Dipartimento della Gioventù – POAT Per la Gioventù - CUP J71I09000020007

Supporto allo sviluppo della sicurezza e legalità informatica nell'ambito delle iniziative rivolte ai giovani

Michele Crudele - 2011-10-06

B.1.a) Linee guida sulla tutela dell'identità digitale - Guida operativa

Scenario

Identità digitale indica l'insieme di informazioni che fanno riferimento a una persona fisica e sono pubblicate in rete, in forma leggibile a tutti oppure riservata al proprietario e a chi autorizzato. Si mostra sotto tre aspetti: la digitalizzazione dei dati personali, che consentono di identificare una persona in modo facile e sicuro; gli strumenti utilizzati per esprimere la propria identità e per partecipare alle attività; le possibili rappresentazioni di sé stessi.

Si tratta di aspetti che intersecano altri concetti come quello di "cittadinanza digitale", riferito in particolare agli strumenti di partecipazione alla vita pubblica e di espressione democratica attraverso Internet, condizionati dal cosiddetto *digital divide*, che non vede tutti ugualmente in condizione di utilizzare le risorse di rete.

È più corretto parlare di identità digitale piuttosto che di identità virtuale, perché ha sempre conseguenze reali sulla persona. A volte però il termine virtuale vuole sottolineare la differenza radicale tra l'identità reale e quella esposta in rete. Non è infatti infrequente una dissociazione – anche con la rappresentazione di molteplici identità – determinata da motivazioni diverse: anonimato per discrezione o autodifesa, frustrazione, esibizionismo, gioco, indagine. I cosiddetti "nativi digitali", cioè ragazzi che hanno iniziato da piccoli a utilizzare Internet, hanno un'identità digitale multiforme e ricca, ma anche più fragile e vulnerabile, perché soggetta a manipolazione o falsificazione, rispetto alle identità reali dei loro coetanei di epoche precedenti.

Come nell'identità reale anche in quella digitale esistono forme autodeterminate di rappresentazione della stessa (cosa voglio mostrare di me agli altri) e forme eterodirette (ciò che gli altri pensano o dicono di me). Queste ultime possono essere il frutto di informazioni indirette messe in relazione per costruire un profilo dettagliato di una persona, anche rilevando aspetti che l'interessato non ha mai voluto dichiarare pubblicamente. Esistono su Internet servizi di aggregazione automatica che raccolgono tutto ciò che è disponibile su una persona di cui si conosce nome e cognome. In questo modo si può, per esempio, conoscerne le opinioni politiche perché si associano alcuni suoi interventi nei *blog* all'identità completa presente su *social network* oppure in siti nei quali si è registrata per ottenere determinati servizi. Ciò accade perché spesso in rete cade la distinzione tra il piano formale e quello informale in cui l'identità si plasma in funzione dell'obiettivo che si desidera raggiungere.

Si pone quindi il problema della gestione della reputazione, intesa come immagine che gli altri percepiscono dalle informazioni pubblicate su Internet su una persona. Commenti negativi, dati parziali, episodi isolati, possono costruire una cattiva reputazione, anche senza che ci siano calunnie esplicite. La difesa della reputazione in rete è una pratica comune tra le istituzioni, gli enti e le aziende, mentre è molto meno diffusa tra le persone, eccezion fatta per i personaggi famosi, soprattutto nello spettacolo o nello sport che intervengono con mezzi legali o rivolgendosi a imprese specializzate nel "ripulire" la rete.

Nei *social network* ci sono approcci diversi, con la facoltà di costruire identità del tutto immaginarie oppure totalmente aderenti alla realtà con narrazioni di particolari condivisi con tutti o con molti, quando nella vita reale sono riservati ai vicini più intimi. Interessante è il recente approccio di

Google+ che pretende nome e cognome verosimili impedendo di creare profili con nomi fantastici o generici.

Un'identità digitale falsificata può anche essere sintomo di incapacità di intessere relazioni stabili con altre persone. Infatti le relazioni generate in rete sono molto spesso "senza vincoli", cioè si intessono e rompono con molta facilità senza lasciare particolari conseguenze. Alcuni autori le definiscono "liquide", sottolineandone l'assenza di forma stabile.

Le responsabilità legali di azioni illecite svolte sotto falsa identità non cambiano la fattispecie dei reati e la Polizia Postale e delle Comunicazioni è sempre in grado di risalire al vero autore.

La tutela della *privacy* nei *social network* è continuamente oggetto di discussione, perché questi devono bilanciare l'esigenza commerciale di raggiungere la massima diffusione dei propri servizi, attraverso la semplicità di pubblicazione, con la necessità di dare all'utente gli strumenti per decidere con chi condividere quanto mettono in rete. Negli ultimi anni si è assistito a una politica molto "aperta" in fase di lancio di un nuovo *social network* per favorirne l'uso, con una impostazione successiva più limitativa e protettiva, a volte in risposta alle proteste di alcuni utenti.

Un limite significativo, statisticamente rilevato, è dato dalla leggerezza dell'utente medio che non legge le politiche di *privacy* o le guide per proteggere i propri dati nel *social network* che sta utilizzando. Nonostante lo utilizzi per ore al giorno, non dedica pochi minuti per imparare come funziona. Un caso clamoroso è stata la votazione fatta nel 2009 da Facebook sul cambiamento dei propri principi, diritti e doveri, decidendo che il risultato della votazione sarebbe stato vincolante per Facebook se avesse votato almeno il 30%, altrimenti sarebbe stato considerato solo indicativo. Su 200 milioni di utenti nel mondo hanno votato in 650.000, numero oggettivamente alto, ma corrispondente allo 0,3%, lontanissimo dai 60 milioni auspicati.

Le proposte di innovazione legislativa in Italia, volte a tutelare in rete il buon nome dei cittadini, hanno provocato forti reazioni per non compromettere la libertà di espressione. La Wikipedia ha addirittura oscurato tutte le sue voci italiane per alcuni giorni, in modo da sensibilizzare il pubblico al problema.

Linee guida

Al fine di migliorare il rapporto con gli utenti dei portali destinati ai giovani, le tre schede seguenti riportano informazioni con linguaggio accessibile, pubblicabili integralmente o con le opportune modifiche, sui portali stessi. Sono volutamente sintetiche per non scoraggiare i potenziali lettori. Ovviamente non sono esaustive, ma riportano gli elementi essenziali per la tutela della propria e altrui identità.

Si suggerisci che siano adattate graficamente per renderle accattivanti, mettendo in evidenza alcuni punti maggiormente importanti in relazione ai servizi prestati dal portale.

La prima scheda, sull'identità digitale dei giovani, è destinata direttamente agli utenti, per renderli consapevoli della questione.

La seconda scheda, sulla tutela dell'identità degli utenti da parte dei gestori dei portali, è una raccolta di buone pratiche, utile anche per difendersi da possibili conseguenze legali. Non è un manuale tecnico, né giuridico. Per una trattazione più formale si può far riferimento ad altri documenti prodotti in questa attività di "Supporto allo sviluppo della sicurezza e legalità informatica nell'ambito delle iniziative rivolte ai giovani".

La terza scheda è una sintesi di consigli da pubblicare accanto alla sezione dedicata alla registrazione degli utenti di un portale per giovani. Con gli opportuni adattamenti è utile anche per altri portali.

La mia giovane identità digitale

1. Ogni volta che accedo a Internet resta una traccia da qualche parte. L'indirizzo IP del mio computer viene registrato dal fornitore di connettività che ha alcuni obblighi legali di conservazione a fini investigativi. Non esiste quindi abitualmente l'anonimato totale in rete. Anche quando accedo con pseudonimi, soprannomi, *avatar*, se commetto reati, la Polizia può rintracciarmi.
2. Ogni volta che pubblico qualcosa in rete sto dicendo qualcosa di me, anche sotto mentite spoglie. Ci sono sistemi automatici che riescono a mettere in relazione i mie contenuti sparsi su Internet e costruire di me un profilo abbastanza realistico. È un motivo in più per non pubblicare stupidaggini o, peggio ancora, calunnie, diffamazioni, oscenità, menzogne.
3. Il Garante della *privacy* ha stabilito il diritto all'oblio, cioè alla cancellazione dai motori di ricerca delle informazioni negative su di me, dopo un po' di tempo dall'evento. Per esempio se ho commesso anche solo un reato minore e i giornali ne hanno parlato oppure ho avuto una sanzione amministrativa che è sul sito del mio datore di lavoro pubblico, fra qualche anno non deve essere possibile che di me i motori di ricerca mettano al primo posto proprio quella notizia. Tuttavia questo diritto non si applica ai contenuti che ho pubblicato io da studente (il video mentre brucio la cattedra in classe) e di cui mi vergognerò quando andrò a lavorare. E il mio possibile datore di lavoro fra dieci anni riuscirà a trovarlo anche solo in base alla mia fotografia. Perciò devo tutelare la mia identità evitando di pubblicare materiale che mi possa nuocere in futuro.
4. Quando mi registro a un sito che chiede *username* e *password* (per scrivere su un *blog* o un *forum*, ad esempio), devo verificare che l'operazione avvenga su una URL che inizia con *https* e non solo *http*. In questo modo i miei dati segreti sono crittografati e non intercettabili.
5. Alcuni siti mi mandano la *password* in chiaro via *mail*. È poco sicuro e, in questo caso, conviene che uso una *password* molto diversa da quella per servizi importanti come la posta o i *social network* o la banca. E devo comportarmi su quel sito poco sicuro in modo particolarmente attento, evitando di inserire dati riservati o sensibili.
6. Scegliere una *password* complicata è facile, sceglierne una diversa per ogni sito è difficile perché non me le ricordo tutte. E se me le scrivo, rischio di farle conoscere a chi trova il pezzo di carta o il *file* dove le ho messe. Una *password* è abbastanza sicura se è almeno di otto caratteri, con lettere e numeri. Non deve essere una parola di dizionario, di nessuna lingua. Posso concatenare due parole e aggiungere in una posizione intermedia un carattere speciale o un numero: ad esempio, cavallocuspid-e. Un'alternativa è prendere le iniziali di una frase con delimitatori intorno: ad esempio "*fin che la barca va lasciala andare*" diventa "+*fclbvla*-".
7. Per distinguere le *password* dei diversi siti, partendo da una *password* universale, posso inserire un identificatore del tipo di servizio che mi offre ogni sito. Ad esempio inizio la *password* con P se è posta elettronica, finisco con S se è *social network*, premetto un € se è banca. Tutto ciò a volte non è possibile perché ci sono siti che impongono *password* di sole lettere e numeri oppure non più lunghe di un certo numero di caratteri o, peggio ancora, obbligatoriamente di tot caratteri. Purtroppo in questo modo gli attacchi per scoprirle sono più facili e devo stare quindi più attento.
8. Non mi devo difendere solo dai possibili attacchi di specialisti del furto di identità. Il primo pericolo è la mia disattenzione o pigrizia. Non devo rivelare le *password* a nessuno, neppure ai miei familiari o amici intimi, non devo usarne di banali, come quelle che contengono il nome del mio cane o del cantante preferito, e non devo salvarle sia perché poi me le dimentico, sia perché se il computer che uso va in mano ad altri, possono accedere con la mia identità.
9. Devo evitare di cadere nelle trappole dei messaggi di *phishing* che mi chiedono di inserire le mie credenziali per ottenere qualcosa di interessante o nuovo. Un sano scetticismo di fronte a messaggi di grande fortuna o di promesse eccezionali, fa sempre bene.

Il mio codice di condotta di gestore del portale per i giovani per la tutela della loro identità

1. Mi impegno a tutelare gli utenti che accedono al portale che gestisco.
2. D'accordo con i gestori dei contenuti, curerò che non siano pubblicate affermazioni diffamatorie, calunniose o volgari, né contrarie alle leggi vigenti.
3. Se i contenuti protetti richiedono la maggiore età, chiederò i dati anagrafici e il codice fiscale, pur sapendo che è possibile inventarseli.
4. Per l'accesso alle zone riservate agli utenti registrati utilizzerò, per lo meno per la fase di autenticazione, il protocollo *https* per dare garanzia di trasmissione crittografata delle credenziali.
5. Se anche i contenuti trasmessi sono sensibili, attiverò il protocollo *https* per tutte le transazioni.
6. Nella fase di registrazione di un nuovo utente chiederò il minimo di dati personali necessari all'erogazione del servizio e li conserverò in un *database* accessibile solamente allo stesso utente, per poterli modificare, e agli amministratori di sistema espressamente nominati.
7. Nella fase di scelta della *password* da parte dell'utente attiverò un meccanismo che impedisca le *password* banali oppure imporrò una lunghezza di almeno otto caratteri di cui almeno uno non alfabetico.
8. Non salverò la *password* in chiaro, ma ne conserverò solamente un *hash* impiegando le buone pratiche comuni in questo campo.
9. Non invierò mai la *password* via mail, né per conferma, né su richiesta dell'utente. Attiverò invece un sistema di invio di un *link* a una pagina protetta *https* che permetta la reimpostazione della *password*.
10. Se dovrò dare la possibilità di pagare elettronicamente, non chiederò i dati della carta di credito dell'utente, ma farò svolgere tutta la procedura sul sito della banca o del fornitore di servizi di pagamento.

La tua identità nel nostro portale

1. Non divulghiamo i dati personali che hai trasmesso quando ti sei iscritto/a ai servizi su questo portale.
2. Il tuo nome di accesso e la tua *password* sono trasmessi sempre con sistema sicuro (*https* invece di *http*) per cui non possono essere intercettati.
3. La tua *password* è sufficientemente sicura da decifratura se è di almeno 8 caratteri fra lettere e numeri e non coincide con parole intere in qualsiasi lingua. Puoi comporre una buona *password* concatenando due parole e aggiungendo un carattere non alfabetico in una qualsiasi posizione, oppure prendendo le iniziali di una frase che ricordi facilmente, con l'aggiunta di un numero.
4. Ti suggeriamo di non usare la stessa *password* in altri siti: ognuno dovrebbe averne una distinta, magari semplicemente differenziata con un'aggiunta relativa al servizio che dà. Per esempio potresti aggiungere +po per il sito di posta elettronica, +di per il *blog*, +sn per *social network*, ecc. (non seguire alla lettera questo consiglio, ma inventati tu un sistema analogo).
5. Quando dimentichi la *password* non te la mandiamo via posta elettronica: noi non la conosciamo. Invece ti diamo la possibilità di reimpostarla, mandandoti un *link* a una pagina apposita. Ovviamente, devi poter accedere alla casella di posta corrispondente all'indirizzo *e-mail* che hai fornito al momento della registrazione.
6. Sei responsabile delle azioni che compi quando sei registrato/a sul portale. Per questo non cedere la tua *password* a nessuno, perché potrebbe agire al tuo posto commettendo azioni che ti sarebbero imputate.
7. Nei nostri *server* registriamo alcuni dati relativi alla tua connessione, per motivi tecnici e legali. Non ne facciamo alcun uso individuale, ma possono essere utilizzati in forma aggregata, per fini statistici, senza possibilità di risalire al singolo utente.
8. Ti diamo la possibilità di cancellare la tua utenza dal nostro portale. I tuoi dati personali sono cancellati, ma è possibile che resti traccia dei tuoi interventi e pubblicazioni e che questi non siano automaticamente eliminabili o facciano parte di collezioni ormai consolidate.

Michele Crudele - 2011-10-06