diritto&diritti dal 1996
diritto.it
direttore Francesco Brugaletta

**ISSN 1127-8579**

**Pubblicato dal 14/10/2010**

**All'indirizzo http://www.diritto.it/docs/30315-la-sicurezza-dei-dati-durante-la-fase-di-primo-accesso-a-databases**

**Autori: Giglio Alessandra, Scalia Roberto**

# La sicurezza dei dati durante la fase di “primo accesso” a databases

# LA SICUREZZA DEI DATI DURANTE LA FASE DI "PRIMO ACCESSO" A *DATABASES*

ALESSANDRA GIGLIO ([1]) E ROBERTO SCALIA ([2])

## I.) Premessa.

Sempre più di frequente, enti, associazioni, consorzi, ordini professionali etc. elaborano forme di fruizione di dati, notizie e servizi mediante l'accesso a *pagine web* dell'ente (o associazione et c.).

Ciò avviene mediante la dematerializzazione dei dati che dalla forma cartacea sono trasformati in *databases* informatici accessibili da parte dei fruitori (associati, professionisti protetti etc.) i quali dispongono di credenziali d'accesso che dovrebbero consentirne la tutela sotto il profilo della *privacy.*

Nella prassi, tuttavia, capita d'imbattersi in "pratiche di accreditamento" che, al fine di consentire l'accesso e la fruizione di dati elettronici, prevedono l'inserimento di dati "elementari" quali il nome (o cognome) dell'utente e/o suoi dati sensibili (data di nascita, n° partita IVA, n° identificativo d'iscrizione all'ente/albo/associazione, codice fiscale *et similia*).

Ciò accade, precipuamente, nelle fasi del c.d. "primo accesso" ove varie esigenze (di speditezza, in primo luogo) inducono gli amministratori dei sistemi ad adottare *chiavi d'accesso* semplificate; già note al gestore del sistema non perché "generate" dallo stesso ma perché già nel suo dominio conoscitivo. Si pensi, in particolar modo, alle seguenti chiavi: nome/cognome; cognome/codice fiscale; nome/partita IVA; cognome/data di nascita; etc.

Il presente contributo si prefigge l'obiettivo di analizzare le norme all'interno delle quali debbano essere sussunte *policies* sulla sicurezza della raccolta dei dati quali quelle esposte *breviter* nei capoversi precedenti che si basino su forme di accreditamento facilmente individuabili (l'esempio

1) Specialista nelle Professioni Legali (Università "Tor Vergata" Roma), Avvocato e Conciliatore societario in Trento. L'avv. Giglio può essere contattato agli indirizzi *avvalessandragiglio@recapitopec.it* e *giglio_alessandra@libero.it*.

2) Cultore del Diritto Tributario (Libera Università di Bozen/Bolzano), Avvocato e Conciliatore societario in Trento. L'avv. Scalia può essere contattato agli indirizzi *roberto.scalia@pec.ordineavvocaticatania.it* e *scalia_roberto@libero.it*.

classico può essere quello della coppia *username/password e-mail*/codice fiscale) .

L'importanza dell'argomento in esame è evidente sol che si ponga mente a taluni esempi come quello delle banche dati gestite da consorzi che veicolano contributi a favore di settori (o aree) svantaggiati(e); detti consorzi sovente rappresentano il *trait d'union* d'informazioni sulla scorta delle quali viene determinato tanto l'*an* del contributo, che il *quantum* dello stesso; informazioni, queste ultime, che nella quasi totalità dei casi si basano su dati economici alcuni dei quali, certamente, *"sensibili"*.

In questo senso, al fine di comprendere se le politiche di "primo accesso" semplificate descritte sopra possano ritenersi conformi alla normativa interna in materia di *privacy*, sarà svolta una disamina delle norme del D.Lgs. 30 giugno 2003, n. 196 "Codice in materia dei dati personali", meglio noto come "Codice della *privacy*" (di seguito, per brevità, individuato con l'acronimo "C.d.P.") con peculiare riferimento a quelle disposizioni poste a presidio della sicurezza dei dati, oltreché di quella dei sistemi.

## II.) La sicurezza dei dati e dei sistemi nel c.d. "Codice della privacy"

La sicurezza dei dati e dei sistemi è disciplinata dagli artt. da 31 a 36 (Parte I, Titolo V, *Sicurezza dei dati e dei sistemi*) del C.d.P., i quali prevedono stringenti obblighi gravanti in capo ai c.d. titolari del trattamento ([3]); obblighi che, con riferimento alle fattispecie evidenziate in seno al par. 1.) di questo scritto, incombono in capo agli enti, associazioni, ordini professionali *et al.*

Il C.d.P., da un lato (e conformemente a quanto già faceva la Legge 31 dicembre 1996, n. 675), opera una distinzione fra *idonee e preventive misure di sicurezza* e *misure minime di sicurezza* ([4]), ma, dall'altro (e in soluzione di continuità rispetto a quanto previsto dalla L.n. 675/96), introduce una disciplina articolata su due livelli con riguardo alle c.d. *misure minime* ([5]).

3) Ovvero ai soggetti cui competano le decisioni in ordine alle finalità e modalità del trattamento nonché, per l'appunto, *"… il profilo della sicurezza"* (così, art. 3, comma 1, lett. f), C.d.P.).

4) In riferimento ai sistemi informatici e telematici, il tema delle *misure di sicurezza* costituisce uno degli snodi fondamentali, anche nella materia penalistica (al fine di determinare la responsabilità dei terzi nelle fattispecie di accessi abusivi, detenzione e diffusione abusiva di codici d'accesso a sistemi informatici, di cui agli artt. 615-*ter* e 615-*quater* c.p.) e non è ridondante notare come il bene giuridico protetto, anche in detta materia, sia individuato nella segretezza dei dati e programmi cui le citate "misure" fungano da presidio. In questo senso, S. ATERNO, *Le misure di sicurezza nel reato di accesso abusivo: l'agente deve averle neutralizzate*, in Diritto dell'internet, 2007, pag. 596, (a commento di Cass. pen., Sez. V, 15 febbraio 2007, n. 6459). Cfr., inoltre, C. Cass., sez. lav., 9 gennaio 2007, n. 153, in Dir. dell'Internet, 2007, pag. 126.

5) In questo senso, in luogo di molti, cfr. P. TROIANO, *Sicurezza dei dati e dei sistemi*, in, C. M. Bianca e F. D. Busnelli, La protezione dei dati personali, Padova, 2007, pag. 689.

Distinzione, quest'ultima che si basa sull'utilizzo (cfr. art. 34) o meno (art. 35) di "strumenti elettronici" e che comporta un diverso regime di responsabilità nell'ipotesi di loro omissione.

Nell'un caso – *i. e.* ove siano impiegati sistemi elettronici –, infatti, all'omessa adozione di *idonee misure di sicurezza*, può associarsi una responsabilità civile per il risarcimento dei danni patrimoniali e non patrimoniali ai sensi dell'art. 15, commi 1 e 2, C.d.P. ([6]), nell'altro – *id est*, mancato impiego di sistemi elettronici –, invece, all'omissione riguardante le *misure minime*, il legislatore associa la responsabilità penale oltreché quella civile. In questo caso, a mente dell'art. 169 C.d.P., il Legislatore ha previsto le seguenti sanzioni penali (applicabili in una con quelle civili, *ut supra* enunciate): arresto sino a due anni o ammenda da diecimila a cinquantamila euro (contravvenzione che può esser ridotta, *ex* comma 2, art. 169, ad un quarto del massimo dell'ammenda) ([7]).

Le due distinte ipotesi sono ricollegabili, rispettivamente, alle fattispecie previste dagli artt. 31 e 33 del C.d.P.

Analizzando, in concreto, le citate disposizioni, può affermarsi che ove il trattamento dei dati avvenga, a' sensi dell'art. 31 C.d.P., mediante strumenti elettronici, sul titolare del trattamento, incomberà l'onere di predisporre misure preventive che siano, da un lato, connesse ai rischi potenzialmente incidenti sulla sua attività e, dall'altro, riconducibili nell'area del suo "controllo". Ciò è reso evidente, con particolare riguardo alle forniture di servizi di comunicazione elettronica accessibili al pubblico, dal disposto recato dal comma 3 dell'art. 32 ove viene stabilito che, con riferimento ad una speciale condizione di maggior periglio (il c.d. "… *particolare rischio di violazione della sicurezza della rete* …"), il titolare non assuma una responsabilità di "assoluta garanzia" (fatti salvi, com'è ovvio, gli obblighi di "ridurre al minimo" i pericoli e, ulteriori, particolari obblighi d'informazione).

E infatti, la prova liberatoria da parte del titolare, al fine di escludere la responsabilità per colpa, dovrà estrinsecarsi nella dimostrazione di aver adottato la diligenza dovuta nell'esercizio di una attività professionale ([8]).

L'adozione di preventive e idonee misure, quindi, si concretizza nella predisposizione di misure tecniche e organizzative "adeguate" al rischio esistente (cfr. art. 32, comma 1, 1° cpv., C.d.P.); misure la cui adeguatezza

---

6() A. PINORI, *Internet e responsabilità civile per il trattamento dati personali*, in Contr. e impr., 2007, pag. 1565 e ss., § 2.

7() In questo senso, importa rilevare che in virtù del rinvio espresso di cui all'art. 169, comma 2, ult. cpv., C.d.P., al D.Lgs. 758/1994, l'ente accertatore è la Guardia di Finanza.

8() In questo senso, con riferimento alla disciplina vigente *ante* C.d.P. del 2003, cfr. G. COMANDÈ, *Commento all'art. 18*, in, a cura di C.M. Bianca e F.D. Busnelli, Tutela della Privacy, Padova, 1999, pag. 494.

deve essere valutata, in concreto, in relazione al rischio di violazione della sicurezza, cui i sistemi risultino esposti.

In altri termini, nella previa predisposizione delle citate misure, il titolare sarà tenuto a svolgere una valutazione dei rischi (in particolare quello dell'"*… accesso non autorizzato …*") al fine di individuare quali possano essere i migliori correttivi (rimedi, che, non necessariamente debbano essere quelli più onerosi).

## II.1.) Le "*idonee misure*" e le "*misure minime*" *ex* artt. 31 e 33 C.d.P.

Con riferimento alle idonee misure *ex* art. 31, C.d.P., la migliore dottrina – occupandosi di definire i contorni della responsabilità, per omissione delle stesse – ha valorizzato il carattere *dinamico* di tale condotta che deve tendere al continuo aggiornamento di sistemi tecnologici, anche in considerazione della rapida obsolescenza delle misure tecniche dirette alla protezione dei sistemi ([9]). Tale *onus* è ricondotto, sovente, al complesso di obblighi relativi all'aggiornamento dei programmi volti a prevenire la vulnerabilità di strumenti elettronici ed a correggerne i difetti ([10]).

In questo senso, la fattispecie presa in esame in questo contributo non pare palesare, immediatamente, aspetti problematici che facciano ritenere che tali programmi di "primo accesso" possano rappresentare, di per sé, "misure inidonee". Tale valutazione, infatti, dovrebbe esser svolta analizzando in concreto le caratteristiche degli stessi e risentirebbe, com'è ovvio, delle modifiche che, nel tempo, possano intervenire al fine di renderli "impermeabili" alle *minacce della rete*.

Per quanto attiene, viceversa, l'art. 33 C.d.P., la norma dispone che i titolari del trattamento siano tenuti *"… ad adottare le misure minime … volte … ad assicurare il livello massimo di protezione dei dati personali"* ([11]).

Il caso che si esamina in questo scritto deve essere sussunto all'interno della disciplina, ulteriormente definita nel corpo della Parte I del Titolo V, del C.d.P., ossia quella relativa al trattamento mediante strumenti elettronici. Il disposto di cui all'art. 34 C.d.P., che individua le misure di sicurezza *ex* art

9) Cfr. P. TROIANO, *Commento*, in C.M. Bianca, F. Donati Busnelli, a cura di, Protezione dei dati personali – Commentario, Padova, 2007, pag. 705 e F. DI RESTA, *Misure minime, soggetti obbligati e adempimenti*, in AA.VV., Protezione delle informazioni – Privacy e sicurezza, Torino, 2008, pag. 107. In senso conforme, nella giurisprudenza di merito, Giudice di Pace, Bari, 7 giugno 2005, in Riv. Internet, 2005, pag. 573 e ss.

10) In termini concreti, il disposto normativo pare adattarsi alle pratiche di aggiornamento dei c.d. *antivirus*, *patch*, *et alia*, su cui si sofferma, *amplius*, G. ZICCARDI, *Informatica giuridica*, Tomo II, Torino, 2008, pag. 218 e ss.

11) Cfr., art. 33, C.d.P. Sul punto, per il rilievo che esso assume, si rinvia al del Parere del Garante della Privacy del 22 marzo 2004, § 1.

33, prevede che siano adottate le seguenti "misure minime": autenticazione informatica, adozione di procedure di gestione delle credenziali di autorizzazione e utilizzazione di un sistema di autenticazione (cfr. art. 34, comma 1, lett. a), b) e c) del C.d.P.). Inoltre, l'Allegato B (§§ da 1 a 26) fornisce importanti elementi che consentono di tratteggiare con maggiore dettaglio il nucleo delle iniziative volte ad integrare le misure minime ([12]).

Le *misure minime*, nel caso di trattamento con strumenti elettronici si articolano essenzialmente nell'adozione di un "… *sistema di autorizzazione* …" (art. 34, comma 1, lett. a), C.d.P. e §§ 1-11 del Disciplinare) che consenta una "… *autenticazione informatica* …" (*ex* art. 34, comma 1, lett. a) mediante le procedure di gestione delle credenziali di autorizzazione (lett. b).

Elemento centrale del sistema di autenticazione è rappresentato dalle *"credenziali di autenticazione"*, ossia dall'insieme di quei dati e dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati che, ai sensi del § 2 del Disciplinare, possono consistere in un codice per l'identificazione dell'incaricato associato ad una parola chiave riservata, conosciuta solamente dal medesimo.

Proprio la "riservatezza" della *password* – nel suo duplice atteggiarsi di preclusione della sua conoscenza (attuale) e conoscibilità (potenziale), da parte di terzi – rappresenta un elemento di centrale importanza nel tema che ci occupa.

Con riferimento alla parola chiave (c.d. *password*), il Disciplinare, si sofferma sull'individuazione delle circostanze in cui un sistema di chiavi possa ritenersi "debole" favorendo l'accesso da parte di soggetti "terzi".

## II.2.) Sulla sicurezza dei sistemi di "chiavi d'accesso".

Il tema della sicurezza della *password* impone una premessa. Deve ritenersi che la valutazione circa la "forza" o "debolezza" di un sistema di accesso *low authorization*, quale quello che si basa sulla richiesta di inserimento di *username* e *password*, implichi un previo esame empirico basato sull'esperienza sensibile che consenta di distinguere pratiche all'avanguardia ed efficaci da pratiche desuete ed inadeguate.

Una *password* può dirsi tanto più sicura, quanto più complessa ne sia l'individuazione da parte di "terzi". Tale circostanza ha condotto alla ricerca

12) Sul rapporto fra art. 33 e All. B, cfr. M. LUBERTO, *I reati informatici contro il diritto alla privacy. La tutela fornita dal D.Lgs. n. 196 del 2003 e dal Codice Penale*, Giur. Merito, 2008, pag. 898. Con l'ovvia precisazione che il "trattamento", a norma dell'art. 30 C.d.P., deve essere – materialmente – effettuato da incaricati persone fisiche (cfr. Provv. Garante della Privacy, 8 giugno 1999, in Boll. N. 9, pag. 58, Mass. 65).

di tecniche avanzate di autenticazione quali l'individuazione per mezzo di caratteristiche fisiche (impronta digitale, forma della mano, retina *etc.*) rispetto alle quali la tecnica lumeggiata in premessa si presenta alquanto desueta, ma ciò che più conta, del tutto insicura posto che i dati prescelti (ad es. codice fiscale/partita iva) sono nella libera disponibilità di ognuno, mediante poche, semplici operazioni ([13]).

Ne deriva che, nelle more del "primo accesso" da parte del legittimo titolare, altri soggetti potrebbero abusivamente accedere all'interno del "profilo" dello stesso con le più svariate (e meno lodevoli) intenzioni ([14]).

Sembra, quindi, che si possa affermare che *policies* di accesso a banche dati (quali quelle citate in premessa, mediante *username* e *password* di semplice "ricostruzione"), siano, alla luce del disposto di cui all'art. 34, comma 1, lett. a), b) e c) C.d.P., certo permeabili alle minacce della rete. Esse possono, quindi, rappresentare fonte di responsabilità per i titolari ([15]), per inidoneità ai sensi dell'art. 31, ma anche per mancata adozione di "misure minime", ai sensi dell'art. 34, C.d.P.

Vieppiù che, nella fattispecie analizzata in premessa, potrebbe ritenersi che anche altra fase del trattamento venga in considerazione; in particolare, si ha mente alla "raccolta dei dati", *ex* art. 4, comma 1, lett. a), C.d.P. L'esempio può essere rappresentato, ritornando al caso ipotizzato in precedenza, dall'accesso finalizzato alla modificazione dei dati da comunicarsi all'ente (nell'esempio, il consorzio "titolare" del trattamento) al fine della fruizione di agevolazioni.

Tale ulteriore profilo comporta altre, più attente, valutazioni in merito alla prestazione del "consenso" nel peculiare caso di attività economiche.

## II.3.) Consenso al trattamento dei dati in relazione allo svolgimento di attività economiche.

Il Capo III (Tit. I, Parte I) del C.d.P. reca le norme relative alla prestazione del "consenso".

L'art. 24 è volto a disciplinare i casi in cui la prestazione del consenso non sia richiesta. Segnatamente, alla sua lettera c), prevede che il consenso

13) Sul tema, di recente, si confronti Garante della Privacy, Provv. del 07 ottobre 2009, § 4., in Boll. 109/ottobre 2009 con riferimento ad un sistema di "primo accesso" adottato dall'Agenzia delle Entrate.

14) In questo senso, ulteriori lumi possono trarsi dalle indicazioni tecniche contenute nel § 5 e ss. dell'Allegato B, "Disciplinare tecnico in materia di misure minime di sicurezza (artt. da 33 a 36)", Trattamenti con strumenti elettronici.

15) Così la procedura di gestione delle credenziali di autorizzazione richiede che la parola chiave riservata sia nell'esclusivo dominio del soggetto che deve accedere (cfr., F. DI RESTA, *Misure minime*, cit., pag. 111).

non debba esser richiesto ove riguardi registri, elenchi, atti o documenti conoscibili da chiunque ([16]).

Ciò comporta che, qualora i dati oggetto della trasmissione, siano, ad esempio, accessibili da registri come quelli tenuti dalle camere di commercio e *similia* ([17]), al titolare del trattamento non sarà fatto obbligo di richiedere il relativo consenso ([18]).

Questa previsione potrebbe erroneamente consentire di affermare che la comunicazione di dati di questa specie, esoneri dai relativi obblighi (*i.e.* richiesta del consenso) il titolare.

Pare, tuttavia, che tale precetto possa non avere vigore assoluto e incondizionato in confronto dei *soggetti* che svolgano attività economiche (e dei *dati* ad essi relativi) anche alla luce del disposto di cui alla lett. d), art. 24 *cit*.

Il Legislatore ha infatti previsto quale deroga alla regola *ex* art. 24, comma 1, lett. c), C.d.P., quella secondo la quale la prestazione del consenso possa mancare laddove riguardi i dati *relativi allo svolgimento di attività economiche* ([19]).

Occorre, tuttavia, dar contezza del fatto che non ogni dato relativo allo svolgimento di attività economiche rilevi ai fini della (deroga alla) disciplina della previa prestazione del consenso ([20]).

---

16) Non si tratta, tuttavia, di un diritto incondizionato, coma rileva il Garante per la protezione dei dati personali, nel doc. 1570327 del 30.10.2008, ove, al § 3.1., chiarisce che *"… la società risulta effettuare … un trattamento di dati personali che, in termini generali … è da ritenersi lecito nella misura in cui lo stesso riguarda informazioni ricavate da pubblici registri che possono essere utilizzate senza il consenso degli interessati ai sensi dell'art. 24, comma 1, lett. c), del Codice. Nel trattare tale tipologia di dati … [il titolare] … deve tuttavia rispettare i princìpi di cui all'art. 11 del Codice, trattando i dati in modo lecito e secondo correttezza, per finalità non incompatibili rispetto a quelle della raccolta; i dati devono essere altresì esatti, completi, pertinenti e non eccedenti.* [sottolineature di chi scrive]". In dottrina, in senso conforme, R. MONTINARO, *Tutela della riservatezza e risarcimento del danno nel nuovo «codice in materia di protezione dei dati personali»*, in Giust. civ., 2004, 05, 247

17) Il registro dei protesti cambiari (su cui Trib. Roma 10 febbraio 2003).

18) Deve trattarsi, tuttavia, di dati che siano *"… sottoposti ad un regime di piena conoscibilità"*, come rileva il Garante per la Privacy, provv. 11 gennaio 2001, in Boll. n. 16.

19) Così, il Garante interpreta la locuzione "attività economiche" (cfr. provv. del 16 febbraio 1999, in Boll., n. 7).

20) Così si esprime il Garante nel citato provv. 16 febbraio 1999. L'esempio concreto, pure preso in esame nel provv. citato, è quello relativo alla destinazione ad uso personale di beni aziendali. Sul tema, cfr., inoltre, Trib. Venezia, sez. III, 20 giugno 2005, in Danno e resp., 2006, pag. 666 e ss., con riferimento alla divulgazione dei dati relativi ad un rapporto bancario. Più di recente, con valutazioni circa l'esatto ambito applicativo della disciplina sulla *privacy*, in riferimento agli interessi tutelati, cfr. C. Cass., sez. IV, 30 giugno 2009, n. 15327, in Nuova giur. civ., 2010, 1, pag. 71 e Cass. civ., sez. III, 11 febbraio 2009, n. 3358.

Il problema si pone in riferimento a quelle tipologie di "interessati" che svolgano attività economiche che fortemente s'identificano nella persona stessa (quali, per chiarezza, l'attività libero professionale svolta "in proprio"; quella imprenditoriale semplice). Fattispecie in cui la prestazione del "consenso" appaia, in ogni caso, obbligatoria, possono rinvenirsi, per esempio, nella destinazione ad uso personale dei beni aziendali e in tutti quei casi che, soprattutto in contesti aziendali familiari, possono comportare un diverso (o nuovo) trattamento dei dati (determinando, così, una reviviscenza della regola generale *ex* art. 24, C.d.P.).

## III.) Osservazioni conclusive.

In conclusione, può affermarsi che tanto il disposto normativo quanto la giurisprudenza e la prassi in materia, inducono a ritenere che possa rivelarsi rischiosa l'adozione di tecniche di identificazione "semplificate", quali quelle esposte nel par. 1. di questo contributo, possano facilmente essere passibili di una censura alla luce dell'art. 34 C.d.P. in quanto non coerenti col criterio dell'adozione di "… *misure minime* …".

È, poi, utile rammentare che, ove all'atto del primo accesso, il sistema di accreditamento richieda la trasmissione di dati relativi ad attività economiche che, tuttavia, possano riguardare la sfera "privata" del soggetto che trasmette i dati, ulteriori profili d'incompatibilità col C.d.P. – e, segnatamente, coll'art. 24 – potrebbero venire in essere.