Paolo Attivissimo

Identità elettronica, scelta difficile

Il 7 marzo 2021 si voterà sulla legge che disciplina la cosiddetta "identità elettronica" (IE): una base giuridica che consente di creare strumenti semplici, garantiti dallo Stato, per dimostrare su Internet che siamo davvero chi diciamo di essere, per esempio per richiedere un certificato senza andare allo sportello, compilare automaticamente un formulario, aprire un conto, ottenere un finanziamento, fare un pagamento o accedere a servizi pubblici o privati riservati a specifiche categorie. L'IE non sostituisce il passaporto o la carta d'identità tradizionale. Il suo obiettivo è ridurre i costi, aumentare l'efficienza, diminuire le frodi, far circolare meno i nostri dati personali e facilitare chi ha problemi di accesso o mobilità. Molti altri stati europei hanno già da tempo strumenti analoghi, particolarmente popolari nei paesi nordici. Il 50% dei pagamenti in Norvegia avviene tramite IE; il 92% dei danesi usa l'IE abitualmente.

Il problema è decidere chi debba creare e far funzionare questi strumenti: la legge in discussione ne regola il funzionamento, ma prevede che la produzione e la gestione pratica delle app o dei dispositivi che permettono di usare l'identità elettronica vengano affidati ai privati, e questo suscita comprensibili preoccupazioni per possibili abusi o sfruttamenti commerciali. Molti preferirebbero che l'intero sistema venisse gestito dallo Stato.

Purtroppo ci si scontra subito con una realtà tecnica: gli Stati non hanno le risorse, esperienze e competenze necessarie per una gestione completa delle identità elettroniche, ben diverse da quelle convenzionali. La sicurezza, l'affidabilità e la riservatezza sono requisiti estremamente difficili da gestire su vasta scala nel mondo digitale. I veri esperti in questi settori sono le banche, che infatti già ora gestiscono le identità elettroniche all'estero con successo, sotto controllo statale. I paesi che hanno tentato la via interamente statale hanno avuto spesso problemi di frodi e accessi indebiti, facilitati dal fatto che tutti i dati dei cittadini erano centralizzati: è emblematico il caso del sistema statale indiano Aadhaar, con informazioni private in vendita nei bassifondi di Internet per pochi dollari e con abusi diffusi da parte dei funzionari.

La separazione fra Stato, che fa da garante e regolamentatore, e privati, che si occupano della parte pratica, ha il vantaggio tecnico di creare una barriera naturale contro gli abusi, sia commerciali sia governativi. In un sistema di identità elettronica ben fatto, ognuna delle parti vede soltanto i dati di cui ha bisogno per erogare il proprio servizio e non vede tutti gli altri. Le uova non sono tutte nello stesso paniere. Per esempio, lo stato non può creare dossier che raccolgano tutte le attività di un cittadino; un negozio online non può sapere quali altri acquisti ha fatto altrove il suo cliente; una farmacia sa che il cliente è autorizzato a ricevere un certo medicinale sensibile, ma non viene a sapere chi è e dove abita. Questo aiuta le persone vulnerabili a ottenere assistenza.

Un altro esempio: un sito Internet dedicato ai minori, uno spazio sicuro di gioco fra coetanei, può bloccare l'accesso agli adulti malintenzionati chiedendo che gli utenti usino l'identità elettronica. Il sito riceve dallo Stato soltanto l'informazione che l'utente è davvero minorenne, ma non riceve il suo nome e cognome o altri dati. È un metodo decisamente più rispettoso della privacy rispetto ai sistemi attuali commerciali, che raccolgono enormi quantità di dati personali e anzi basano il proprio successo economico proprio sulla profilazione meticolosa di ogni aspetto della vita dei loro utenti.

Tutto questo, però, è vero a una condizione: che il sistema di identità elettronica sia fatto bene. Di certo non può essere fatto bene se non ha una base giuridica, se non gode di una supervisione critica, severa e trasparente da parte dello Stato e se non ha la fiducia dei cittadini. La votazione del 7 marzo permette appunto di scegliere se gettare queste basi e cominciare a costruire bene l'identità elettronica oppure restare fermi al sistema attuale, che spesso dipende da una password appiccicata su un Post-It, dissemina fotocopie dei nostri documenti d'identità completi e mortifica chi non può muoversi agevolmente.

Istockphoto

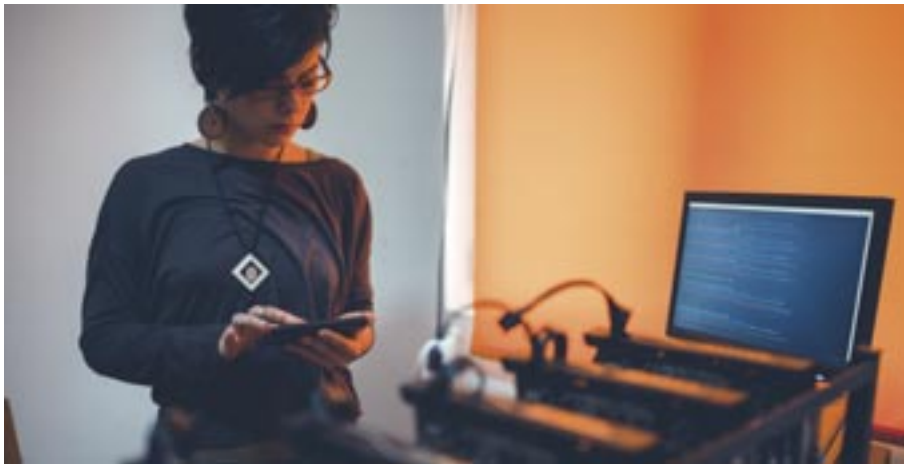
Consigli ACSI

- L'identità elettronica non è obbligatoria; si affianca ai metodi di identificazione tradizionali senza sostituirli.
- L'IE può essere integrata per esempio in un telefonino oppure in una semplice tessera o in una chiavetta USB: la legge non prescrive la tecnologia, ma solo gli standard che deve rispettare. Questo consente di creare strumenti di IE adatti a tutti i livelli di competenza tecnologica degli utenti.
- Le identità digitali che già abbiamo (account su Google o Facebook o simili) possono restare separate dall'IE garantita dallo Stato e rimane possibile usare pseudonimi o essere anonimi.

Paolo Attivissimo

Disseminati **i dati dei social network**, cosa si rischia

I dati di oltre 500 milioni di utenti di Facebook sono stati disseminati su Internet: includono nome, cognome, situazione relazionale, data di nascita, indirizzo di casa, luogo di lavoro e numero di telefono. In Svizzera gli utenti coinvolti sono circa 1,6 milioni. Anche Donald Trump e lo stesso Mark Zuckerberg, cofondatore di Facebook, sono fra le vittime. Anche i dati di mezzo miliardo di utenti di LinkedIn, sito dedicato alla ricerca di lavoro, sono stati rastrellati e poi pubblicati su Internet. Analoga sorte è successa a un milione e trecentomila utenti del social network Clubhouse.



Mentre i dati carpiti a Facebook sono in molti casi riservati, quelli sottratti a LinkedIn e a Clubhouse sono pubblici: chiunque potrebbe trovarli consultando i rispettivi siti. Ma allora dove sta il problema? Cosa può succedere a chi è stato coinvolto in queste raccolte di massa?

Nel caso di Facebook, il problema comportato dalla violazione delle promesse di riservatezza è evidente; il pericolo principale è che i numeri di telefono possono essere usati per molestie e per tentativi di furto d'identità. È particolarmente a rischio chiunque sia vittima di partner o ex partner violenti oppure di molestatori o pettegoli di vario genere. Chi ha cambiato numero di telefono per sottrarsi a questo tipo di situazione e lo ha usato per il proprio profilo Facebook rischia di vedersi ricontattato dai suoi persecutori e di dover cambiare numero ancora una volta.

Più in generale, chi ha affidato a Facebook (e a WhatsApp e Instagram, che condividono dati con Facebook) un numero di telefono che voleva tenere confidenziale farebbe bene a presumere che quel numero non sia più riservato e che chiunque possa associarlo al suo nome. Se questo è un problema, è opportuno procurarsi un nuovo numero di telefono da tenere riservato, lasciando però su Facebook quello ormai diventato pubblico.

Per quel che riguarda LinkedIn e Clubhouse, anche se i dati rastrellati erano comunque già consultabili, il fatto di averli radunati in un unico archivio consente di fare ricerche rapide e di massa, e di incrociare questi dati con quelli di Facebook per profilare in grande dettaglio le persone. Questa profilazione facilita e rende molto più credibili i tentativi di commettere reati come il furto di password o di identità: l'impostore non fa fatica a impersonare le vittime perché ha tutti i loro dati personali. Malviventi o molestatori possono così prendere il controllo di conti correnti, accedere a foto private o ficcare profondamente il naso nella vita privata dei loro bersagli, causando equivoci e interferenze molto pesanti. Il movente può essere il denaro oppure una vendetta personale.

I rimedi, purtroppo, sono pochi ma sono semplici: chiudere e far cancellare i propri profili sui social network, se possibile, o almeno riempirli di dati di fantasia. Anche se le password non sono state sottratte, è prudente cambiarle, usandone una differente per ciascun servizio, e proteggere i propri account non con il solito SMS di verifica (che grazie a questi furti di dati può essere imitato o intercettato) ma con i numeri generati dalle cosiddette "app di autenticazione", come Authy o Google Authenticator; le istruzioni per farlo sono sui siti dei rispettivi social network.

Incidenti come questi dimostrano ancora una volta che nonostante tutte le loro rassicurazioni, i social network non sono buoni custodi dei nostri dati personali e quindi non è opportuno affidarglieli. Ma per molte persone sono un canale di comunicazione importante con amici e famiglia, soprattutto in questo periodo in cui i contatti sociali sono limitati; se non è praticabile eliminare i profili social, perlomeno si possono modificarne i dati, togliendo quelli sensibili o sostituendoli con altri fittizi (compreso il nome e cognome e la foto nel profilo). Il regolamento di Facebook chiede di usare nomi e cognomi veri, ma la necessità di tutelare la propria sfera privata è più importante delle regole di un social network. Io, per esempio, sono su Facebook da anni con un nome finto e non se n'è ancora accorto nessuno dei sorveglianti dell'azienda di Zuckerberg. Nonostante il mio nome di fantasia includa proprio la parola Fittizio.

Consigli ACSI

- Consultate Haveibeenpwned.com per sapere se il vostro numero di telefono è fra quelli resi pubblici: basta immetterlo con prefisso internazionale ma senza 00 iniziale (il "+" non è necessario e viene ignorato).
- Attenzione a eventuali prese di contatto, sui social network o al telefono, da parte di sedicenti banche, casse malati, parenti e amici: potrebbero essere impostori che cercano di farsi i fatti vostri per truffarvi o ficcare il naso.
- Verificate l'identità delle persone chiamandole al loro numero di telefono: quello che avete voi in rubrica, non quello dal quale vi chiamano.

Computer **Apple**, occhio all'etichetta

Paolo Attivissimo

Se state pensando di acquistare un computer della Apple, fate molta attenzione all'indicazione del tipo di processore, per esempio sull'etichetta o sulla confezione: da qualche mese, infatti, questi computer sono disponibili in due versioni esternamente molto simili ma internamente assai differenti. Il rischio, se acquistate la versione non adatta alle vostre esigenze, è che le applicazioni che desiderate usare non funzionino.

Nel centro commerciale nel quale sono andato ad acquistare di recente un Mac è successo proprio questo: il cliente che mi precedeva ha restituito un accessoriatissimo laptop Apple perché non riusciva a farlo funzionare come serviva a lui, come invece aveva sempre fatto con i sui Mac precedenti.

I due tipi di processore dei Mac odierni sono quello classico, fabbricato da Intel, e quello nuovo, denominato M1 e progettato da Apple. L'M1 offre prestazioni superiori: maggiore velocità e potenza con minore consumo energetico. Le elaborazioni sono più rapide, specialmente per video e foto. Nei modelli portatili, inoltre, la batteria dura molto più a lungo e il computer si scalda parecchio meno. In aggiunta, su questi computer funzionano anche quasi tutte le app dell'iPhone e iPad. Infine, cosa non trascurabile, i modelli Apple con processore M1 costano meno di quelli che usano ancora i processori Intel.

Ma tutti questi vantaggi hanno un prezzo non strettamente monetario: infatti non tutte le applicazioni per computer Apple sono compatibili con i processori M1. Quelle più popolari e recenti sono già disponibili in edizioni apposite, per cui se volete usare l'ultima versione di Microsoft Office o Photoshop, per esempio, non avrete problemi. Apple ha inoltre installato in questi computer un convertitore (denominato Rosetta 2) che "traduce" le applicazioni non realizzate appositamente. Risultato: quasi tutte funzionano senza problemi e anche molto velocemente, ma se usate qualche applicazione insolita e non recente, specialmente per montaggi video o per giochi o fatta su misura per la vostra azienda, oppure volete collegare qualche apparecchiatura esterna non molto diffusa, potreste scoprire che neppure il "traduttore" di Apple riesce a farla funzionare su questi nuovi computer.

Un esempio molto vistoso di questa incompatibilità è Windows. Molte persone comprano un Mac e poi vi installano Windows, da solo o in "coabitazione" con macOS. Ma sui Mac dotati di processore M1, Windows non funziona. Più precisamente, è necessario procurarsi una versione speciale di Windows, denominata Windows 10 on Arm, tramite una procedura decisamente complicata e senza garanzie. Anche così, purtroppo, alcune applicazioni Windows rischiano di non funzionare. Era proprio questo il problema del cliente citato sopra.

Infatti la differenza fra i due tipi di processore non è semplicemente la potenza: è la cosiddetta "architettura". In parole povere, i computer Apple con M1 e con Intel sono come le auto diesel o a benzina: quasi uguali fuori, ma completamente differenti sotto il cofano. Sbagliare processore è un po' come sbagliare carburante: le conseguenze sono dolorose.

L'alternativa è acquistare un computer Apple tradizionale, ossia dotato di un processore Intel: in questo modo i problemi di compatibilità spariscono, ma si perdono tutte le prestazioni migliorate offerte dai nuovi processori M1 e si spende parecchio di più (per contro diventa possibile installare più memoria e avere schermi più grandi).

Inoltre c'è, a lungo termine, il problema che Apple intende abbandonare i processori Intel in favore degli M1, col risultato che fra qualche anno chi ha un Mac con processore Intel potrebbe avere difficoltà a trovare versioni aggiornate delle applicazioni.

La decisione, insomma, non è semplice: con M1 si è a prova di futuro ma si rischia nel presente; con Intel si è al sicuro nel presente ma si rischia per il futuro.

Consigli ACSI

- Chiedete al negoziante e controllate bene sulla confezione il tipo di processore, oppure guardate attentamente le specifiche tecniche sul sito di vendita online, specialmente nel caso di offerte speciali.
- I Mac M1 costano meno dei Mac Intel, ma includete nel bilancio la spesa per le versioni aggiornate e compatibili delle applicazioni che potrebbero essere necessarie.
- I laptop Apple hanno sempre meno connettori esterni: probabilmente vi servirà acquistare una serie piuttosto costosa di adattatori.

Informatica per restare **autosufficienti**

Paolo Attivissimo

Incidenti, malattie e invecchiamento possono ridurre le capacità motorie e cognitive di una persona, ma la tecnologia informatica può compensare almeno in parte questa riduzione, consentire una migliore qualità della vita, mantenere più a lungo l'autosufficienza e facilitare l'assistenza domiciliare.

A volte si tratta di tecnologia tutto sommato banale: un tablet o un telefonino che consente una videochiamata diventa importantissimo per poter mostrare i volti dei familiari a chi ha difficoltà nel riconoscere le voci e a ricordare le facce. Molti degli orologi "smart" oggi disponibili includono sensori che rilevano cadute e possono chiamare i soccorsi.

Gli altoparlanti dotati di assistenti vocali, come Alexa o Google Home/Nest, sono molto più facili da usare rispetto ai computer, proprio perché si comandano con la voce, senza dover maneggiare mouse o tastiere; permettono di impostare promemoria e aiutano a rispondere, con incrollabile pazienza, alle domande spesso ripetitive che caratterizzano alcune difficoltà cognitive o visive. Per chi ha perso la capacità di leggere un orologio o un calendario, avere una voce alla quale chiedere per esempio che ore sono o che giorno è tutte le volte che vuole, sapendo di non dare fastidio, è un conforto notevole.

Ma la tecnologia consente ben di più: si possono installare piccoli sensori che rilevano fumo, temperatura, acqua a terra, fughe di gas, aperture di porte o finestre, frigoriferi lasciati aperti, presenza a letto e possono avvisare telefonicamente i familiari.

Uno dei problemi principali è non eccedere nella sorveglianza, che sminuisce la persona, ed evitare i falsi allarmi o gli allarmi mancati: per questo le telecamere, che potrebbero a prima vista sembrare una soluzione facile ed efficace, sono invece spesso sconsigliate. Al loro posto si possono installare sensori che non raccolgono immagini ma si limitano a rilevare movimenti e presenze, allertando soltanto in caso di attività fuori dagli orari e ambienti abituali, preservando la sfera privata. I loro dati, inoltre, possono essere analizzati da programmi di intelligenza artificiale per notare se rivelano anomalie o cambiamenti nelle abitudini nel corso del tempo.Questi ausilii tecnologici, benefici sia per l'assistito sia per chi fornisce assistenza, vanno sotto vari nomi: tecnologie assistive intelligenti, gerontecnologia o Ambient Assisted Living. Il loro compito è complementare, ma non sostituire, il lavoro assistenziale dei familiari e dei professionisti del settore.

Oltre alle soluzioni per il monitoraggio e la sicurezza, l'informatica offre alle persone con disabilità anche strumenti di stimolo per le funzioni cognitive e il movimento fisico: app che presentano foto di famiglia e chiedono, sotto forma di gioco, di ricordare come si chiamano le persone ritratte oppure altri dettagli delle loro vite; app che leggono ad alta voce i testi inquadrati dal tablet o smartphone; e app che usano speciali pedane per rilevare i passi, lo spostamento del peso e il bilanciamento durante attività fisiche, come il dispositivo Senso sviluppato da Dividat, uno spinoff dell'ETH di Zurigo, i cui primi risultati sperimentali indicano un rafforzamento di attenzione, concentrazione, memoria e orientamento. Anche l'iHome Lab dell'Università di scienze applicate e arti di Lucerna (hslu.ch) è molto attivo in questo campo, con progetti come l'assistente digitale Anne, che è un tablet progettato specificamente per facilitarne l'uso a persone con difficoltà cognitive, che lo usano per restare in contatto audio-video con le famiglie e i prestatori di assistenza e per ricevere promemoria vocali di scadenze e appuntamenti; a differenza degli assistenti digitali commerciali, Anne gestisce tutti i dati localmente e anche il suo riconoscimento vocale non richiede l'uso di servizi esterni, rispettando quindi maggiormente la privacy. Lo stesso iHome Lab ha sviluppato iWalkActive anche un deambulatore "smart", dotato di motore elettrico e di sistema di navigazione per interni ed esterni, nonché di grandi ruote e di componenti resistenti alle intemperie che lo rendono utilizzabile anche in ambienti sconnessi.

L'obiettivo di tutte queste tecnologie è consentire di mantenere il più a lungo possibile indipendenza e libertà di movimento: due ingredienti di dignità e benessere che sono sempre più preziosi in una società che invecchia.

Consigli ACSI

- È essenziale coordinarsi con uno specialista in campo medico prima di adottare qualunque tecnologia assistiva per sé o per altri.
- Le persone con difficoltà visive, motorie o cognitive hanno bisogno di app e dispositivi con icone e tasti grandi e non numerosi.
- Per chi vuole creare app, siti o risorse per queste esigenze è importante rispettare le regole di semplicità e chiarezza descritte dalla guida disponibile presso www.navigazionefacile.ch.
- Il sito dell'Ufficio federale per le pari opportunità delle persone con disabilità è ricco di spunti, riferimenti, documenti e contatti (www.edi.admin.ch >ufpd).

Aiuto, mi sono **consumerizzato**!

Paolo Attivissimo

Se rispondete ai messaggi WhatsApp di lavoro sul vostro telefonino o sul vostro computer di casa, che magari è più potente e aggiornato di quello che avete in ufficio, e anzi portate in ufficio il vostro computer e smartphone personali, anche voi siete consumerizzati. Non vi preoccupate, non è necessariamente una brutta cosa.

La consumerizzazione informatica o IT consumerization è appunto l'uso dei dispositivi tecnologici personali per scopi lavorativi, ma è anche la trasformazione delle tecnologie nate per uso aziendale in prodotti per i consumatori. Al loro debutto parecchi decenni fa, le prime calcolatrici elettroniche tascabili erano strumenti costosi, giustificabili solo per ragioni di lavoro o di studio; oggi sono un'app gratuita nell'angolino dello schermo del telefonino. Computer e telefoni mobili sono nati nel mondo del lavoro e poi, crollando man mano di prezzo, sono diventati accessibili ai consumatori, che ne hanno influenzato il design e le funzioni. Quest'influenza è poi tornata nelle aziende, cambiando il modo di lavorare. Per esempio, oggi un sistema di mail o messaggistica aziendale è sempre più raro e ci si appoggia a servizi nati per i consumatori, come Gmail, Google o WhatsApp.

Questa è una delle tendenze economiche e tecnologiche più importanti degli ultimi due decenni, secondo gli esperti di Gartner*: per i consumatori e lavoratori ha portato parecchi vantaggi, ma anche alcuni effetti collaterali poco evidenti.

In passato era l'azienda a fornire gli strumenti di lavoro, ma questo spesso significava trovarsi a lavorare con telefoni, fotocopiatrici, stampanti, computer e programmi vecchi e scontrarsi con la burocrazia di un ufficio acquisti lento e riluttante, al quale bisognava giustificare ogni minimo acquisto tecnologico; oggi, invece, il mondo del lavoro incoraggia il cosiddetto BYOD, bring your own device, ossia "porta (in ufficio) il tuo dispositivo (privato)". Il dipendente è contento, perché si sceglie da solo lo smartphone, il tablet, la stampante, il mouse o il computer che preferisce per lavorare; se li compra e li sostituisce quando vuole, senza sottostare a procedure complicate; ci installa le app che vuole e che sa usare per lavorare più efficacemente; inizia a scrivere un documento in Google Docs sul telefonino a casa e lo completa sul computer in ufficio, invece di appoggiarsi al sistema informatico aziendale che non è altrettanto flessibile.

Ma la consumerizzazione significa, appunto, che è il (o la) dipendente a pagare per gli strumenti di lavoro. L'azienda, invece, risparmia, e spesso non trasferisce questo risparmio al dipendente, che in sostanza sovvenziona il datore di lavoro. Inoltre l'uso dello strumento personale, in particolare del telefonino, rende molto più facile estendere il lavoro anche fuori dall'ufficio e dagli orari consueti. La recente tendenza al lavoro da casa ha annacquato ulteriormente i confini fra attività professionale e vita privata.

E naturalmente se si guasta il computer o se il bimbo intinge lo smartphone nella fondue o cancella per errore i documenti di lavoro dal tablet giocandoci a Peppa Pig o Fortnite, i disagi e i costi sono a carico del lavoratore. Ci sono questioni delicate anche per i datori di lavoro che adottano questo approccio: gli addetti informatici aziendali possono avere maggiori difficoltà a fornire assistenza a dispositivi eterogenei che non conoscono (con i classici rimproveri "ma su Windows funziona!" o "ma sull'iPhone basta fare così"). C'è la questione della sicurezza informatica, se i dispositivi usati promiscuamente dai dipendenti vengono collegati alla rete aziendale. Non da ultimo, chi lavora con metodi, app e dispositivi non selezionati e certificati dall'azienda potrebbe violare le regole interne e le leggi sulla protezione dei dati personali.

Nel complesso, però, i benefici superano gli svantaggi: la consumerizzazione rende più efficienti, flessibili e competitivi e rende più agile e piacevole il lavoro grazie ad app e dispositivi scelti personalmente e su misura. Ma attenzione ai costi occulti. E alla fondue.

Pixabayphoto

Consigli ACSI

- Separate il più possibile le attività digitali personali da quelle di lavoro, usando dispositivi o almeno profili e account distinti (per esempio Firefox per lavoro, Chrome per la vita privata), installate un antivirus anche sugli smartphone e tablet Android e usate dispositivi e app aggiornati.
- La sicurezza diventa doppiamente importante: usate password difficili e sempre differenti e proteggetevi attivando l'autenticazione a due fattori (le istruzioni sono su Google).
- Creare e condividere documenti online con Google Docs e simili è comodo ma aumenta il rischio che i criminali possano intercettare dati sensibili.
- Le aziende devono investire nel rendere attenti i dipendenti al rischio che un'app scaricata o un clic su un link