il loro livello di fiducia vari a seconda del tipo di competenza considerata.

L'uso quotidiano dei dispositivi digitali risulta ampiamente diffuso: il 77,8% dei rispondenti ha valutato l'utilizzo quotidiano di smartphone o computer ai livelli più alti della scala, 4 o 5, con un punteggio medio di 4,19/5. Anche la fiducia generale nell'uso di Internet è relativamente elevata, con una media di 3,79/5, suggerendo che la maggior parte dei partecipanti si sente a proprio agio nello svolgimento di attività online di routine. Tuttavia, questa fiducia diventa meno solida quando si considerano competenze più specifiche di sicurezza digitale. I comportamenti auto-riferiti più forti riguardano le pratiche precauzionali di base nella navigazione quotidiana. Una larga maggioranza dei rispondenti ha dichiarato di evitare di cliccare su link sconosciuti o sospetti, pari al 73,0%, e di controllare le informazioni prima di condividerle online, pari al 71,4%; inoltre, il 60,3% ha dichiarato di bloccare o segnalare messaggi, profili o siti web sospetti. Questi risultati indicano la presenza di abitudini difensive di base sviluppate attraverso l'esperienza.

Allo stesso tempo, competenze più tecniche o specialistiche rivelano lacune evidenti. Meno della metà dei rispondenti, il 47,6%, ha dichiarato di essere in grado di identificare se un sito web è sicuro, ad esempio controllando la presenza del protocollo HTTPS o di indicatori di sicurezza. Analogamente, solo il 50,8% si sente sicuro nel modificare le impostazioni di privacy o sicurezza sui propri dispositivi, e la stessa percentuale ha dichiarato di utilizzare password forti e uniche. Risultati ancora più deboli emergono in relazione alla manutenzione di dispositivi e software: solo il 36,5% ha dichiarato di aggiornare regolarmente dispositivi, applicazioni e antivirus, mentre una quota significativa ha espresso incertezza su questo aspetto.

La criticità più rilevante riguarda il riconoscimento dei contenuti generati o manipolati tramite intelligenza artificiale. Solo il 38,1% dei rispondenti si è valutato positivamente nella capacità di identificare immagini, video o messaggi alterati, e meno della metà ha dichiarato di verificare regolarmente se un contenuto digitale possa essere stato manipolato. Questo conferma un significativo gap di competenza rispetto ai rischi digitali emergenti.

La consapevolezza delle frodi online è presente, ma non uniforme rispetto alle diverse tipologie di minaccia. I rischi tradizionali, come il phishing e la disinformazione sui social media, sono relativamente conosciuti: circa due terzi dei rispondenti hanno dichiarato una consapevolezza moderata o forte. La consapevolezza risulta leggermente inferiore per le truffe legate a falsi negozi online, frodi nei pagamenti o furto d'identità, e diminuisce ulteriormente quando si tratta di minacce basate sull'intelligenza artificiale. Solo il 54,0% dei rispondenti ha dichiarato una consapevolezza moderata o forte delle truffe generate tramite IA, mentre una quota consistente ha indicato una consapevolezza limitata o assente.

Anche l'esperienza diretta di frode risulta significativa. Più di un terzo dei rispondenti, pari al 38,1%, ha dichiarato di essere stato vittima di una qualche forma di frode digitale, principalmente frodi bancarie o finanziarie e truffe legate a falsi acquisti, seguite da phishing e furto d'identità. Ciò indica che l'esposizione ai rischi digitali non è solo percepita, ma anche vissuta concretamente.

La preoccupazione rispetto a una possibile futura vittimizzazione è particolarmente elevata: l'84,1% dei rispondenti ha espresso un chiaro livello di preoccupazione rispetto alla possibilità di diventare vittima di frodi online o misinformazione. Nel complesso, i risultati evidenziano un disallineamento tra l'uso digitale di routine e competenze più avanzate di sicurezza digitale.

Interpretazione

I risultati italiani confermano che un uso frequente del digitale non si traduce necessariamente in competenze efficaci di sicurezza digitale tra gli adulti di età pari o superiore a 45 anni.

Una prima questione chiave può essere descritta come una "illusione di competenza". Molti partecipanti fanno affidamento sull'uso abituale e sull'apprendimento esperienziale, sviluppando abitudini precauzionali di base, come evitare link sospetti o verificare informalmente le informazioni. Tuttavia, questa familiarità non è sostenuta da conoscenze strutturate, generando debolezze in aree quali il riconoscimento dei siti web sicuri, la gestione delle impostazioni di privacy, l'aggiornamento dei software e l'identificazione di contenuti manipolati o generati tramite intelligenza artificiale. Di conseguenza, gli utenti possono sovrastimare la propria capacità di muoversi in sicurezza negli ambienti digitali.

Una seconda vulnerabilità critica è legata all'evoluzione delle minacce online. La difficoltà nel riconoscere contenuti generati tramite IA segnala un cambiamento nel rischio digitale, in cui le strategie tradizionali di rilevazione diventano sempre più insufficienti. Ciò evidenzia un divario generazionale, poiché le forme emergenti di frode richiedono nuove forme di consapevolezza critica e tecnica.

I dati evidenziano inoltre una tendenza verso strategie informali e reattive di gestione dei problemi. Molti rispondenti si affidano all'intuizione, a comportamenti di evitamento o al supporto esterno — ad esempio chiedendo aiuto ai familiari — piuttosto che a strategie strutturate di prevenzione. Sebbene tali approcci possano offrire una protezione parziale, non sono sufficienti negli scenari più complessi e possono contribuire a generare insicurezza o un coinvolgimento limitato con i servizi digitali.

Allo stesso tempo, l'elevato livello di preoccupazione rispetto a una possibile vittimizzazione, combinato con la quota significativa di rispondenti che ha già sperimentato frodi, indica un forte bisogno percepito di supporto. I partecipanti appaiono consapevoli dei rischi, ma non dispongono degli strumenti necessari per gestirli in modo efficace.

Dal punto di vista dell'apprendimento, questi risultati evidenziano la necessità di interventi educativi mirati, pratici e accessibili. La formazione dovrebbe andare oltre la consapevolezza generale e concentrarsi sullo sviluppo di competenze concrete, tra cui il riconoscimento dei pattern fraudolenti, la verifica delle informazioni digitali, la gestione sicura dei dati personali e la risposta appropriata a situazioni sospette. Particolare attenzione dovrebbe essere dedicata ai rischi emergenti, soprattutto quelli legati all'intelligenza artificiale e ai contenuti manipolati.

Gli approcci educativi dovrebbero essere user-friendly e basati su scenari di vita reale, al fine di colmare il divario tra le pratiche digitali quotidiane e competenze di sicurezza più avanzate. Rafforzare la fiducia digitale in modo strutturato e informato sarà essenziale per sostenere gli adulti di età pari o superiore a 45 anni nella transizione verso un uso sicuro, autonomo e resiliente delle tecnologie digitali.

5.2 Spagna

Scopo e metodologia

Il questionario spagnolo è stato condotto nell'ambito dell'analisi dei bisogni di digiSAFE, con l'obiettivo di raccogliere dati quantitativi sulle abitudini digitali, sulla consapevolezza dei rischi online, sulle esperienze di frode online e sui fabbisogni formativi tra gli adulti di età pari o superiore a 45 anni. L'obiettivo era fornire evidenze comparabili tra i Paesi partner.

Il questionario è stato somministrato online e distribuito attraverso le reti di Asociación UNO, comprese associazioni locali e canali informali di apprendimento per adulti. La partecipazione è stata volontaria e anonima, nel pieno rispetto del Regolamento generale sulla protezione dei dati (GDPR).

Sono state raccolte almeno 50 risposte valide da partecipanti spagnoli di età pari o superiore a 45 anni, soddisfacendo i requisiti di comparabilità del progetto e garantendo l'affidabilità del dataset. Il campione includeva una lieve maggioranza di donne, pari al 58,8%. I rispondenti erano concentrati nelle fasce d'età 45-54 e 65-74 anni, con tutti i partecipanti di età superiore a 45 anni.

Il campione risultava relativamente istruito, con la maggior parte dei partecipanti in possesso di almeno qualifiche di istruzione secondaria o terziaria. Una quota significativa era costituita da pensionati, pari al 47,1%, mentre i restanti rispondenti erano lavoratori dipendenti o autonomi. Dal punto di vista territoriale, la maggior parte dei partecipanti viveva in aree urbane, con una quota minore residente in contesti rurali o semi-urbani. Nel complesso, il campione fornisce una panoramica rappresentativa di adulti di età pari o superiore a 45 anni digitalmente attivi in Spagna, riflettendo al contempo differenze nelle situazioni di vita e nei livelli di autonomia digitale.

Risultati principali

Il dataset spagnolo mostra che gli adulti di età pari o superiore a 45 anni sono attivamente coinvolti nell'ambiente digitale, in particolare in relazione alle attività quotidiane. La

maggior parte dei rispondenti ha dichiarato di utilizzare strumenti digitali quotidianamente, soprattutto per la comunicazione — applicazioni di messaggistica ed email —, l'online banking, i social media e l'accesso ai servizi pubblici.

Allo stesso tempo, i risultati rivelano vulnerabilità importanti. L'uso quotidiano complessivo dei dispositivi raggiunge un livello moderato, con una media di 3,29/5, mentre la fiducia generale nell'uso di Internet è leggermente inferiore, con una media di 3,00/5, e una quota considerevole di rispondenti dichiara un livello di fiducia limitato. Le risposte qualitative suggeriscono che molte persone si affidano a un supporto esterno — in particolare a familiari più giovani — quando incontrano difficoltà online, indicando un certo grado di dipendenza digitale piuttosto che una piena autonomia.

Le competenze digitali autovalutate risultano generalmente limitate in diverse aree chiave. Competenze di base, come il riconoscimento di siti web sicuri, mostrano livelli di fiducia relativamente bassi, con una media di 2,76/5, mentre competenze più tecniche, come la modifica delle impostazioni di privacy, la gestione di password sicure o l'identificazione di contenuti generati dall'intelligenza artificiale, rappresentano le aree più deboli. Inoltre, molti rispondenti hanno dichiarato incertezza nel distinguere messaggi legittimi da tentativi di phishing e nel sapere come rispondere correttamente in caso di sospetta frode.

La consapevolezza dei rischi online varia a seconda del tipo di minaccia. Le forme tradizionali di frode, come il phishing e le false offerte di investimento, sono relativamente ben riconosciute, e diversi rispondenti hanno riferito esperienze dirette con tali rischi. Al contrario, la consapevolezza delle minacce più recenti — in particolare quelle legate all'intelligenza artificiale, come deepfake o disinformazione generata tramite IA — è significativamente più bassa, con una quota rilevante di partecipanti che non conosce tali forme di inganno.

I comportamenti di sicurezza auto-riferiti mostrano un quadro misto. Le pratiche più intuitive, come evitare link sospetti o verificare le informazioni prima di condividerle, sono relativamente comuni. Tuttavia, comportamenti più tecnici e preventivi, come aggiornare regolarmente il software, gestire le impostazioni di privacy o verificare contenuti manipolati, sono adottati in modo meno costante. Ciò suggerisce che la consapevolezza di base non si traduce sempre in pratiche di protezione efficaci.

Le esperienze di frode digitale sono relativamente frequenti. Oltre un terzo dei rispondenti, pari al 35,3%, ha dichiarato di essere stato vittima di truffe online, principalmente phishing, acquisti fraudolenti e frodi finanziarie. Anche nei casi in cui non si è verificata una perdita economica, tali esperienze hanno contribuito a ridurre la fiducia negli ambienti digitali e ad aumentare l'incertezza nelle interazioni online.

La preoccupazione rispetto a una possibile vittimizzazione futura è particolarmente elevata, con oltre l'80% dei rispondenti che esprime livelli di preoccupazione moderati o forti. Allo stesso tempo, i partecipanti hanno mostrato un forte interesse per ulteriori percorsi formativi, in particolare in aree quali il riconoscimento e la prevenzione delle

frodi online, la protezione dei dati personali, la sicurezza nelle pratiche di online banking, l'identificazione della disinformazione e lo sviluppo di strategie pratiche per migliorare la sicurezza digitale nella vita quotidiana.

Nel complesso, i risultati evidenziano un divario tra un'ampia partecipazione digitale e competenze più avanzate di sicurezza digitale.

Interpretazione

I risultati spagnoli indicano un divario strutturale tra la partecipazione digitale e la capacità di gestire autonomamente i rischi online tra gli adulti di età pari o superiore a 45 anni.

Sebbene l'uso digitale di base sia diffuso, le conoscenze specifiche relative alla prevenzione delle frodi, alle pratiche di cybersecurity e al riconoscimento dei rischi restano limitate. Ciò crea una situazione in cui le persone sono attivamente coinvolte negli ambienti digitali, ma non pienamente attrezzate per navigarli in sicurezza, aumentando la loro esposizione sia alle minacce tradizionali sia a quelle emergenti.

Un elemento particolarmente rilevante è rappresentato dalla dipendenza dal supporto informale. Il frequente ricorso all'aiuto dei familiari, soprattutto delle generazioni più giovani, indica che molti adulti non si sentono pienamente autonomi nella gestione delle situazioni digitali complesse. Sebbene tale supporto possa essere utile, esso può anche rafforzare una dipendenza continuativa e limitare lo sviluppo di competenze personali e fiducia.

Un secondo aspetto critico riguarda il carattere disomogeneo dei comportamenti di sicurezza. I partecipanti adottano più facilmente pratiche intuitive, come evitare link sospetti, ma mostrano maggiori difficoltà nell'applicare comportamenti più tecnici o preventivi, come la gestione delle impostazioni di privacy, l'aggiornamento dei dispositivi o il riconoscimento di contenuti manipolati. Ciò suggerisce che la formazione dovrebbe concentrarsi non solo sulla consapevolezza dei rischi, ma anche sulla costruzione di routine pratiche e ripetibili.

La bassa familiarità con le minacce legate all'intelligenza artificiale rappresenta una vulnerabilità emergente. Deepfake, contenuti manipolati e disinformazione generata tramite IA possono risultare particolarmente difficili da individuare per persone che già sperimentano livelli moderati o bassi di fiducia digitale. Questo rende necessario integrare nei percorsi formativi esempi visivi, scenari realistici e strumenti semplici di verifica.

Dal punto di vista educativo, i risultati indicano la necessità di percorsi formativi accessibili, pratici e rassicuranti. Le attività dovrebbero utilizzare un linguaggio semplice, evitare spiegazioni tecniche eccessive e partire da situazioni quotidiane, come l'online banking, gli acquisti online, l'uso delle applicazioni di messaggistica e l'accesso ai servizi pubblici digitali.

La formazione dovrebbe inoltre rafforzare la capacità dei partecipanti di riconoscere segnali di rischio, verificare l'affidabilità delle informazioni, proteggere i propri dati

personali e sapere cosa fare in caso di sospetto incidente o frode. L'obiettivo non dovrebbe essere quello di generare paura, ma di aumentare autonomia, fiducia e capacità decisionale.

Nel complesso, il caso spagnolo conferma la necessità di un modello educativo non formale, basato su scenari reali, esercizi pratici e supporto graduale. Tale approccio può aiutare gli adulti di età pari o superiore a 45 anni a passare da una partecipazione digitale dipendente o incerta a un uso più autonomo, consapevole e sicuro degli strumenti digitali.

5.3 Slovacchia

Scopo e metodologia

Il questionario slovacco è stato condotto nell'ambito dell'analisi dei bisogni di digiSAFE, con l'obiettivo di valutare le abitudini digitali, la fiducia tecnica, la consapevolezza dei rischi online e le esperienze di frode digitale tra gli adulti di età pari o superiore a 45 anni. I dati raccolti sono destinati a orientare direttamente lo sviluppo del curriculum educativo e del toolkit per la sicurezza digitale del progetto.

La ricerca ha adottato un approccio quantitativo, utilizzando un questionario online standardizzato, progettato per garantire accessibilità e comparabilità tra i Paesi partner. Il questionario comprendeva una combinazione di domande basate su scale Likert e domande a scelta multipla, finalizzate a valutare aree chiave quali l'uso quotidiano di Internet, le competenze digitali auto-percepite, la consapevolezza sia delle minacce informatiche tradizionali sia di quelle emergenti, nonché le esperienze dirette di frodi online.

A livello transnazionale sono state raccolte complessivamente 131 risposte. Ai fini dell'analisi nazionale, il dataset è stato accuratamente filtrato per includere esclusivamente i rispondenti residenti in Slovacchia o in un altro Paese europeo, in linea con i criteri del progetto. Questo processo ha prodotto un campione finale di 51 risposte valide, raggiungendo la soglia minima richiesta per la comparabilità.

Il campione è composto principalmente da persone in fase professionale attiva o di pre-pensionamento: il 43% dei rispondenti ha un'età compresa tra 45 e 54 anni, il 35% tra 55 e 64 anni e il 22% ha 65 anni o più. Le donne rappresentano il 65% del campione. I partecipanti risultano relativamente istruiti, con la maggior parte in possesso di qualifiche di istruzione secondaria superiore o post-secondaria, e sono distribuiti in modo abbastanza equilibrato tra aree urbane, pari al 55%, e aree rurali, pari al 45%. Nel complesso, il campione riflette una popolazione digitalmente attiva, con caratteristiche socio-demografiche diversificate.

Risultati principali

Il dataset slovacco evidenzia un elevato livello di coinvolgimento digitale tra gli adulti di età pari o superiore a 45 anni, accompagnato da significative lacune nelle competenze di cybersecurity.

La connettività risulta particolarmente forte: il 92% dei rispondenti dichiara di utilizzare quotidianamente uno smartphone o un computer. Anche la fiducia generale nello svolgimento di attività online di base, come l'invio di email o gli acquisti online, è relativamente elevata, pari al 68%. Tuttavia, questo uso frequente non si traduce in una sicurezza tecnica effettiva.

Emergono debolezze importanti nelle competenze fondamentali di sicurezza digitale. Solo il 35% dei rispondenti si sente pienamente sicuro nel riconoscere se un sito web sia sicuro, ad esempio identificando protocolli HTTPS o indicatori di sicurezza. Analogamente, meno della metà dei partecipanti, pari al 41%, dichiara di essere in grado di modificare le impostazioni di privacy e sicurezza sui propri dispositivi. Questi risultati suggeriscono che, sebbene gli utenti siano operativamente attivi online, non dispongono delle competenze tecniche necessarie per gestire i rischi in modo autonomo.

Si osserva un divario evidente nella consapevolezza delle diverse tipologie di minacce informatiche. I rischi tradizionali sono ampiamente riconosciuti: l'85% dei rispondenti dichiara una consapevolezza moderata o forte rispetto a email di phishing, SMS fraudolenti e falsi negozi online. Al contrario, la consapevolezza delle minacce emergenti è significativamente più bassa. Un dato particolarmente rilevante è che il 78% dei partecipanti dichiara di essere solo leggermente consapevole o per nulla consapevole delle truffe generate tramite intelligenza artificiale, come deepfake o clonazione vocale. Analogamente, il 72% indica un basso livello di fiducia nella propria capacità di identificare media o contenuti informativi manipolati tramite IA.

Anche l'esperienza diretta di frode digitale è significativa. Un quarto dei rispondenti, pari al 25%, dichiara di essere stato vittima di truffe online. I modelli di risposta tra le vittime evidenziano un problema critico: la maggior parte si affida a reazioni informali, con il 62% che dichiara di aver cancellato il messaggio malevolo oppure di aver chiesto aiuto a familiari e amici. Solo una piccola minoranza, pari al 15%, ha segnalato formalmente l'incidente a banche, piattaforme online o autorità di polizia.

Nel complesso, i risultati indicano un forte squilibrio tra elevati livelli di attività digitale e limitata capacità di gestire sia i rischi online tradizionali sia quelli emergenti.

Interpretazione

I risultati slovacchi evidenziano un divario marcato tra coinvolgimento digitale ed effettive competenze di cybersecurity tra gli adulti di età pari o superiore a 45 anni.

Sebbene i rispondenti siano utenti frequenti e sicuri delle tecnologie digitali per scopi quotidiani, la loro capacità di gestire i rischi resta limitata. Questo crea un "confidence gap", cioè un divario di fiducia, in cui le persone possiedono le competenze operative necessarie per muoversi negli ambienti digitali, ma non dispongono delle conoscenze

tecniche richieste per garantire la propria sicurezza. L'adozione del digitale appare guidata principalmente dalla comodità e dalla necessità, piuttosto che da una comprensione complessiva dell'ecosistema digitale.

Una vulnerabilità chiave riguarda la rapida evoluzione delle minacce digitali. Sebbene i rispondenti dimostrino una solida consapevolezza delle forme tradizionali di criminalità informatica, come phishing o falsi negozi online, risultano significativamente meno preparati ad affrontare forme di frode più avanzate. La bassissima consapevolezza delle truffe generate tramite IA e la limitata capacità di identificare contenuti manipolati indicano un divario generazionale critico. Queste minacce emergenti si basano spesso sulla manipolazione psicologica e su trigger emotivi, rendendole più difficili da individuare attraverso strategie convenzionali.

Un altro aspetto importante riguarda le risposte comportamentali agli incidenti informatici. I dati rivelano un forte ricorso a meccanismi informali di gestione, come ignorare i messaggi sospetti o chiedere aiuto alla propria rete personale. Il tasso estremamente basso di segnalazione formale suggerisce sia una mancanza di conoscenza delle procedure ufficiali, sia la presenza di barriere psicologiche, tra cui imbarazzo, paura o senso di inevitabilità. Ciò limita l'efficacia dei meccanismi istituzionali di protezione e aumenta l'impatto a lungo termine delle frodi.

Dal punto di vista dell'apprendimento, questi risultati indicano la necessità di passare da una semplice partecipazione digitale a competenze di sicurezza digitale più strutturate e proattive. Gli interventi educativi dovrebbero dare priorità ad approcci pratici e basati su scenari, consentendo ai discenti di riconoscere e rispondere a situazioni reali, in particolare quelle che coinvolgono truffe sofisticate o guidate dall'intelligenza artificiale. Inoltre, la formazione dovrebbe includere indicazioni chiare e accessibili sulla configurazione delle impostazioni di privacy e sicurezza, nonché istruzioni passo dopo passo su come segnalare gli incidenti e cercare supporto istituzionale. Sarà inoltre essenziale affrontare la dimensione psicologica della criminalità informatica, normalizzando la vittimizzazione e riducendo lo stigma, al fine di incoraggiare comportamenti più proattivi e sicuri.

Rafforzare sia le competenze tecniche sia la fiducia degli utenti sarà fondamentale per sostenere gli adulti di età pari o superiore a 45 anni in Slovacchia nel passaggio da strategie passive o reattive a un coinvolgimento più autonomo, informato e resiliente nell'ambiente digitale.

6. Analisi transnazionale

Il confronto tra i risultati nazionali di Italia, Spagna e Slovacchia evidenzia una serie di convergenze significative, che rimandano a una sfida europea condivisa, insieme ad alcune differenze nazionali rilevanti, con implicazioni importanti per la progettazione di interventi educativi personalizzati.

6.1 Sfide comuni tra i Paesi

Tutti e tre i Paesi mostrano un divario coerente e strutturalmente significativo tra coinvolgimento digitale e competenze di sicurezza digitale. Gli adulti di età pari o superiore a 45 anni in Italia, Spagna e Slovacchia sono, in misura diversa, utenti regolari e attivi di Internet, utilizzando i servizi digitali per comunicare, effettuare operazioni bancarie, cercare informazioni e fare acquisti online. Tuttavia, in tutti e tre i contesti, la fiducia auto-percepita e le competenze effettive diminuiscono nettamente quando vengono valutate competenze più specifiche di sicurezza digitale: riconoscere siti web sicuri, gestire le impostazioni di privacy, mantenere aggiornati i software e trattare i dati in modo sicuro.

Un secondo pattern convergente è la debolezza quasi universale nel riconoscere contenuti generati o manipolati tramite intelligenza artificiale. In tutti e tre i Paesi, questa viene costantemente identificata come l'area di maggiore vulnerabilità tra i rispondenti, ben al di sotto della consapevolezza relativa alle minacce tradizionali, come il phishing o i falsi negozi online. Questo risultato è particolarmente urgente: le frodi basate sull'IA — deepfake, clonazione vocale, messaggi fraudolenti generati tramite IA — rappresentano la categoria di minaccia digitale in più rapida crescita, ma sono anche quella rispetto alla quale la popolazione 45+ in Europa risulta meno preparata.

Una terza sfida condivisa riguarda il ricorso a strategie informali e reattive di gestione del rischio. In Italia, Spagna e Slovacchia, molti rispondenti si affidano all'intuizione, alla prudenza o al supporto esterno dei familiari, piuttosto che a conoscenze e competenze strutturate. Questo approccio di "difesa informale" può ridurre alcuni rischi, ma è del tutto insufficiente di fronte a forme di inganno sofisticate e assistite dall'intelligenza artificiale. Inoltre, tende a rafforzare comportamenti di evitamento digitale, anziché costruire una reale resilienza.

Infine, tutti e tre i Paesi registrano livelli significativi di preoccupazione rispetto a una futura vittimizzazione — 84,1% in Italia, oltre l'80% in Spagna, e livelli elevati anche in Slovacchia — nonché tassi rilevanti di vittimizzazione pregressa: 38,1% in Italia, 35,3% in Spagna e 25% in Slovacchia. Il divario tra preoccupazione e competenza rappresenta una caratteristica costante del dataset transnazionale.

6.2 Principali differenze

Nonostante tali convergenze, esistono differenze significative tra i tre contesti nazionali. Italia e Slovacchia mostrano entrambe livelli molto elevati di coinvolgimento digitale quotidiano — rispettivamente il 77,8% e il 92% dei rispondenti ha valutato l'uso quotidiano dei dispositivi ai livelli più alti — mentre i rispondenti spagnoli mostrano modelli di coinvolgimento leggermente più moderati, con una media di utilizzo quotidiano dei dispositivi pari a 3,29/5. Ciò suggerisce che i rispondenti spagnoli, pur

essendo digitalmente attivi, potrebbero essere meno inseriti in routine digitali intensive rispetto ai loro omologhi italiani e slovacchi.

La natura delle minacce fraudolente predominanti varia a seconda dei contesti. In Slovacchia è stato documentato un modello di minaccia particolarmente grave e specifico: attacchi sofisticati di vishing, in cui i truffatori si fingono agenti di polizia o funzionari bancari per manipolare le vittime e indurle a trasferire denaro. Questa forma di ingegneria sociale sfrutta la fiducia nelle istituzioni in modi meno documentati nei contesti italiano e spagnolo. La Slovacchia affronta inoltre una sfida peculiare legata al volume e all'impatto delle campagne di disinformazione, amplificate dalla situazione geopolitica del Paese.

I tassi di segnalazione formale degli incidenti differiscono in modo marcato. I rispondenti slovacchi hanno mostrato un tasso di segnalazione formale allarmante, pari ad appena il 15% delle vittime che hanno formalmente segnalato gli incidenti, significativamente inferiore rispetto a quanto emerso nei contesti italiano e spagnolo. Ciò indica una più forte cultura della vergogna legata alla vittimizzazione in Slovacchia e/o una minore consapevolezza dei canali istituzionali di segnalazione: un'area specifica che richiede un intervento mirato.

L'Italia presenta un'infrastruttura istituzionale e programmatica più solida per l'inclusione digitale — Repubblica Digitale, CPIA, Programma GOL — rispetto alla Slovacchia, dove i programmi guidati a livello nazionale sono più recenti e hanno raggiunto un numero minore di persone. La Spagna occupa una posizione intermedia, con quadri nazionali solidi — INCIBE, Digital Spain 2026 — ma un'attuazione disomogenea tra le regioni.

6.3 Modelli comportamentali

In tutti e tre i Paesi, i rispondenti mostrano un modello comportamentale coerente: la fiducia nelle attività di routine ad alta frequenza — controllare le email, usare l'online banking, utilizzare app di messaggistica — coesiste con insicurezza e basse competenze nelle attività meno frequenti ma ad alto rischio, come verificare la sicurezza di un sito web, configurare le impostazioni di privacy o identificare contenuti manipolati. Questo modello suggerisce che l'abitudine digitale generi un falso senso di competenza complessiva, che però non si estende ai comportamenti critici per la sicurezza.

La fiducia negli strumenti digitali è generalmente moderata o elevata per piattaforme e servizi familiari e conosciuti, ma cala significativamente quando i partecipanti si trovano di fronte a fonti sconosciute, richieste insolite o situazioni ambigue. In tutti e tre i Paesi, i rispondenti tendono ad affrontare tale ambiguità attraverso l'evitamento — non cliccare, non interagire — piuttosto che tramite una verifica attiva. Si tratta di un approccio che riduce il rischio, ma non lo gestisce realmente.

L'esposizione al rischio risulta più elevata in Italia, con un tasso di vittimizzazione del 38,1%, seguita dalla Spagna, con il 35,3%, e dalla Slovacchia, con il 25%. Tuttavia, tali differenze possono riflettere in parte la diversa composizione dei campioni e i differenti

canali di diffusione del questionario. In tutti e tre i Paesi, le forme più comuni di frode subita sono di natura finanziaria — frodi bancarie, falsi acquisti, phishing — confermando che l'ambito finanziario rappresenta il principale terreno di danno.

6.4 Evidenze transnazionali dalle buone pratiche

In Italia, Spagna e Slovacchia, l'analisi delle buone pratiche rivela una serie di pattern comuni che superano i singoli contesti nazionali e mettono in luce approcci condivisi all'educazione alla sicurezza digitale per adulti di età pari o superiore a 45 anni.

In tutti e tre i Paesi emerge con forza l'attenzione all'apprendimento non formale e orientato alla pratica. Le iniziative raramente si basano esclusivamente su una didattica teorica; al contrario, privilegiano attività pratiche, scenari di vita reale e indicazioni passo dopo passo. Ciò riflette la necessità di tradurre i rischi digitali astratti in situazioni concrete e comprensibili per gli adulti in apprendimento. In Slovacchia, questo orientamento è particolarmente evidente nelle Smart Senior Academies ospitate dalle biblioteche pubbliche regionali, dove bibliotecari e formatori volontari guidano piccoli gruppi attraverso esercitazioni pratiche secondo i loro tempi, e nei seminari di base organizzati dall'Unione dei Pensionati (JDS), che si concentrano su minacce immediate e localmente rilevanti, come e-shop fraudolenti e false telefonate.

Molte buone pratiche adottano inoltre un approccio inclusivo e basato sulla comunità, attuato attraverso centri locali, associazioni o istituzioni pubbliche già familiari e considerate affidabili dal gruppo target. In tutti e tre i Paesi, gli ambienti di apprendimento sono progettati per essere accessibili e a bassa soglia, riducendo le barriere alla partecipazione e favorendo la fiducia dei discenti. Il modello decentralizzato slovacco — in particolare attraverso il programma Zrelí na dobu digitálnu del Fondo di dotazione Slovak Telekom, che indirizza finanziamenti direttamente a case di cura e centri comunitari — offre un esempio particolarmente replicabile di come l'erogazione a livello territoriale possa raggiungere senior isolati nelle aree rurali, che potrebbero non partecipare a corsi ampi e organizzati centralmente.

Un modello più visibile in Slovacchia rispetto agli altri due Paesi è il coinvolgimento attivo del settore privato nell'educazione digitale pubblica. Il portale Bezpečne na nete, creato dalla società di cybersecurity ESET, mostra come le competenze del settore privato possano essere trasformate in contenuti educativi gratuiti, costantemente aggiornati e accessibili al pubblico; si tratta di un modello che altri contesti europei potrebbero replicare attraverso quadri di responsabilità sociale d'impresa.

Accanto a queste convergenze, si osservano anche differenze significative. L'Italia mostra una maggiore integrazione tra strategie nazionali e iniziative multilivello, con azioni coordinate che collegano quadri di policy, programmi formativi e campagne di sensibilizzazione. La Spagna presenta un panorama più decentralizzato e variegato, nel quale un'ampia gamma di attori opera a livello nazionale, regionale e locale, talvolta senza un forte coordinamento tra loro. La Slovacchia si colloca in una posizione intermedia:

sebbene il suo quadro istituzionale sia robusto — coordinato da enti come NBÚ e MIRRI — la portata dei programmi formali tra le persone di età compresa tra 45 e 64 anni resta limitata, e le iniziative più efficaci tendono a essere non formali e guidate dalla comunità. Le evidenze complessive emerse nei tre Paesi partner conducono alla stessa conclusione: un'educazione efficace alla sicurezza digitale per adulti di età pari o superiore a 45 anni si basa su una combinazione di accessibilità, rilevanza pratica, apprendimento sociale e fiducia. Questi elementi rappresentano componenti trasferibili fondamentali che dovrebbero orientare direttamente lo sviluppo del curriculum e del toolkit digiSAFE.

7. Principali risultati

Dall'analisi transnazionale dei risultati delle ricerche nazionali emergono i seguenti principali risultati:

1. Il coinvolgimento digitale non equivale alla sicurezza digitale. In Italia, Spagna e Slovacchia, gli adulti di età pari o superiore a 45 anni sono utenti attivi e frequenti di Internet, ma mostrano costantemente competenze limitate nelle abilità specifiche di sicurezza digitale, come il riconoscimento di siti web sicuri, la configurazione delle impostazioni di privacy e la gestione della sicurezza degli account.
2. Le minacce basate sull'intelligenza artificiale rappresentano il gap più critico e universale. La consapevolezza e il riconoscimento delle truffe generate tramite IA, dei deepfake e dei media manipolati costituiscono le aree di competenza più deboli in tutti e tre i Paesi. Allo stesso tempo, questa è la categoria di minaccia online in più rapida crescita, rendendola la priorità più urgente per gli interventi educativi.
3. Le strategie informali di gestione prevalgono e sono insufficienti. La principale risposta comportamentale al rischio percepito nei tre campioni nazionali è informale, intuitiva e reattiva — evitamento, supporto familiare, cautela generale — piuttosto che strutturata e proattiva. Questo approccio offre una protezione inadeguata contro forme sofisticate di social engineering e frodi assistite dall'intelligenza artificiale.
4. I tassi di vittimizzazione pregressa sono elevati e sottostimati. Tra un quarto e quasi due quinti dei rispondenti al questionario nei tre Paesi hanno dichiarato di aver avuto esperienza diretta di frodi digitali, confermando che tali rischi non sono teorici, ma reali e immediati per il gruppo target.
5. La preoccupazione è elevata, ma non è accompagnata da competenze adeguate. In tutti e tre i Paesi, la grande maggioranza dei rispondenti — oltre l'80% — esprime una chiara preoccupazione rispetto a una futura vittimizzazione. Questo elevato livello di preoccupazione, combinato con i deficit di competenze riconosciuti, indica una domanda forte e non soddisfatta di formazione mirata.

6. La segnalazione formale degli incidenti è criticamente sottoutilizzata. Un pattern coerente nei tre Paesi — particolarmente marcato in Slovacchia — è la tendenza a gestire gli incidenti di frode in modo informale, senza segnalarli a banche, piattaforme o forze dell'ordine. Questa sotto-segnalazione limita le risposte sistemiche e lascia le vittime senza supporto istituzionale.
7. Il “confidence gap” è una vulnerabilità sistemica. In tutti e tre i Paesi, i rispondenti tendono a sovrastimare la propria sicurezza digitale complessiva sulla base di una buona padronanza delle attività di routine, sottovalutando invece la propria vulnerabilità specifica in situazioni ad alto rischio e meno familiari. Questa illusione di competenza richiede approcci educativi capaci di mettere in discussione le convinzioni esistenti e costruire una consapevolezza digitale realmente critica.
8. I quadri nazionali di policy esistono, ma la loro attuazione è disomogenea. Tutti e tre i Paesi hanno sviluppato quadri normativi rilevanti e programmi per le competenze digitali, ma la loro capacità di raggiungere il target 45+ resta limitata, in particolare in Slovacchia e nelle aree rurali di tutti e tre i Paesi.

8. Gap individuati e fabbisogni formativi

Sulla base della ricerca documentale, dell'analisi dei questionari e del confronto transnazionale, sono stati individuati i seguenti gap specifici e fabbisogni formativi per gli adulti di età pari o superiore a 45 anni in Italia, Spagna e Slovacchia. Sebbene diversi di questi gap siano comuni a tutti e tre i contesti, la loro intensità e modalità di manifestazione differiscono in modi direttamente rilevanti per la progettazione del curriculum.

8.1 Gap di competenze

In tutti e tre i Paesi emerge un divario significativo tra la frequenza con cui gli adulti di età pari o superiore a 45 anni utilizzano le tecnologie digitali e la loro effettiva capacità di gestire i rischi online. In Slovacchia, il 92% dei rispondenti ha dichiarato di utilizzare quotidianamente uno smartphone o un computer — un dato coerente con gli elevati livelli di connettività osservati in Italia e Spagna —; tuttavia, questa frequenza d'uso non si traduce in una conoscenza strutturata delle pratiche di sicurezza digitale. In Slovacchia, solo il 35% dei rispondenti si sente sicuro nel riconoscere un sito web protetto, e meno della metà, il 41%, dichiara di sapere come modificare le impostazioni di privacy e sicurezza sui propri dispositivi. Questo modello, che il report slovacco descrive efficacemente come “confidence gap”, è strutturalmente presente in tutti e tre i campioni nazionali, anche se appare più acuto in Spagna, dove il forte ricorso ai familiari come principale fonte di supporto digitale suggerisce una forma di dipendenza più che una reale autonomia digitale.

Più nello specifico, la capacità di verificare tecnicamente la sicurezza e l'autenticità degli ambienti digitali resta debole in tutti e tre i Paesi: identificare siti web sicuri, ad esempio attraverso indicatori HTTPS o icone del lucchetto, riconoscere gli indicatori di email di phishing, o distinguere SMS legittimi da SMS fraudolenti sono competenze che una quota significativa dei rispondenti non ha sviluppato. La gestione della sicurezza di dispositivi e account — inclusa la configurazione delle impostazioni di privacy, l'utilizzo di password forti e uniche, l'attivazione dell'autenticazione a due fattori e l'esecuzione regolare di aggiornamenti software e antivirus — è praticata da una minoranza e compresa da una quota ancora più ridotta. I rispondenti italiani appaiono leggermente più sicuri in alcuni comportamenti protettivi di routine, mentre i partecipanti spagnoli e slovacchi mostrano maggiore incertezza nell'applicare tali pratiche in modo costante.

8.2 Gap di conoscenza

Il gap di conoscenza più critico e universale nei tre Paesi riguarda il riconoscimento dei contenuti generati o manipolati tramite intelligenza artificiale. In Italia, questa è già identificata come una delle aree di competenza più deboli, con punteggi di autovalutazione costantemente bassi nell'identificazione dei rischi basati sull'IA. I dati slovacchi rafforzano questa evidenza con particolare chiarezza: il 78% dei rispondenti ha indicato di essere solo leggermente consapevole, o del tutto inconsapevole, delle truffe generate tramite IA, come deepfake e clonazione vocale, e il 72% ha ammesso una fiducia scarsa o nulla nella propria capacità di identificare media o notizie manipolati tramite IA. In Spagna, la consapevolezza di tali minacce è ancora meno sviluppata, con una quota significativa di rispondenti che dichiara scarsa o nessuna familiarità con le truffe legate all'intelligenza artificiale. Nei tre contesti, questo rappresenta il gap educativo più urgente: un gap che richiede una formazione dedicata e basata su scenari, piuttosto che una generica attività di sensibilizzazione.

Oltre alle minacce legate all'intelligenza artificiale, persistono significativi deficit di conoscenza riguardo ai meccanismi di social engineering e alle tattiche di manipolazione psicologica utilizzate dai criminali informatici. In Slovacchia, questo aspetto è aggravato da uno scenario di minaccia specifico e particolarmente dannoso: i truffatori si fingono frequentemente agenti di polizia o dipendenti bancari utilizzando tecnologie di spoofing del numero telefonico, sfruttando proprio quella fiducia nelle istituzioni che gli adulti più anziani sono più propensi ad accordare — un modello che la formazione formale non ha ancora affrontato in modo adeguato. Anche la conoscenza dei diritti in materia di protezione dei dati e delle procedure formali da seguire dopo un episodio di frode — a chi segnalare, quali opzioni di recupero esistono — risulta criticamente insufficiente in tutti e tre i campioni nazionali.

8.3 Gap di consapevolezza e risposta agli incidenti

Un ulteriore gap, costantemente presente ma con diversa intensità nei tre Paesi, riguarda la risposta agli incidenti e i comportamenti di segnalazione. Tra il 25% dei rispondenti slovacchi che aveva sperimentato una frode digitale, solo il 15% ha scelto di segnalare

formalmente l'incidente a una banca, a una piattaforma o a un'autorità di polizia. La maggioranza, pari al 62%, si è limitata a cancellare il messaggio malevolo oppure ha cercato aiuto informale da familiari o amici. Questo modello si riflette anche nei risultati italiani e spagnoli e rimanda a un insieme condiviso di barriere psicologiche: vergogna, imbarazzo e una percezione fatalistica della criminalità informatica scoraggiano attivamente le vittime dal rivolgersi ai sistemi istituzionali di supporto. Affrontare questa barriera richiede non solo indicazioni procedurali sui canali di segnalazione, ma anche un impegno deliberato a destigmatizzare la vittimizzazione all'interno dei programmi educativi.

A livello di consapevolezza generale, il gap più significativo riguarda le minacce emergenti. Le truffe basate sull'IA, i deepfake, la clonazione vocale e la disinformazione generata tramite IA sono categorie di rischio rispetto alle quali la maggior parte dei rispondenti nei tre Paesi ha una familiarità limitata o nulla. Esiste inoltre una più ampia mancanza di consapevolezza rispetto alle conseguenze concrete della vittimizzazione — finanziarie, sociali e psicologiche — che può contribuire a sottovalutare il rischio tra coloro che non sono ancora stati direttamente colpiti.

Nel complesso, il quadro comparativo tra Italia, Spagna e Slovacchia evidenzia l'importanza di progettare approcci formativi che siano al tempo stesso coerenti a livello transnazionale e adattabili ai bisogni specifici nazionali. La Slovacchia presenta una vulnerabilità particolarmente marcata rispetto alle minacce guidate dall'IA e allo sfruttamento della fiducia istituzionale; la Spagna mostra una maggiore dipendenza dalle reti informali di supporto; l'Italia riflette una base di fiducia tecnica leggermente più elevata, ma comunque fragile. Queste differenze indicano il valore di un quadro curricolare modulare, capace di affrontare i gap di competenza condivisi, consentendo al tempo stesso una contestualizzazione a livello nazionale.

9. Raccomandazioni per lo sviluppo del curriculum

Le evidenze raccolte nelle tre fasi di ricerca nazionale forniscono una base chiara e fondata su dati concreti per il Curriculum di educazione non formale (NFE) di digiSAFE. Le seguenti raccomandazioni riflettono i gap e i fabbisogni formativi individuati nella Sezione 8 e sono strutturate intorno agli ambiti fondamentali che dovrebbero essere affrontati dal curriculum.

9.1 Moduli tematici

Il curriculum è organizzato in una sequenza strutturata di componenti di apprendimento, composta da sei moduli principali, supportati da una fase iniziale di orientamento e da una fase finale di chiusura e pianificazione dell'azione.

La progettazione complessiva consente flessibilità nell'erogazione. Il curriculum completo può essere realizzato come workshop intensivo di 2 giorni, come serie di sessioni più brevi, oppure in formato blended, combinando elementi in presenza e online. Allo stesso tempo, ciascun modulo è progettato per funzionare come sessione autonoma della durata di circa 90 minuti, rendendo il curriculum adattabile a diversi ambienti di apprendimento e vincoli di tempo.

Questa struttura modulare garantisce che il curriculum possa essere al tempo stesso completo e flessibile, supportando sia l'erogazione dell'intero programma sia interventi mirati basati su bisogni locali specifici.

1. **Modulo 0: Orientamento e pre-valutazione.** Questo modulo introduttivo risponde ai diversi livelli di partenza in termini di fiducia digitale individuati in tutti i Paesi partner. La ricerca mostra che, sebbene molti adulti di età pari o superiore a 45 anni siano utenti digitali attivi, la loro consapevolezza dei rischi e le competenze auto-percepite variano in modo significativo. Questo modulo è essenziale per costruire fiducia, ridurre l'ansia iniziale e aiutare i partecipanti a riflettere sulle proprie abitudini digitali, sull'esposizione al rischio e sui propri bisogni di apprendimento prima di affrontare contenuti più tecnici.
2. **Modulo 1: Uso digitale quotidiano sicuro.** Questo modulo affronta direttamente il divario individuato tra uso frequente del digitale e limitata comprensione dei principi di sicurezza di base. In tutti i Paesi, i rispondenti hanno riportato alti livelli di coinvolgimento digitale quotidiano, ma hanno mostrato incoerenze nel riconoscere ambienti sicuri e nell'applicare comportamenti protettivi di routine. Il modulo supporta i discenti nell'identificare pratiche di uso sicuro, riconoscere segnali di affidabilità e sviluppare abitudini digitali quotidiane più consapevoli e sicure.
3. **Modulo 2: Phishing, smishing e pattern di truffa.** Questo modulo risponde agli elevati livelli di esposizione alle frodi online individuati nella ricerca. Nei tre Paesi, phishing, messaggi fraudolenti e truffe finanziarie sono risultati tra le minacce più comuni sperimentate dai rispondenti. I risultati evidenziano la necessità che i partecipanti imparino a riconoscere i pattern delle truffe, individuare segnali di allarme e sviluppare la capacità di fermarsi e valutare criticamente comunicazioni sospette prima di agire.
4. **Modulo 3: Pagamenti sicuri, shopping online e protezione finanziaria.** Questo modulo è giustificato dalla diffusa esperienza di frodi finanziarie e false offerte online emersa nei dataset. Molti rispondenti hanno segnalato difficoltà nel distinguere transazioni legittime da transazioni fraudolente, in particolare nell'ambito dello shopping online e dei pagamenti digitali. Il modulo si concentra sul rafforzamento di comportamenti finanziari più sicuri, aiutando i discenti a riconoscere piattaforme inaffidabili e ad applicare strategie decisionali più sicure.

5. Modulo 4: Privacy, password e protezione dei dispositivi. Questo modulo affronta debolezze ricorrenti nelle pratiche tecniche di sicurezza individuate in tutti i Paesi. La ricerca evidenzia una conoscenza limitata e un uso non costante delle impostazioni di privacy, delle password sicure e degli aggiornamenti software. Tali gap aumentano significativamente la vulnerabilità alle minacce informatiche. Il modulo si concentra quindi sul rafforzamento della protezione degli account e sulla promozione di routine pratiche di sicurezza quotidiana.
6. Modulo 5: IA, disinformazione e contenuti manipolati. Questo modulo risponde a uno dei gap più critici e trasversali individuati dalla ricerca: la limitata capacità di riconoscere contenuti generati tramite intelligenza artificiale e nuove forme di manipolazione digitale. In tutti i Paesi partner, la consapevolezza delle minacce basate sull'IA, come deepfake, clonazione vocale e media sintetici, è risultata significativamente inferiore rispetto alla consapevolezza dei rischi tradizionali. Il modulo mira a sviluppare il pensiero critico e le competenze di verifica necessarie per orientarsi in ambienti informativi digitali sempre più complessi.
7. Modulo 6: Cosa fare quando qualcosa va storto. Questo modulo affronta un gap rilevante nella conoscenza e nei comportamenti di risposta emerso dai dataset. Molti rispondenti hanno dichiarato incertezza su come reagire in caso di frode e si sono affidati principalmente a strategie informali, come ignorare l'incidente o chiedere aiuto ai familiari. I tassi di segnalazione formale risultano bassi. Il modulo si concentra quindi sulla definizione di percorsi chiari di risposta, sul miglioramento della fiducia nella gestione degli incidenti e sull'aumento della consapevolezza dei meccanismi di supporto disponibili.
8. Chiusura: Piano personale di sicurezza digitale. La componente conclusiva risponde alla necessità di tradurre l'apprendimento in un cambiamento comportamentale concreto. I risultati della ricerca mostrano livelli elevati di preoccupazione rispetto ai rischi digitali, ma strategie strutturate limitate per affrontarli. Questo passaggio finale supporta i discenti nel consolidare le conoscenze acquisite, definire azioni personali di sicurezza e aumentare la fiducia nella propria capacità di muoversi negli ambienti digitali in modo sicuro e autonomo.

9.2 Principi metodologici

I risultati della ricerca indicano chiaramente una serie di principi metodologici che dovrebbero guidare la progettazione del curriculum.

1. Apprendimento non formale ed esperienziale: il curriculum deve fondarsi su scenari di vita reale, casi studio ed esercitazioni pratiche, piuttosto che su un insegnamento teorico. Gli adulti di età pari o superiore a 45 anni rispondono meglio ad apprendimenti immediatamente applicabili alla loro esperienza digitale quotidiana.

2. Pratica basata su scenari: particolare attenzione dovrebbe essere dedicata a scenari simulati in cui i discenti possano esercitarsi in sicurezza nel riconoscere e rispondere a tentativi di frode, come email di phishing, chiamate sospette e messaggi generati tramite intelligenza artificiale, senza correre rischi reali.
3. Linguaggio e formato accessibili: i concetti tecnici di cybersecurity devono essere tradotti in un linguaggio chiaro e privo di gergo tecnico. Materiali visivi, guide passo dopo passo e contenuti multimediali dovrebbero essere utilizzati per supportare discenti con diversi livelli di alfabetizzazione.
4. Complessità progressiva: il curriculum dovrebbe essere strutturato in modo da costruire gradualmente la fiducia, partendo da rischi immediatamente riconoscibili e procedendo verso minacce più complesse ed emergenti. Questo approccio progressivo evita di sovraccaricare i discenti e riduce i comportamenti di evitamento digitale.
5. Destigmatizzazione della vittimizzazione: considerata la documentata riluttanza a segnalare formalmente gli episodi di frode, il curriculum dovrebbe affrontare esplicitamente gli aspetti psicologici della vittimizzazione da cybercrime, normalizzando l'esperienza e mettendo i discenti nelle condizioni di cercare supporto istituzionale senza vergogna.
6. Adattabilità ai contesti nazionali e locali: sebbene il quadro curricolare debba essere transnazionale, i moduli dovrebbero consentire adattamenti che riflettano le specifiche tipologie di frode, i quadri giuridici e i canali di segnalazione rilevanti in ciascun Paese partner.

10. Conclusione

Il Report transnazionale del progetto digiSAFE sintetizza i risultati delle ricerche nazionali condotte in Italia, Spagna e Slovacchia, fornendo un quadro completo e basato su evidenze delle sfide legate alla sicurezza digitale e dei bisogni di apprendimento degli adulti di età pari o superiore a 45 anni in tre Paesi europei.

Le evidenze sono chiare e coerenti: sebbene gli adulti appartenenti al gruppo target siano sempre più attivi negli ambienti digitali — utilizzando Internet per operazioni bancarie, comunicazione, servizi pubblici e informazione — essi non sono adeguatamente preparati ad affrontare i rischi online che tali attività comportano. Il divario tra partecipazione digitale e competenze di sicurezza digitale rappresenta una caratteristica strutturale di tutti e tre i contesti nazionali, non un fallimento individuale. Esso riflette il ritmo della trasformazione digitale, l'insufficienza dell'offerta educativa esistente rivolta a questa fascia d'età e la natura in rapida evoluzione delle minacce, in particolare l'emergere di frodi basate sull'intelligenza artificiale, che superano le attuali strategie di consapevolezza e difesa.

La ricerca ha individuato gap concreti e operativi: nelle competenze — verifica tecnica, sicurezza dei dispositivi, riconoscimento dei contenuti generati tramite IA —; nelle conoscenze — meccanismi di frode, diritti in materia di protezione dei dati, procedure di segnalazione —; e nella consapevolezza — minacce emergenti legate all'IA e canali istituzionali di supporto. Questi gap costituiscono l'input diretto per il Curriculum di educazione non formale di digiSAFE e per il Toolkit per la prevenzione delle frodi digitali, che saranno sviluppati nella fase successiva del progetto.

Le buone pratiche individuate nei tre Paesi dimostrano che interventi educativi efficaci, accessibili e basati sulla comunità, rivolti alla fascia di popolazione 45+, sono pienamente realizzabili. Iniziative che spaziano dalla rete italiana di facilitazione digitale ai seminari slovacchi di apprendimento tra pari, fino ai programmi spagnoli di mentoring digitale guidato da volontari, mostrano cosa funziona e forniscono modelli replicabili per gli output educativi di digiSAFE.

Costruendo direttamente sui risultati delle ricerche nazionali presentate in questo report, il progetto digiSAFE stabilisce un collegamento chiaro tra evidenze e azione. I gap, i bisogni e i pattern comportamentali individuati orienteranno direttamente la progettazione e la struttura del Curriculum di educazione non formale e del Toolkit per la prevenzione delle frodi digitali, garantendo che entrambi gli output siano fondati sui bisogni reali degli utenti. In questo modo, il progetto è in grado di offrire un contributo significativo e misurabile alla resilienza digitale degli adulti più anziani in Italia, Spagna, Slovacchia e oltre, sostenendo una partecipazione più sicura, informata e autonoma alla società digitale europea.

Bibliografia

1. Agency for Digital Italy (AgID) (n.d.). Digital Skills Initiatives. <https://www.agid.gov.it/it/agenzia/competenze-digitali>
2. Bank of Italy (n.d.). Financial Education and Cybersecurity Awareness. <https://economiepertutti.bancaditalia.it>
3. CERTFin (n.d.). I Navigati Campaign. <https://inavigati.certfin.it/index.html>
4. Civic Association eSlovensko (n.d.). Zdpovedne.sk. <https://www.zdpovedne.sk/>
5. Department for Digital Transformation, Italy (n.d.). Repubblica Digitale Strategy. <https://repubblicadigitale.gov.it/portale/strategia>
6. Digitálna koalícia (n.d.). Improving the Digital Skills of Seniors. <https://digitalnakoalicia.sk>
7. Digital Skills and Jobs Platform – European Commission (2024). Spain: A Snapshot of Digital Skills. <https://digital-skills-jobs.europa.eu/en/latest/briefs/spain-snapshot-digital-skills>

8. Digital Skills and Jobs Platform – European Commission (2024). Slovakia: A Snapshot of Digital Skills.
<https://digital-skills-jobs.europa.eu/en/latest/briefs/slovakia-snapshot-digital-skills>
9. ESET (n.d.). Bezpečne na nete. <https://bezpecnenanete.eset.com/sk/>
10. EU DisinfoLab (2023). Disinformation Landscape in Slovakia.
<https://www.disinfo.eu>
11. European Commission (2024). Slovakia 2025 Digital Decade Country Report.
<https://digital-strategy.ec.europa.eu/en/factpages/slovakia-2025-digital-decade-country-report>
12. European Commission (2025). Italy Digital Decade Country Report 2025.
<https://digital-strategy.ec.europa.eu/en/factpages/italy-2025-digital-decade-country-report>
13. European Commission – Joint Research Centre (2025). How to Reach the EU Target of 80% of Adults with Basic Digital Skills by 2030. https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/how-reach-eu-target-80-adults-basic-digital-skills-2030-2025-03-05_en
14. European Parliament and Council of the EU (2016). Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR). OJ L 119, 4.5.2016.
15. European Parliament and Council of the EU (2022). Directive (EU) 2022/2555 – NIS2 Directive.
16. Eurostat (2024). Digitalisation in Europe – 2024 Edition.
<https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2024>
17. Fundación Cibervoluntarios (n.d.). Digital Inclusion Programmes.
<https://www.cibervoluntarios.org>
18. Gobierno de España (2018). Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDgdd). BOE.
19. Gobierno de España (2021). Plan Nacional de Competencias Digitales.
<https://portal.mineco.gob.es>
20. Gobierno de España (2022). España Digital 2026 – Agenda Nacional de Transformación Digital. <https://espanadigital.gob.es/espana-digital>
21. INCIBE (2024). Los incidentes de ciberseguridad de 2023 gestionados por INCIBE.
<https://www.incibe.es>
22. INCIBE (n.d.). Línea de Ayuda en Ciberseguridad 017. <https://www.incibe.es/linea-017>
23. ISTAT (2024). Citizens and ICT Report.
https://www.istat.it/wp-content/uploads/2025/04/REPORT_CITTADINI-E-ICT_2024.pdf
24. ISTAT (2024). Digital Skills Statistics.
<https://www.istat.it/wp-content/uploads/2024/04/2.pdf>

25. ISTAT (2025). Crimes Against Persons and Property Report. Italian National Institute of Statistics.
26. Italian Data Protection Authority – Garante (n.d.). Personal Data Protection Code. <https://www.garanteprivacy.it>
27. Krajská knižnica Žilina (n.d.). Smart Senior Academies. <https://www.krajskakniznicazilina.sk/>
28. Ministerio de Educación y Formación Profesional, Spain (n.d.). Aula Mentor. <https://www.aulamentor.es>
29. Ministry of Investments, Regional Development and Informatization of the Slovak Republic – MIRRI (n.d.). Digitálni seniори Programme. <https://www.digitalniseniori.gov.sk>
30. Ministry of Labour and Social Policies, Italy (n.d.). GOL Programme. <https://www.lavoro.gov.it/temi-e-priorita/occupazione/focus/pagine/programma-gol>
31. National Cybersecurity Agency – ACN, Italy (n.d.). National Cybersecurity Strategy 2022–2026. <https://www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza>
32. National Security Authority – NBÚ, Slovak Republic (2021). National Cybersecurity Strategy 2021–2025. <https://www.nbu.gov.sk/national-cybersecurity-strategy-of-the-slovak-republic-for-years-2021-2025/>
33. OECD (2024). Enhancing the Digital Skills of Seniors in the Slovak Republic. <https://www.oecd.org/en/about/programmes/dg-reform/enhancing-the-digital-skills-of-seniors-in-the-slovak-republic.html>
34. Policía Nacional, Spain (n.d.). Plan Mayor Seguridad. https://www.policia.es/_es/colabora_plan_mayor_seguridad.php
35. Polizia Postale, Italy (n.d.). Annual Cybersecurity Reports and Data. <https://www.commissariatodips.it>
36. Repubblica Digitale (2025). Quarto rapporto di monitoraggio – Ottobre 2025. Department for Digital Transformation, Italy.
37. SafeHorizon Project (2026). Spain's Situation in the Cyberspace Domain. <https://www.project-safehorizon.eu>
38. Slovak Republic (2018). Act No. 18/2018 Coll. on the Protection of Personal Data. National Council of the Slovak Republic.
39. Slovak Republic (2018). Act No. 69/2018 Coll. on Cybersecurity. <https://www.sk-cert.sk>
40. Slovak Republic (2024). Act No. 366/2024 Coll. – Transposition of the NIS2 Directive. National Council of the Slovak Republic.
41. Slovak Telekom Endowment Fund (n.d.). Zrelí na dobu digitálnu. <https://nadacnyfondtelekom.sk/>
42. Union of Pensioners in Slovakia – JDS (n.d.). <https://www.jednotadochodcov.sk/>

