CONSIGLIO NAZIONALE DEL NOTARIATO

Studio n. 6-2007/IG

Password, credenziali e successione *mortis causa*

Approvato dalla Commissione Studi di Informatica Giuridica l'11 maggio 2007

Lo Studio in sintesi *(Abstract)*

Al fine di attribuire a soggetti predeterminati l'accesso a risorse informatiche protette da credenziali (username, PIN, password), dopo il decesso del loro titolare, è possibile far ricorso sia al mandato "post mortem" che all'istituto dell'esecutore testamentario. In linea di principio, inoltre, le risorse online passano nella disponibilità dei successori "mortis causa".

———————

1. Il problema del diritto all'accesso alla posta elettronica di un defunto ebbe, forse per la prima volta, eco mondiale nella primavera 2005. Su richiesta della famiglia di Justin Ellsworth, un Marine scomparso ventenne in Iraq, la *Probate Court* della Oakland County, Michigan, ordinò al *provider* statunitense Yahoo di consegnare ai genitori tutta la corrispondenza giacente nella casella di posta elettronica dello sfortunato giovane militare [(1)]. Una circostanza contribuiva a rendere il caso particolarmente interessante sul piano giuridico: secondo le condizioni generali d'uso di Yahoo, in caso di morte del titolare la casella deve essere soppressa insieme all'intero suo contenuto [(2)].

Si tenterà una prima sistemazione della questione [(3)] sotto un duplice profilo: quale sia il regime applicabile in caso di assenza di disposizioni dettate dal defunto, e quali soluzioni possano essere utilmente proposte a chi, in vita, sottoponga tale questione al notaio. Previsioni in materia di *password* risulterebbero ormai comuni nella prassi testamentaria statunitense [(4)], e non par dubbio che tale esigenza possa divenire d'attualità anche nel nostro Paese.

2. Nel prosieguo si impiegherà l'espressione *credenziali* per designare qualun-

que combinazione di caratteri utilizzata per governare l'accesso a risorse elettroniche; comprende le figure note nella prassi come PIN, password ed username. Nel gergo informatico, si utilizza talvolta l'espressione riassuntiva *something you know* (qualcosa che conosci) [5].

E' opinabile se le credenziali abbiano o meno natura giuridica di firma elettronica (cosiddetta firma elettronica *semplice* o *leggera*) ai sensi dell'articolo 1 del decreto legislativo 5 marzo 2005, n. 82, *Codice dell'amministrazione digitale*, nel testo modificato con decreto legislativo 4 aprile 2006, n. 159, che detta la seguente definizione: *l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.* Si tratta infatti certamente di dati in forma elettronica, ma non pare di scorgere il requisito dell'*associazione logica ad altri dati elettronici* prevista dalla norma [6]. Più probabilmente, i metodi di accesso basati su credenziali debbono semplicemente considerarsi come un metodo, contrattualmente definito, per l'identificazione telematica dell'avente diritto all'accesso, dinamicamente rassomigliante ai documenti di legittimazione di cui all'articolo 2002 del codice civile.

Anche ammettendo che di firma elettronica leggera si tratti, va però sottolineato un profilo ai nostri fini assai rilevante di tale figura, che si può desumere dal confronto con la nozione di firma elettronica qualificata, che la medesima legge definisce come *la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario.* Mentre per la firma elettronica qualificata, la necessità di un rapporto univoco con un determinato firmatario rende assai discutibile la possibilità di un utilizzo *post mortem*, tale perplessità non sussiste per la firma elettronica semplice.

Può quindi preliminarmente affermarsi che eventuali negozi tesi a porre a disposizione di altri soggetti una credenziale dopo la morte del suo titolare, non incontrano ostacoli derivanti dall'intrinseca natura giuridica della credenziale stessa.

Ai nostri fini possiamo dividere le credenziali in due categorie.

2a. Un primo gruppo è rappresentato dalle credenziali che consentono l'accesso a risorse online. Non si tratta soltanto della semplice posta elettronica. Sono sempre più diffusi in Rete i cosiddetti dischi remoti, ove possono essere conservati files di ogni genere. E' ormai costume tutt'altro che raro riporvi informazioni delicate, magari di carattere finanziario, che si preferisce non memorizzare sui computers di casa od ufficio. Scelta solo a prima vista scriteriata: difficile semmai dar torto a chi reputa un'intrusione in tali sistemi online eventualità meno preoccupante della curiosità di colleghi, dipendenti, tecnici della manutenzione, coniugi e partners. Diffusissimi sono i siti dedicati alle fotografie, ove gli utenti possono pubblicare le proprie immagini, ma anche conservarle privatamente, sotto password. Esistono pure

siti che offrono servizi di word processing, ove si possono creare, elaborare e conservare testi, il tutto interamente online. Sono di diffusione più recente, ma già assai apprezzati da chi usa più di un computer (non ci si deve più preoccupare di trasferire i testi da una macchina ad un'altra) e da chi desidera condividere un determinato lavoro con altre persone.

Va poi considerato che diversi servizi (quelli di Telecom Italia, ad esempio) proteggono con le medesime credenziali posta, dischi remoti e fotografie. E la stessa posta elettronica ha la capacità di veicolare in allegato qualsivoglia contenuto, anche multimediale.

2b. Un secondo gruppo è rappresentato dalle credenziali che governano l'accesso ad un computer, ad altre risorse fisiche (una penna USB, ad esempio) od a singoli files o gruppi di files, ivi comprese le chiavi private impiegate a fini di decriptazione.

3. Per quanto concerne il primo gruppo, e cioè le credenziali di accesso a sistemi governati da operatori online, un soggetto correttamente legittimato (in primis, quale successore nel rapporto contrattuale relativo all'uso del sistema) può puntare ad ottenere dal gestore un duplicato delle credenziali o nuove credenziali. Non è quindi indispensabile ricorrere alla conservazione diretta della credenziale (si veda però infra, § 8). Qualora invece il defunto porti con sé nella tomba credenziali di accesso a dispositivi fisici, si può solo contare sull'aiuto di tecnici capaci di padroneggiare (per finalità lecite, in questo caso) le tecniche tipiche degli *hackers* (ma forse dovrebbe meglio dirsi *crackers*) [(7)].

In entrambi i casi una credenziale può governare l'accesso al materiale più svariato, che va dalla semplice corrispondenza personale, ad informazioni finanziarie, a veri e propri prodotti, come il lavoro di un fotografo professionista o di un traduttore, oggetto di diritto d'autore o di altre tipologie di rapporto dominicale.

Sulla scorta di tale rilievo, si potrebbe ipotizzare che il diritto alla password dia vita ad una nuova figura meritevole di originale inquadramento ed autonoma ricostruzione sul piano della disciplina, una sorta di nuovo diritto digitale [(8)].

In effetti, la diffusa propensione a ricondurre a tutti i costi i nuovi fenomeni digitali alle categorie giuridiche note ha spesso contribuito a produrre radicali incomprensioni. Non si deprecherà mai abbastanza, ad esempio, l'acritica equiparazione concettuale tra firma digitale e firma tradizionale, prima responsabile della scarsa attenzione che certa dottrina ha prestato alle decisive differenze tra le due figure [(9)]. Pur accolto e metabolizzato questo *caveat* metodologico, che costituisce anzi un tratto tradizionalmente ben riconoscibile dell'approccio degli specialisti di matrice notarile, non sembra che nel nostro caso la natura digitale dei contenuti sia

rilevante. Archivi, carte e corrispondenza su supporto tradizionale possono perfettamente contenere la medesima varietà di materiale. Se l'argomento richiede qualche modesta riflessione, non è quindi a causa del suo oggetto mediato, e cioè del materiale cui grazie alle credenziali è possibile accedere, ma in relazione alla figura "credenziali" in sé.

4. Anche se il fenomeno non sembra dunque possedere soverchi caratteri di originalità, ci troviamo dinanzi ad una stratificazione di posizioni soggettive non poi così banale.

Da un lato, il diritto (di natura obbligatoria) di accedere ad una risorsa online, non corrisponde necessariamente ad un diritto (dominicale) su tutti i contenuti cui si ha accesso.

D'altro lato, mentre nel mondo cartaceo il valore intrinseco del supporto del documento è per lo più irrilevante, lo stesso non può dirsi di un computer. Occorrerà quindi tenere ben distinti i diritti sul computer (od altra risorsa fisica) in quanto tale, e le disposizioni relative al suo contenuto. Può ben darsi che un computer sia oggetto di legato e che contemporaneamente un terzo sia incaricato di accedervi, utilizzando le credenziali ad hoc rimesse, (ad esempio) per distruggerne il contenuto. In tal caso pare ragionevole reputare che, nel silenzio, la distruzione (o, comunque, la diversa sorte) debba limitarsi ai documenti contenuti nella macchina, e non al software (sistema operativo ed applicativi), che in quanto pertinenza deve probabilmente considerarsi ricompresa nell'oggetto del legato. Potrà pure accadere che il *de cuius* non abbia alcun diritto sul computer in quanto tale, magari concesso in comodato da un terzo; ciò non precluderà, ovviamente, la tutela dei diritti sul contenuto della macchina.

Non va poi trascurata la possibilità che le risorse informatiche protette dalla credenziale contengano (a vario titolo) materiali altrui, o su cui altri possono comunque vantare diritti: il caso più evidente è quello di materiale aziendale [(10)] conservato in risorse private.

5. Per le ragioni accennate al § 2, deve probabilmente escludersi la liceità di ogni disposizione od accorgimento diretto ad assicurare a qualsivoglia soggetto la disponibilità del PIN o password di accesso a dispositivi di firma elettronica qualificata dopo la morte del titolare; a fortiori ciò vale per la firma digitale, che della firma elettronica qualificata rappresenta un sottotipo. Neppure per un istante può poi pensarsi ad un utilizzo *post mortem* di sistemi di firma/funzione, che documentano non solo l'identità del sottoscrivente, ma anche la specifica funzione da lui ricoperta: è il caso della firma digitale del notaio

Restano pure escluse le credenziali che non siano nella piena titolarietà del di-

sponente: la password relativa ad una casella aziendale, ad esempio, non potrà essere efficacemente oggetto di disposizione qualsivoglia. Altra questione, che esula evidentemente dal nostro esame, è la sorte del materiale privato contenuto in caselle aziendali.

Un caso particolare è l'accesso alle risorse che il notaio impiega per la sua professione, come ad esempio le caselle di posta del dominio “notariato.it”. Potrebbe ipotizzarsi che, in quanto risorse informatiche relative all'attività di studio, anch'esse debbano essere “sigillate” (in altri termini: impedito il prelievo della posta) dal Capo dell'Archivio ai sensi dell'articolo 39 della legge notarile.

In contrario può fondatamente obiettarsi che l'intervento dell'Archivio è finalizzato all'individuazione e ritiro della documentazione destinata alla conservazione presso l'Archivio medesimo, ma che allo stato, nessun documento informatico è attualmente conservato, se non alcuni indici che sono però creati ad hoc per l'Archivio medesimo. Non pare quindi, in prima approssimazione, che alle risorse del sistema informatico notarile debbano applicarsi regole particolari, anche se in prospettiva il problema merita di essere sorvegliato. E' facilmente prevedibile infatti che nelle caselle di posta elettronica (specie la nuova PEC, Posta Elettronica Certificata) e nel sistema di Archiviazione e Conservazione (SANNI) si troverà materiale eterogeneo, suscettibile di differenziata sorte in ottica successoria. Se gli eredi del notaio, ad esempio, hanno certamente diritto ad accedere ai dati relativi alla registrazione degli atti, atteso che ne possono derivare crediti o debiti nei confronti dei clienti, altrettanto sicuro è che i dati relativi all'iscrizione RGT di un testamento pubblico (che pure viaggia via PEC) dovranno essere tenuti segreti anche nei confronti degli eredi. Ne potrebbe derivare qualche problema pratico di non così ovvia soluzione.

6. Per converso, non presentano particolare interesse, ai nostri fini, i servizi che prevedono Internet quale modalità di accesso alternativa: il caso più evidente è quello dell'*home banking*, ove la perdita delle credenziali non impedirà agli aventi diritto di far valere i propri diritti nelle forme ordinarie. Si potrà presentare piuttosto l'eventualità inversa, e cioè un impiego abusivo delle credenziali da parte di altri soggetti, questione estranea al tema in esame.

7. Le soluzioni a disposizione di chi voglia espressamente disporre intorno alle proprie credenziali sono verosimilmente riconducibili a due gruppi, a seconda che siano dirette a:

a) far pervenire *post mortem* le credenziali ad un soggetto predeterminato, oppure

b) legittimare un determinato soggetto ad ottenere le credenziali d'accesso dal gestore del servizio: strategia inapplicabile, evidentemente, alle risorse fisi-

che, a meno che le credenziali non siano conservate presso un ulteriore soggetto.

Esaminiamo le due ipotesi partitamente.

7a. Immaginiamo che l'interessato voglia compilare una lista delle credenziali in suo possesso, da rimettere ad un terzo (anche il notaio, eventualmente) con le istruzioni da seguirsi in caso di decesso. Due osservazioni preliminari sul piano pratico:

- le password sono soggette ad essere modificate: un periodico rinnovo delle password è anzi una delle più ovvie misure di sicurezza. Occorrerà quindi raccomandare all'interessato di procedere all'aggiornamento della lista ogniqualvolta necessario;
- improponibile l'inclusione delle credenziali nel corpo di un testamento, giacché in tal modo ci si porrebbe irreparabilmente alla mercé del più lesto a richiedere la pubblicazione. E' ben vero che l'articolo 7 del DPR 513/97 prevedeva il deposito presso notaio, nella forma del testamento segreto, della chiave privata di firma, e cioè del dato informatico segreto per eccellenza. Ma l'argomento *a fortiori* sarebbe qui fallace: a tacer d'altro, la norma ormai abrogata disciplinava la conservazione di un dato per definizione inutilizzabile dopo il decesso del titolare.

Deve però affrontarsi una questione ben più impegnativa: la liceità sul piano strettamente giuridico di un siffatto *modus operandi*. Pare di poter dare risposta affermativa, sotto un duplice profilo:

- *l'oggetto.* Come già ricordato (§2), con l'eccezione delle credenziali relative a sistemi di firma qualificata, non esiste un divieto generale di svelare le proprie credenziali a terzi, salva l'autoresponsabilità in relazione alle attività che vengono così rese possibili. Possono certamente sussistere divieti contrattuali, da esaminarsi caso per caso;
- *lo strumento*. Il mandato *post mortem* è reputato generalmente valido [(11)] qualora non tenda a realizzare un'attribuzione patrimoniale. E questo pare esattamente il caso dacché, come già si è osservato, consentire l'accesso ad una risorsa fisica od online non equivale ad intervenire sui rapporti giuridici, dominicali o d'altra natura, di cui sono oggetto i materiali che la risorsa stessa custodisce.

Il mandato sarà a forma libera, benché lo scritto sia ovviamente preferibile. Lecito pure immaginare che un soggetto sia costituito depositario delle credenziali, e che altro soggetto sia legittimato dal mandato ad ottenere *post mortem* le credenziali dal depositario per compiere le attività previste dal mandante. In ogni caso, tali attività dovranno essere analiticamente previste, specialmente laddove siano

suscettibili di produrre conflitti con altrui posizioni soggettive: è soprattutto il caso del mandato a distruggere contenuti informatici, nei limiti in cui questo sia da reputarsi lecito secondo i principi.

7b. Se le conclusioni cui si è appena pervenuto sono esatte, deve parimenti riconoscersi la possibilità di designare un mandatario *post mortem* con l'incarico di ottenere dagli operatori l'accesso alle risorse online indicate. Lo stesso potere potrà essere altresì conferito per via testamentaria ad un esecutore, figura probabilmente preferibile in quanto estremamente familiare al mondo di common law.

8. Molti servizi *online* correntemente utilizzati anche da residenti in Italia sono infatti localizzati all'estero, perlopiù in giurisdizioni di *common law*: è il caso anche del più celebre servizio di posta elettronica su web, Hotmail. Pure il presente scritto è stato redatto utilizzando un servizio per la redazione di testi via web localizzato in California, le cui condizioni generali fanno rinvio alle leggi di quello stato e sanciscono la competenza esclusiva delle corti della Contea di Santa Clara.

In molti casi sarebbe quindi miope basarsi esclusivamente sulle norme di diritto interno, che risulterebbero del tutto irrilevanti qualora ad esempio si volesse, come nel caso richiamato in apertura, ottenere l'ordine di un giudice statunitense.

Sul piano teorico, occorrerebbe tener conto anche dei principi di diritto internazionale privato. Far valere il diritto successorio italiano presso una giurisdizione straniera, compatibilmente con il sistema internazionalprivatistico della *lex fori*, rischia però di trasformarsi in un impervio esercizio.

Il linea più generale, appare nettamente preferibile adottare soluzioni che, attribuendo il controllo diretto delle credenziali, non impongano il ricorso ad iniziative giudiziali o stragiudiziali da condurre nell'ambito di ordinamenti stranieri.

9. In assenza di disposizioni, gli eredi, almeno in diritto italiano, hanno diritto a ricevere la corrispondenza diretta al defunto (articolo 34 lettera c del R.D. 18 aprile 1940 numero 689) e non v'è ragione di pensare che (in assenza di contraria volontà del defunto) non spetti agli eredi l'accesso alla corrispondenza già pervenuta. Il principio pare applicabile de plano alle risorse digitali, sia residenti su risorse fisiche che online. In tal senso è pure la prassi seguita da Telecom Italia [(12)], nonché, negli USA, da America On Line e da Hotmail [(13)]. Eventuali contenuti intimi o confidenziali potranno essere portati a conoscenza del pubblico (il che, evidentemente, è cosa ben diversa dall'accesso dell'avente diritto) solo con l'osservanza delle disposizioni di cui all'articolo 93 della legge 22 aprile 1941 n. 633.

Su queste basi, potrebbe reputarsi *prima facie* inutile disporre espressamente, qualora si desideri semplicemente rendere accessibili le proprie risorse informatiche

agli eredi.

Vale però il rilievo operato al paragrafo precedente.

10. Si ricorderà come, nel caso richiamato al § 1, le condizioni generali del servizio prevedessero la distruzione della casella *e-mail* del defunto con l'intero suo contenuto. Il giudice statunitense è andato in questo caso di contrario avviso, ma non si può escludere che la carica emozionale legata alle specificità della vicenda (il Marine scomparso ventenne in Iraq) abbia giocato il proprio ruolo. Dall'angolo visuale del diritto italiano, la clausola sarebbe da reputarsi probabilmente valida, sostanziandosi in un mandato *post mortem* avente ad oggetto la distruzione della corrispondenza, ipotesi certo non priva di precedenti nel mondo cartaceo.

Resta un qualche disagio nell'accettare l'idea che una semplice clausola nell'ambito delle condizioni generali possa condurre a conseguenze così definitive quale la perdita irreversibile di contenuti digitali [(14)].

Ugo Bechini

———————————

1) Mark D. RASCH, *A Corporal's Death Starts a Dispute on E-Mail Ownership - Should e-mail accounts perish along with their owners? A military death generates a dispute over electronic rights and IP*, in *IP Law & Business*, 23 marzo 2005. L'esito della vicenda è riportato dall'Associated Press: Paul SANCYA (AP), *Yahoo will give family slain Marine's e-mail account*, 21 aprile 2005 11:32 AM.

2) *No Right of Survivorship and Non-Transferability. You agree that your Yahoo! account is non-transferable and any rights to your Yahoo! ID or contents within your account terminate upon your death. Upon receipt of a copy of a death certificate, your account may be terminated and all contents therein permanently deleted*. (Assenza di diritti successori e non trasferibilità. Si conviene che *l'account* Yahoo non sia trasferibile e che i diritti sulle credenziali Yahoo e sui contenuti s'estinguano con la morte. Ricevuta copia del certificato di morte, l'account può essere chiuso ed i suoi contenuti irreversibilmente cancellati).

3) Per un inquadramento generale delle problematiche che possono verificarsi in caso di decesso del proprietario di un computer, Jeffrey SELING, *Whose Data Is It, Anyway?*, in *The New York Times*, 3 giugno 2004.

4) Elinor MILLS, *Taking passwords to the grave*, in *CNET News.com*, 22 settembre 2006, ha raccolto la testimonianza in tal senso di un avvocato specializzato in *estate planning,* il californiano Michael Blacksburg.

5) S*omething you have* (qualcosa che hai) individua le tecniche di identificazione basate sul possesso di un oggetto fisico (come la smart card); *something you are* (qualcosa che sei) si riferisce alle tecniche biometriche. Tali soluzioni possono combinarsi, come nel caso della firma digitale, che richiede il possesso di un oggetto (la smart card) e la conoscenza del relativo PIN.

6) Nello stesso senso Manlio CAMMARATA e Enrico MACCARONE, *Un messaggio e-mail non è "prova scritta"* in *Interlex* (http://www.interlex.it), 29 gennaio 2004.

7) Esistono società specializzate in questo campo, come Password Crackers Inc (Maryland, USA: http://www.pwcrack.com).

8) *Private e-mails are a new category. It's not immediately clear how to treat them, but it's a form of digital property*. (le emails private appartengono ad una nuova categoria. Non è immediatamente chiaro a quale regime debbano essere sottoposte, ma è una forma di proprietà digitale). Marc Rotenberg, executive director dell'Electronic Privacy Information Center, intervistato da Elinor

Mills, *Taking passwords to the grave*, in *CNET News.com*, 22 settembre 2006.

9) Silvia MICCOLI, *La sicurezza giuridica nel commercio elettronico* (tesi di laurea), reperibile in Rete (formato Word) alla pagina http://web.tiscalinet.it/conoge/silmic.doc, seguita da Danilo GIAQUINTO e Paola RAGOZZO, *Il sigillo informatico*, in *Notariato*, 1997, 80; vedasi però soprattutto Mario MICCOLI, *Commercio telematico: una nuova realtà nel campo del diritto*, IPSOA, Milano 1998, p. 35. Chris REED, *What is a Signature?*, in *The Journal of Information, Law and Technology (JILT)*, 2000 (3), http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/ paragona la firma digitale ad un semplice timbro di gomma (*rubber stamp*), mentre Stephen MASON, *Electronic Signatures in Law*, LexisNexis UK, London 2003, p. 318, avvicina la firma digitale ad un particolare tipo di sigillo in uso in Giappone sin dall'ottavo secolo, lo *Jitsuin*.

10) Più precisamente, si intende qui alludere alla corrispondenza relativa all'esercizio di un'azienda di cui il titolare della casella sia dipendente o collaboratore.

11) Vedi tra gli altri Marco IEVA, *I fenomeni cd parasuccessori*, in *Donazioni e successioni*, a cura di Pietro Rescigno, Padova 1994, tomo I, p. 82.

12) Nota informativa di Telecom Italia, a firma Elena Arieta, indirizzata al Consiglio Nazionale del Notariato il 30 novembre 2006; la diffusione del contenuto è stata espressamente autorizzata.

13) Così riferisce la BBC in *Who owns your e-mails?* BBC News, Tuesday, 11 January, 2005, 14:29 GMT. AOL ed Hotmail sono probabilmente, insieme a Google (servizio Gmail) ed alla già citata Yahoo, i maggiori operatori di posta elettronica al mondo.

14) In relazione alla vicenda citata al § 1, BBC News (*Who owns your e-mails?*, Tuesday, 11 January, 2005, 14:29 GMT) riportava l'opinione di un avvocato inglese, Leigh Ellis: *They are attempting, in effect, by contract, to extinguish a property right to the contents in the account* (stanno tentando, in effetti, di estinguere per contratto il diritto di proprietà sui contenuti della risorsa).

(Riproduzione riservata)