

Stefano Allegrezza

*Il problema dell'eredità digitale
nella trasmissione di archivi e biblioteche personali*

Introduzione

La rivoluzione digitale che da almeno un paio di decenni sta trasformando radicalmente ogni settore della società non ha trascurato di operare delle profonde modificazioni anche nella vita personale di ciascuno di noi. La nostra vita sta diventando sempre più 'digitale', così come la nostra identità (si parla, a questo proposito, di 'identità digitale') ed anche la nostra produzione documentaria. Tramite il personal computer, il tablet e lo smartphone lavoriamo, produciamo documenti, leggiamo libri, comunichiamo sui social network, facciamo acquisti, gestiamo il conto corrente e gli investimenti. I servizi digitali, in particolare quelli basati sul *cloud*, sono diventati parte integrante della nostra vita. L'accesso a questi servizi avviene nella maggior parte dei casi tramite credenziali di accesso (dette anche credenziali di 'autenticazione' o 'identificazione') – costituite solitamente da una combinazione di due o più tra la *username* (o *user-id*), il PIN (*Personal Identification Number*) e la *password* – che sono

conosciute solo dall'utente e senza le quali non è possibile accedere.¹ Ciò riguarda anche gli archivi di persona e le biblioteche personali: i documenti sempre più spesso si formano direttamente in formato digitale (si parla, a tal proposito, di 'documenti digitali nativi'); analogamente libri, riviste, giornali vengono sempre più spesso acquistati in formato digitale. In questo modo la componente digitale nei fondi personali sta diventando progressivamente più rilevante.² Inoltre, con la crescente diffusione dei servizi basati sul *cloud*, in molti casi tali fondi vengono archiviati su server remoti, accessibili solo on-line tramite apposite credenziali. Ma in molti cominciano a domandarsi: cosa accadrà ai nostri ricordi digitali quando non ci saremo più? Chi saranno gli eredi dei nostri fondi digitali? Questo articolo intende fornire una risposta a queste domande.

L'eredità digitale

La rivoluzione digitale ha operato una profonda trasformazione anche nel patrimonio personale di ciascuno di noi, aggiungendovi una nuova componente, il cosiddetto *patrimonio digitale*. Esso è composto

¹ Tra le credenziali, la più utilizzata nel mondo digitale è la combinazione costituita da *username* e *password* (autenticazione ad un solo fattore). Tuttavia si stanno diffondendo sempre più sistemi di autenticazione a due o più fattori (*strong authentication*), costituiti dalla combinazione di una *username* e due o più 'fattori di autenticazione', individuati tra i seguenti: 'qualcosa che si conosce' (per esempio una password o il PIN), 'qualcosa che si ha' (come uno smartphone o un token di sicurezza) o 'qualcosa che si è' (come l'impronta digitale, il timbro della voce, l'iride dell'occhio, le sembianze del volto o altro dato biometrico).

² Per *fondi personali* si intendono i «complessi organici di materiali editi e/o inediti raccolti e/o prodotti da persone significative del mondo della cultura, delle professioni e delle arti prevalentemente dalla seconda metà del XIX secolo in poi. Si possono riconoscere alcune categorie di beni culturali, già definite dalle scienze archivistiche, biblioteconomiche e museali, tra cui le biblioteche d'autore, gli archivi di persona, gli archivi culturali, ma anche collezioni di varia natura presenti nei fondi». Cfr. AIB 2019.

da una categoria di *beni* prima sconosciuta, quella dei 'beni digitali' cioè «beni rappresentati in formato binario (ovverosia da una serie di 0 e 1 [...]), di cui si possiedono i relativi diritti di utilizzo, contenuti all'interno di un dispositivo di memorizzazione (fisico o virtuale)». ³ Ad esempio, sono beni digitali i documenti testuali informatici, le fotografie digitali, i documenti sonori digitali, i documenti audiovisivi digitali, i progetti scritti al computer, le ricerche condotte con strumenti informatici, i libri digitali (eBook), la corrispondenza elettronica (e-mail), i beni acquistati e scaricabili on-line, i programmi per elaboratore (software), i nomi di dominio, le monete virtuali ⁴ e, in generale, «qualsiasi 'dato' che sia stato creato dal defunto o su cui lo stesso poteva vantare un diritto di proprietà esclusivo e assoluto, a prescindere dalla sua incorporazione (o incorporabilità) su un supporto di memorizzazione fisico o virtuale». ⁵

Al pari degli altri beni fisici, anche i beni digitali cadono in successione e costituiscono la cosiddetta *eredità digitale*, ovvero il complesso dei lasciti digitali di un soggetto, al cui contenuto, custodito in supporti fisici o virtuali, è possibile accedere il più delle volte solo conoscendo le credenziali di accesso. ⁶

³ Cfr. D'Arminio Monforte 2020a, p. 70.

⁴ Le monete virtuali (o criptovalute) sono monete prive di un controvalore garantito da un soggetto terzo e la cui autenticità e verifica è affidata alla rete creata dagli stessi utilizzatori della valuta attraverso un sistema chiamato *blockchain*. Il meccanismo di funzionamento della tecnologia blockchain è piuttosto complesso; in questa sede, è sufficiente far presente che ciascun titolare crea on-line un suo account e un suo portafoglio (*wallet*) dove trasferisce denaro reale. Ogni criptovaluta reca l'identificativo (ma non il nome) del suo proprietario il quale, sino a quando lo vorrà, potrà restare anonimo. Nel caso di decesso del titolare, se gli eredi non conoscono la password di accesso tutto il denaro ivi versato è perso per sempre, con conseguenze patrimoniali che possono essere di non lieve entità. Nessuno, compreso il fornitore del servizio, sarà infatti in grado di "recuperare" tale password. Tra le monete virtuali la più conosciuta è certamente il Bitcoin. Cfr. D'Arminio Monforte 2017.

⁵ Cfr. D'Arminio Monforte 2020a, p. 71.

⁶ Cfr. D'Arminio Monforte 2017.

Sebbene non risulti adeguata a rappresentare nella sua interezza e complessità il fenomeno della successione digitale, appare utile, anche al fine di comprendere meglio la loro natura, la distinzione tra *beni digitali a contenuto non patrimoniale* e *beni digitali a contenuto patrimoniale* (Fig. 1). I primi, detti anche *beni digitali a contenuto personale o familiare*, sono tutti quei beni suscettibili di essere valutati «soltanto nella loro rispondenza a interessi individuali, familiari, affettivi o sociali»⁷, quali, ad esempio, gli scritti intimi o personali redatti su supporto informatico (compresi i diari on-line, i *blog*, gli appunti personali, i messaggi SMS, i messaggi inviati e ricevuti via *chat*, i messaggi testuali o vocali inviati tramite Whatsapp, etc.), le corrispondenze via e-mail di tipo personale, le fotografie personali e di famiglia, le registrazioni audiovisive (filmati) personali e familiari, e, in generale, tutti i ricordi digitali che hanno un valore affettivo o sentimentale.

I beni a contenuto patrimoniale, invece, «si caratterizzano per il loro valore economico intrinseco e la correlata facoltà di utilizzazione economica che essi attribuiscono al titolare».⁸ Sono beni a contenuto patrimoniale, ad esempio, le fotografie digitali scattate da un fotografo professionista, le registrazioni audiovisive digitali prodotte da un regista, i progetti di un architetto disegnati attraverso programmi di CAD (*Computer Aided Design*), le opere letterarie scritte al computer da uno scrittore, i disegni creati al computer da un grafico, gli studi e le ricerche prodotte con mezzi informatici da un professore universitario, i programmi per elaboratore (software) scritti da un programmatore, gli studi effettuati da un inventore utilizzando strumenti informatici e relativi ad invenzioni brevettabili, e, più in generale, tutte le opere dell'ingegno create con strumenti digitali. Rientrano in questa categoria anche i nomi di dominio, i marchi, le monete virtuali ed i beni digitali acquistati on-line (eBook, film e musica musicale, etc.).

⁷ Cfr. D'Arminio Monforte 2020a, p. 72.

⁸ *Ivi*, p. 71.

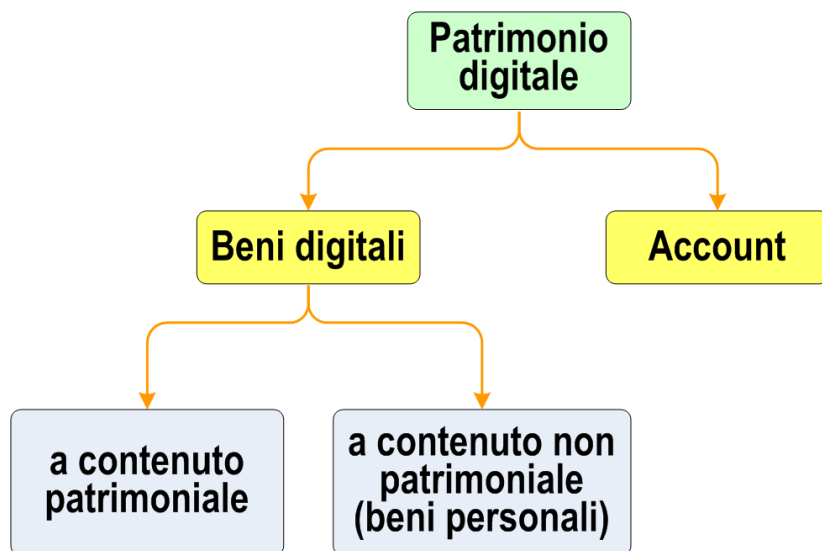


Fig. 1. Classificazione dei beni che costituiscono l'eredità digitale

Sia i beni aventi carattere patrimoniale che quelli aventi carattere non patrimoniale possono poi essere annoverati «tra le opere creative dell'ingegno [...] e, dall'altro lato (o nel contempo), essere equiparati agli 'scritti' di carattere confidenziale o riferiti all'intimità della vita privata».⁹

Il patrimonio digitale è costituito anche dagli *account* digitali, termine con il quale si è soliti definire l'insieme di beni e servizi on-line messi a disposizione da un fornitore (provider) ed accessibili comunemente mediante un meccanismo di identificazione (o autenticazione) che consente ad un utente di essere riconosciuto ed accedervi.¹⁰ Ne esistono di diverse categorie: sono account quelli

⁹ *Ivi*, p. 73.

¹⁰ L'enciclopedia on-line Treccani fornisce la seguente definizione di account: «la registrazione presso un provider di un utente che voglia accedere a un determinato servizio. Per estens., l'insieme delle informazioni (nome, password, etc.), depositate presso il provider medesimo, che identificano l'utente». Si veda <<https://www.treccani.it/vocabolario/account>>

che vengono utilizzati per accedere alla propria casella di posta elettronica (Gmail, Hotmail, Yahoo, Libero, Alice, etc.), per acquistare prodotti su un sito di e-commerce (Amazon, E-bay, Aliexpress, etc.), per effettuare pagamenti on-line (Paypal, Postepay, Googlepay, etc.), per interagire con i Social Network (Facebook, Twitter, Youtube, LinkedIn, Instagram, etc.) o, semplicemente, per effettuare operazioni attraverso la banca on-line. A differenza dei beni digitali, gli account sono sempre di proprietà del gestore, il quale concede in comodato all'utente sia l'account che la password. Anche gli account digitali possono avere un valore patrimoniale che può derivare dal loro contenuto, come nel caso di account di pagamento automatizzato (PayPal) o per il trading on-line (IQ Option, Markets, Plus500, eToro, etc.), oppure dai contratti di sponsorizzazione che lo corredano, dalle recensioni o valutazioni degli utenti (YouTube, E-bay, Trip Advisor, Instagram, etc.).¹¹

Occorre evitare di confondere gli 'account' con le 'credenziali di accesso'; come abbiamo già detto, i primi sono costituiti dai beni e servizi disponibili presso un provider, mentre le credenziali di accesso costituiscono il meccanismo necessario per accedere a tali beni e servizi. Queste ultime, pur non rientrando dal punto di vista tecnico nella categoria dei beni digitali, si rivelano comunque fondamentali in ambito successorio, perché consentono sia la trasmissione *mortis causa* di qualsivoglia diritto sul bene digitale o sul supporto ove è memorizzato, sia l'individuazione dei beni digitali riconducibili al *de cuius*. La trasmissione delle credenziali costituisce uno degli aspetti più complessi da gestire nell'ambito delle successioni di beni digitali, tenuto conto del fatto che queste sono note solo al suo creatore, sono composte di caratteri complessi, sono modificate periodicamente e talvolta associate a un altro dato, come una OTP (One Time Password).

¹¹ Cfr. D'Arminio Monforte 2017.

Le criticità nella trasmissione dell'eredità digitale

Per comprendere quali criticità si possano verificare nella trasmissione di archivi e biblioteche personali, proviamo ad immaginare la situazione che si presenta alla morte di un personaggio illustre quando si tenta di accedere al patrimonio costituito dai fondi personali digitali da lui lasciati in eredità.¹² Nel passato, quando tale patrimonio si sarebbe sedimentato su supporti analogici (si pensi alla carta per i documenti, le fotografie, i libri), era tutto sommato abbastanza semplice recuperare i fondi personali anche a distanza di anni dalla morte del soggetto produttore; sarebbe bastato, infatti, recarsi nei luoghi in cui egli aveva svolto la sua attività (la sua abitazione, il suo studio, etc.) e lì si avrebbe avuto accesso a tutta la documentazione da lui prodotta. Ma oggi, con l'avvento del digitale, le cose sono cambiate drasticamente, come si cercherà di mettere in luce nel seguito.

Innanzitutto, la prima operazione da compiere per recuperare i fondi personali lasciati dal *de cuius* consiste nel cercare di individuare i luoghi (fisici o virtuali) dove essi sono conservati, redigendo una sorta di *inventario*. Si tratta di una operazione che non è né semplice né scontata, a maggior ragione in assenza di un testamento o di disposizioni di ultima volontà. Nel passaggio dal mondo analogico a quello digitale le difficoltà sono aumentate e continueranno ad aumentare sempre più con la crescita del numero di beni e account digitali. Da un lato, infatti, «la vita 'digitale' di una persona può essere del tutto ignota anche ai suoi più stretti familiari e, dall'altro lato, l'immaterialità dei beni facenti parte del patrimonio digitale e il numero di supporti di memorizzazione di quotidiano utilizzo fa sì che questi non siano facilmente reperibili».¹³ La tecnologia «ha, per certi versi, estremizzato l'individualismo e la riservatezza, con la conseguenza che la vita digitale di un individuo può essere oscura persino ai suoi familiari

¹² Cfr. Allegrezza 2018.

¹³ Cfr. D'Arminio Monforte 2020b.

più prossimi».¹⁴

Per prima cosa l'attenzione dovrebbe dirigersi verso i dispositivi tecnologici che potrebbero essere stati utilizzati dal *de cuius* per la produzione di documenti: il personal computer, il notebook, il tablet, lo smartphone, etc. Poi bisognerebbe individuare i supporti di archiviazione da lui utilizzati (*floppy disk*, CD, DVD, Blu-ray disc, chiavette USB, dischi fissi, dischi SSD, etc.): trattandosi di oggetti con una propria 'fisicità', non dovrebbe essere difficile rintracciarli presso la sua abitazione o nel suo studio. Ma già qui si presenta un primo problema legato all'eredità digitale: al di là del fatto che molti di quei dispositivi e supporti potrebbero essere già obsoleti (si pensi ai *floppy disk* di qualche anno fa) e quindi di difficile o impossibile lettura¹⁵, quando si tenterà di recuperare i documenti digitali archiviati su tali

¹⁴ *Ibidem.*

¹⁵ Si tratta del ben noto problema dell'obsolescenza dei supporti di archiviazione. Gli oggetti digitali necessitano di risiedere fisicamente su un 'supporto di archiviazione': può trattarsi del disco fisso del computer dell'utente, di una chiavetta USB, di una memory card; di un nastro magnetico (come quelli utilizzati nei *backup*), di un disco ottico (come i *compact disc* o i DVD) oppure di uno spazio di archiviazione virtuale come quello offerto dai fornitori di servizi *cloud*. Purtroppo, in un periodo di tempo più o meno lungo, tutti i supporti di archiviazione diventano obsoleti. Ciò è legato, da una parte, alla loro limitata durata nel tempo; dall'altra, al fatto che il mercato propone via via supporti sempre più moderni, rendendo di fatto illeggibili quelli che si utilizzavano fino a pochi anni fa e che quindi devono essere sostituiti da altri più moderni. Accanto a questo problema va sempre considerato quello dell'obsolescenza dei formati elettronici: tutti i contenuti digitali, indipendentemente dall'appartenza ad una categoria o ad un'altra (documenti testuali, fotografie, contenuti audio o video, libri, riviste, etc.), sono costituiti in ultima analisi da una sequenza di bit e, quindi, devono essere codificati secondo un certo "formato elettronico" al fine di poter essere letti ed interpretati. Ma anche i formati elettronici diventano obsoleti in tempi che risultano spesso assai brevi, a causa sia della loro rapida evoluzione che del fatto che taluni formati (ad esempio quelli proprietari) dipendono fortemente dagli applicativi software con cui debbono essere interpretati e che nel tempo potrebbero non essere più disponibili. Cfr. Allegrezza 2018

dispositivi vi sarà subito un primo problema da risolvere perché essi risultano sempre più spesso protetti da sistemi di controllo dell'accesso: occorrono delle credenziali di autenticazione per l'accesso ai computer, ai tablet, agli smartphone e perfino per accedere ai documenti registrati su alcuni supporti di archiviazione che utilizzano meccanismi di cifratura per la protezione dei contenuti (come i dischi fissi esterni o le chiavette USB). Se non si conoscono tali credenziali risulta impossibile accedere ai materiali digitali in essi presenti. Oggi, poi, si sta diffondendo sempre più l'utilizzo di meccanismi di accesso di tipo biometrico, collegati, cioè, a caratteristiche fisiche del soggetto produttore (l'impronta digitale, l'iride dell'occhio, il tono della voce, etc.) che, ovviamente, si perdono per sempre alla sua morte, rendendo di fatto impossibile per chiunque accedere ai dispositivi protetti da tali meccanismi. Quindi, quali possibilità ci sono di riuscire ad avere accesso al patrimonio digitale lasciato da un soggetto produttore che si è avvalso di tali meccanismi di autenticazione di tipo biometrico? Praticamente nessuna.

Terminata la rilevazione dei dispositivi e dei supporti di archiviazione 'fisici' occorre rivolgere la propria attenzione agli spazi di archiviazione 'virtuali'. Infatti, sempre più spesso i materiali digitali non vengono più archiviati sui supporti di archiviazione 'fisici' ma sugli 'spazi virtuali' come i servizi di *cloud storage* offerti da Dropbox, Google Drive, OneDrive, Box, Mega, Amazon, etc. La posta elettronica non viene più scaricata 'in locale' (utilizzando i cd. *client* di posta elettronica) ma viene 'lasciata' sui server di posta e gestita tramite servizi remoti (come la *webmail*). Le fotografie personali vengono caricate su servizi di condivisione on-line, come Google Foto. Gli eBook acquistati sono sul server del fornitore del servizio. Di conseguenza, alla morte del personaggio illustre un secondo problema che si presenta è quello di riuscire a sapere in quali spazi virtuali sono collocati i vari 'nuclei' del suo fondo personale. Spesso le informazioni sono frammentarie ed insufficienti; ci si trova a dover rispondere a domande del tipo: il soggetto produttore aveva archiviato dei 'materiali' su Dropbox? su

OneDrive? su Google Drive? su Office 365? Aveva depositato i suoi archivi fotografici su Google Foto? Flickr? Instagram? Possedeva dei profili sui social network (Facebook, Twitter, etc.)? Aveva dei blog? Aveva dei siti web? Aveva delle caselle di posta? Se sì, quali? Su quali server di posta? Quali erano i suoi account? Aveva delle collezioni di libri digitali? Se sì, dove? Spesso è impossibile rispondere a queste domande; nella migliore delle ipotesi si riesce a fornire solo risposte parziali ed incomplete. La maggior parte dei materiali digitali ‘sparsi’ sul web finisce così per scomparire nel nulla.

Sfortunatamente le difficoltà non si esauriscono qui. Infatti, anche nel caso in cui si riesca a sapere dove sono archiviati i vari ‘nuclei’ del fondo personale del soggetto produttore deceduto, ci si imbatte nella difficoltà (e spesso nell’impossibilità) di accedere ad essi, poiché per avere accesso alla webmail, agli spazi virtuali, agli account sui social media, etc. – che nella quasi totalità dei casi sono protetti da sistemi di controllo dell’accesso – occorre conoscere le credenziali di autenticazione (tipicamente costituiti dalla coppia username e password). «Senza tali credenziali, che solitamente nessuno condivide con altri e che quindi si perdono con la morte del soggetto produttore, risulta impossibile per chiunque accedere ai materiali digitali depositati sui vari servizi on-line». ¹⁶

Inoltre, anche qualora si riesca ad entrare in possesso di tali informazioni (magari perché il soggetto produttore, con lucida lungimiranza, aveva comunicato le credenziali di accesso a qualcuno dei suoi congiunti), c’è un ulteriore fattore da considerare: lo scorrere del tempo. Infatti, quando un fornitore di servizi on-line si accorge che un certo servizio non viene più utilizzato da un dato utente, dopo un determinato lasso di tempo provvede alla cancellazione del relativo account e di tutto il materiale digitale ad esso associato. Questo può avvenire, a seconda delle *policy* adottate, in tempi variabili da pochi mesi a qualche anno al più. ¹⁷ I materiali depositati negli spazi virtuali

¹⁶ Cfr. Allegrezza 2020.

¹⁷ Cfr. la sezione “La trasmissione dell’eredità digitale”, *infra*.

possono risultare ancora accessibili a distanza di pochi giorni o di pochi mesi dalla morte del soggetto produttore, ma diventano inaccessibili a distanza di alcuni mesi o alcuni anni al massimo. La situazione non ammette dilazioni ed occorre agire al più presto. Attendere anche solamente pochi mesi potrebbe significare la perdita di tutto il patrimonio digitale.

Appare evidente, quindi, che quando si ha a che fare con archivi e biblioteche digitali personali nessun ritardo è ammesso e gli interventi di salvaguardia devono essere intrapresi subito, pena la scomparsa dei materiali che può avvenire anche solo dopo uno-due anni (a volte anche prima). Come si può intuire l'approccio deve essere diametralmente opposto a quella che si ha nei confronti delle memorie personali analogiche, laddove è possibile porre in essere interventi anche a distanza di anni o decenni dalla morte del soggetto produttore.

Occorre poi considerare anche il fatto che molti dei servizi che oggi vengono utilizzati dalla maggioranza delle persone un domani potrebbero non esistere più, magari perché l'azienda che li offre è in difficoltà economiche e decide di chiudere un determinato servizio non più redditizio, oppure perché, banalmente, gli interessi degli utilizzatori si spostano verso altre piattaforme. Ad esempio cominciano ad essere non così infrequenti i casi in cui i libri digitali diventano 'illeggibili' a distanza di pochi anni – a volte anche mesi – dal loro acquisto. A questo proposito nel 2019 sollevò molto scalpore la notizia che Microsoft avrebbe chiuso la sezione "Libri" del Microsoft Store perché il servizio non era più sostenibile sotto il profilo economico, impedendo così l'accesso ai milioni di libri presenti nelle biblioteche personali digitali degli utenti.¹⁸

¹⁸ «Quando si chiude un negozio di libri digitali non è come quando si chiude una libreria. In quest'ultimo caso i libri venduti restano ai clienti, ma gli eBook, invece, smettono di funzionare. Se spegni i server, gli eBook spariscono, o meglio: spariscono i complicati contratti di licenza (i DRM) che consentono ai clienti di leggere gli eBook. I clienti di Microsoft che avevano comprato eBook sul loro negozio on-line a partire dall'inizio del mese hanno visto sparire i loro libri digitali».

Oppure possono verificarsi veri e propri ‘incidenti’ informatici capaci di distruggere in un solo colpo milioni e milioni di beni digitali, come nel caso dell’incendio di un *datacenter* dell’azienda OVH che si è verificato il 10 marzo 2021.¹⁹ Il caso è paradigmatico perché dimostra quanto sia imprudente affidare i propri beni digitali alle infrastrutture basate sul *cloud* e gestite da privati.²⁰ Nel caso in questione, il provider francese si è tirato fuori da qualsiasi responsabilità attribuendola alla negligenza dei clienti. Infatti, andando a leggere fra le infinite clausole del contratto generale di servizio con OVH, quello che molti clienti hanno firmato negli anni, si legge quanto segue:²¹

OVHcloud non effettua alcun backup particolare dei contenuti memorizzati nell’ambito dei Servizi. Pertanto, il Cliente è l’unico responsabile dell’adozione di tutte le misure necessarie per salvaguardare i suoi dati al fine di

Cfr. Cau 2019.

¹⁹ Il caso, che ha avuto una risonanza mondiale, ha riguardato uno dei *datacenter* dell’azienda francese OVH (il nome è un acronimo di “On Vous Héberge”, “Noi Vi Ospitiamo” in italiano), nata nel 1999 da un’idea di Octave Klaba, allora studente del terzo anno presso l’ICAM di Lille. Ha sede a Roubaix, nel nord della Francia, ma i suoi *datacenter* sono sparsi in tutta Europa. La società offre i suoi servizi in numerosi Paesi tra cui Canada, Finlandia, Francia, Germania, Irlanda, Italia, Polonia, Regno Unito, Stati Uniti; possiede 17 *datacenter* per un totale di 250 mila server. Nel 2019, a vent’anni dalla sua fondazione, Ovh contava più di 1,5 milioni di clienti nel mondo. Durante la notte tra il 9 e il 10 marzo 2021, uno dei quattro *datacenter* del campus di Strasburgo, uno dei più grandi d’Europa, è andato a fuoco ed è stato completamente distrutto. L’incendio ha avuto un impatto grave per le aziende e i professionisti, con centinaia di siti web off-line e conseguenti disagi in tutto il mondo. In Italia, per esempio, hanno registrato problemi i siti istituzionali di diversi Comuni (Pavia, Cattolica, Trapani, etc.) e numerosi piccoli enti, nonché tantissimi utenti singoli che avevano depositato i propri beni digitali sui server del *datacenter* distrutto.

²⁰ Su questo punto si rimanda ai risultati del progetto internazionale InterPARES Trust, che si è occupato di investigare l’affidabilità del cloud per la conservazione digitale a lungo termine. Cfr. <<https://interparestrust.org>>.

²¹ Cfr. le *Condizioni Generali di Servizio* disponibili sul sito del provider OVH all’indirizzo <<https://www.ovh.it/supporto/contratti>>.

proteggerli contro il rischio di perdita o alterazione, indipendentemente dalla causa. [...] OVHcloud non è responsabile per perdita, danneggiamento, alterazione di tutto o parte del contenuto (comprese informazioni, dati, applicazioni, file o altri elementi) presente nell'Infrastruttura.

In sostanza, il provider francese ha escluso ogni attribuzione di responsabilità nei suoi confronti e tantissimi utenti singoli, che avevano depositato i propri archivi di persona o le proprie biblioteche personali sui server di OVH, pensando che fossero al sicuro semplicemente perché 'depositati sul *cloud*', si sono ritrovati senza più nulla.

Anche per questo, oltre che per gli altri motivi già messi in evidenza in precedenza, risulta molto difficile (anzi, il più delle volte impossibile) accedere ai beni digitali lasciati da una persona defunta, siano essi costituiti dall'archivio delle sue e-mail o da quello dei suoi libri digitali. Come si vedrà nel seguito, le norme che riguardano la successione dei beni digitali non sono ancora ben definite e molto è lasciato alla libera interpretazione dei giudici con la conseguenza che in più di un'occasione i familiari di un defunto non sono riusciti ad accedere ai suoi beni digitali. In questo modo, sempre più spesso i fondi personali restano conservati esclusivamente in forma di bit e spesso rimangono per sempre celati dietro a password imperscrutabili e protette a volte da legislazioni che non hanno ancora contemplato, se non in maniera frammentaria e certamente insufficiente, il problema dell'eredità digitale. La conseguenza è che si sta rischiando di lasciare agli eredi il 'nulla digitale' anziché i fondi personali del soggetto deceduto.

Le criticità appena delineate fanno comprendere come non sia affatto scontata la trasmissione dell'eredità digitale nel caso dei fondi personali. Ci si potrebbe domandare se sia possibile recuperare il patrimonio digitale del *de cuius* in base alle disposizioni di legge, anche in considerazione delle norme sulla protezione dei dati personali che potrebbero essere invocate dai fornitore di servizi on-line per negare l'accesso. A tal proposito occorre evidenziare che il Regolamento generale sulla protezione dei dati 679/2016, comunemente conosciuto

come GDPR,²² non si applica ai dati personali delle persone decedute ed è demandata alle singole legislazioni nazionali degli Stati Membri dell'Unione la possibilità di prevedere delle norme interne riguardanti il trattamento dei dati personali delle persone decedute.²³ In tal senso ha provveduto il Decreto legislativo n. 101 del 10 agosto 2018, introducendo nel Decreto legislativo n. 196 del 30 giugno 2003 (Codice in materia di protezione dei dati personali) una specifica disposizione, l'art. 2-terdecies (Diritti riguardanti le persone decedute), specificamente dedicato al tema della tutela *post mortem* e dell'accesso ai dati personali del defunto. Infatti, tale articolo stabilisce quanto segue:

1. I diritti di cui agli articoli da 15 a 22 del Regolamento riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.
2. L'esercizio dei diritti di cui al comma 1 non è ammesso nei casi previsti dalla legge o quando, limitatamente all'offerta diretta di servizi della società dell'informazione, l'interessato lo ha espressamente vietato con dichiarazione scritta presentata al titolare del trattamento o a quest'ultimo comunicata.
3. La volontà dell'interessato di vietare l'esercizio dei diritti di cui al comma 1 deve risultare in modo non equivoco e deve essere specifica, libera e informata; il divieto può riguardare l'esercizio soltanto di alcuni dei diritti di cui al predetto comma.
4. L'interessato ha in ogni momento il diritto di revocare o modificare il divieto di cui ai commi 2 e 3.
5. In ogni caso, il divieto non può produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato nonché del diritto di difendere in giudizio i propri interessi.

²² Regolamento (UE) 2016/679 del Parlamento europeo e del consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

²³ Infatti, il Considerando 27 del Regolamento europeo 2016/679 così recita: «Il presente regolamento non si applica ai dati personali delle persone decedute. Gli Stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute».

Quindi, grazie all'art. 2-terdecies, comma 1, del Decreto legislativo n. 196/2003 (sempreché risulti applicabile la legislazione italiana) è possibile ottenere – in forza dell'art. 15 del GDPR²⁴ – l'accesso ai beni digitali del defunto archiviati sugli account dei vari provider (che hanno la veste di titolari del trattamento). Secondo la dottrina maggioritaria si tratta, dunque, «di 'persistenza', oltre la vita della persona fisica, di quei diritti – quali il diritto di accesso, di rettifica, di limitazione di trattamento, di opposizione, ma anche il diritto alla cancellazione ed alla portabilità dei dati – da parte di determinati soggetti legittimati all'esercizio dei diritti stessi (il cosiddetto 'esercizio *post mortem* dei diritti dell'interessato')». ²⁵ Tuttavia, il secondo comma del medesimo articolo introduce come limite l'espreso divieto con dichiarazione scritta presentata dal *de cuius*, mentre era in vita, al titolare del trattamento o a quest'ultimo comunicata. Tale divieto, tuttavia, non può produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato nonché del diritto di difendere in giudizio i propri interessi. ²⁶

²⁴ L'art. 15, comma 3 del GDPR stabilisce che «Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune».

²⁵ Cfr. Arezzo – Adamo 2021.

²⁶ Oltre all'art. 2 terdecies del D.Lgs. n. 196/2003, già citato, è possibile avanzare richieste di accesso anche ai sensi dell'art. 6 (Liceità del trattamento), par. 1, lett. b e lett. f del Regolamento Europeo 679/2016. Infatti, tale articolo stabilisce che «1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: [...] b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; [...] f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore».

Alcuni esempi meritevoli di considerazione

All'atto pratico l'applicazione delle norme si è rivelata particolarmente problematica. Uno dei primi casi che ha mostrato a quali difficoltà si può andare incontro quando si cerca di accedere all'eredità digitale di un soggetto deceduto in assenza di disposizioni testamentarie risale al 2004.²⁷ Il 13 novembre di quell'anno, un giovane soldato marine americano di nome Justin Ellsworth venne ucciso da una bomba mentre si trovava di stanza in territorio iracheno. Fino al momento della morte, la maggior parte dei contatti con i suoi cari era avvenuta attraverso lo strumento della posta elettronica (all'epoca i social media non erano ancora diffusi) ed in particolare utilizzando un account sul noto servizio di posta elettronica Yahoo!. Successivamente alla sua morte, i genitori del ragazzo, intenzionati a recuperare la corrispondenza con il figlio, inoltrarono al provider del servizio di posta elettronica una richiesta per ottenere l'accesso all'account del figlio ove erano archiviate le e-mail ricevute e inviate. Yahoo! respinse la richiesta per diverse ragioni. In primo luogo, il contratto di servizio sottoscritto elettronicamente da Justin era munito di una clausola di 'no right of survivorship and no trasferability' in forza della quale l'account non

²⁷ Il caso ebbe una vasta eco su tutti i mass media dell'epoca. Ad esempio, il quotidiano "La Repubblica", in un articolo del 21 dicembre 2004 dal titolo *Iraq, muore marine: Yahoo nega password e-mail ai familiari*, riporta la notizia in questo modo: «Senza la necessaria parola-chiave, la casella di e-mail di un defunto non può essere consultata dai suoi familiari, neppure se si tratta di un marine ucciso in Iraq. Yahoo, il colosso americano di internet, ha ribadito la regola ai familiari del caporale Justin Ellsworth, ucciso il mese scorso da una bomba nella provincia irachena di Al Anbar. I portavoce di Yahoo hanno spiegato che la tutela della privacy dei loro clienti non ammette eccezioni e per questo la casella di e-mail è destinata a restare sigillata sul web, una sorta di memoriale virtuale che nessuno potrà visitare. [...] Yahoo! ha espresso solidarietà alla famiglia per la perdita, ma ha ribadito di non poter violare le regole della privacy». Cfr. <<https://napoli.repubblica.it/dettaglio-news/new-york-17:34/758730>>.

poteva essere trasferito e ogni diritto sullo stesso e sui suoi contenuti sarebbe cessato con la morte del contraente. In secondo luogo, lo stesso contratto prevedeva un'altra clausola per la quale il provider non avrebbe potuto comunicare a terze persone le informazioni contenute nell'account, se non dietro un'ordinanza del giudice. Si noti che quella dei genitori era anche una corsa contro il tempo. «Yahoo!, infatti, permette che un account di posta elettronica resti inutilizzato al massimo tre mesi, dopodiché lo chiude. I tre mesi scadranno il prossimo primo febbraio. Se i genitori di Justin non riusciranno ad entrare nell'account prima di quella data, le sue parole andranno perse per sempre».²⁸ I genitori di Justin, in qualità di eredi, tentarono quindi causa contro Yahoo! sostenendo che la casella di posta elettronica poteva essere equiparata ad una cassetta di sicurezza il cui contenuto sarebbe dovuto cadere in successione e, dopo un lungo iter giudiziario, il tribunale di Oakland County diede ragione ai genitori del ragazzo e obbligò il provider a consegnare loro, su un CD, le e-mail ricevute dal figlio, ma non la password per poter accedere all'account in forza della clausola di intrasferibilità prevista nel contratto. La vicenda ebbe rilevanza mondiale e rappresentò probabilmente il primo caso in cui venne alla ribalta il problema della trasmissione dell'eredità digitale.

Un altro caso esemplificativo è quello di una ragazza tedesca di 15 anni che, nel 2012, venne investita e uccisa da un treno della metropolitana a Berlino.²⁹ Sin da subito, le circostanze della morte non erano apparse chiare, tanto che i genitori avevano pensato d'indagare per verificare se si trattasse di una tragica fatalità, di un suicidio o ancor

²⁸ Cfr. l'articolo *Il figlio muore, password protetta. Hacker in aiuto della famiglia* pubblicato sul quotidiano La Repubblica e disponibile all'indirizzo <https://www.repubblica.it/2004/1/sezioni/scienza_e_tecnologia/mailedato/mailedato/mailedato.html>.

²⁹ Si veda l'articolo *Facebook, figlia muore e gli amministratori del social negano ai genitori l'accesso al profilo*, pubblicato il 13 Novembre 2017 sulla rivista on-line "Mr. Informatico" e disponibile all'indirizzo <<https://www.mrinformatico.it/facebook-figlia-muore-e-amministratori-del-social-negano-ai-genitori-laccesso-al-profilo>>.

peggio di un episodio di bullismo. Allora, per tentare di dirimere tutti gli interrogativi la famiglia aveva pensato di effettuare una verifica sul profilo Facebook della figlia, sperando di trovare delle risposte anche nelle *chat* dei messaggi privati. I genitori si erano quindi rivolti al social network chiedendo di poter accedere alla parte riservata del profilo Facebook, ma la richiesta era stata bocciata e, dietro segnalazione di un amico della ragazza morta, il social network aveva trasformato il suo profilo in un profilo 'commemorativo' dove gli amici possono lasciare messaggi o dediche, ma sulla quale nessuno può modificare i dati o leggere i messaggi privati. I genitori non si arresero e portarono la vicenda in tribunale. In tal sede Facebook assunse di non poter dar seguito alla richiesta dei genitori «in quanto, da un lato, l'account non era suscettibile di trasmissione *mortis causa* in base alle *policy* aziendali e alle condizioni generali di contratto sottoscritte in fase di registrazione e, dall'altro, l'istanza non era accoglibile in ragione sia di un divieto di divulgazione dei contenuti previsto dalla legge tedesca, sia del dovere di tutela della personalità del defunto imposto dal GDPR.³⁰ Nonostante un travagliato iter giudiziario che ha visto prima l'accoglimento della richiesta dei genitori e successivamente il rigetto, la domanda veniva definitivamente accolta dalla Suprema Corte tedesca, stabilendo che il profilo Facebook dell'adolescente fosse da intendere coperto dalla legge sull'eredità, inclusi i contenuti digitali creati dalla ragazza, per cui i genitori, in qualità di eredi, erano legittimanti ad accedere all'account.

Sempre nel 2012 si verificò un altro caso degno di attenzione, quello della modella Sahara Daftary, morta in Inghilterra dopo essere precipitata dall'appartamento del marito posto al 12° piano di un palazzo di Manchester. Allo scopo di ricercare elementi utili a chiarire alcune circostanze sospette sulla morte, i genitori chiesero a Facebook l'accesso all'account della modella, ma il social network rigettò la richiesta in quanto contraria alle proprie *policy* e alle norme federali americane

³⁰ Cfr. eLegacy 2020.

poste a tutela della confidenzialità delle comunicazioni. Un accesso sarebbe stato possibile solo con il consenso (precedentemente acquisito) dell'interessato. La Corte Federale per il Northern District della California, pur sposando la tesi difensiva di Facebook (il quale diede in ogni caso la possibilità ai genitori di richiedere la cancellazione dei dati o la trasformazione del profilo in 'commemorativo'), riconobbe comunque una possibilità di divulgazione dei dati ivi memorizzati su base volontaria.

Nel 2014 accadde un altro caso paradigmatico, quello della scrittrice iraniana Marsha Mehran, autrice nel 2005 di un best seller di fama internazionale dal titolo "Caffè Babilonia". Dopo la sua morte improvvisa, i genitori si rivolsero a Google per richiedere di poter verificare se all'interno degli spazi virtuali sul Google Drive, quotidianamente utilizzato dalla scrittrice, non vi fossero altre opere letterarie della figlia. Dopo alcuni negoziati e l'avvio di un'azione giudiziaria, Google consegnò al padre un CD con gli scritti della figlia conservati nel *cloud*.

Un altro caso degno di nota e molto conosciuto, anche per l'eco notevole che ha avuto su tutti i mass media, è quello legato alla strage di San Bernardino (California) che avvenne nel 2015. Il 2 dicembre di quell'anno i due terroristi Syed Farook e Tashfeen Malik, marito e moglie, dopo aver lasciato la propria figlia in custodia alla madre di Farook, si recarono all'Inland Regional Center, un centro sociale per disabili a San Bernardino, in California, a volto coperto e armati di pistole e fucili. Una volta entrati, aprirono il fuoco contro la folla, uccidendo all'istante 14 persone e ferendone gravemente 22, tra cui due poliziotti. Due complici di Farook vennero uccisi quattro ore dopo in un conflitto a fuoco con la polizia, ma prima di morire furono in grado di distruggere i loro telefoni cellulari personali vanificando la possibilità di recupero dei dati da parte della polizia. Al contrario, il telefono di Farook, un iPhone 5C, venne recuperato intatto, ma risultava bloccato da un codice di blocco a 4 cifre e impostato per la cancellazione di tutti i dati dopo dieci tentativi falliti nell'inserimento del

codice di blocco, opzione presente nei dispositivi iPhone. Nella speranza di ottenere prove decisive riguardo la strage, il Federal Bureau of Investigation (FBI) e lo U.S. Department of Justice (DoJ) chiesero ad Apple di produrre un software che consentisse di 'bypassare' i sistemi di sicurezza del dispositivo e, quindi, di 'sbloccare' l'iPhone, ma la società, adducendo sia motivazioni tecniche che giuridiche, rifiutò perché acconsentendo a tale richiesta avrebbe contravvenuto alle politiche commerciali dell'azienda.³¹ Da qui scaturì una causa legale che sarebbe dovuta culminare nell'udienza prevista per il 22 marzo 2016 nella quale il giudice si sarebbe dovuto pronunciare in merito all'accesa disputa, ma il giorno prima dell'udienza l'FBI chiese una proroga temporale dichiarando di aver trovato una terza parte in grado di sbloccare l'iPhone 5C, oggetto di sequestro.³² Il 28 marzo 2016,

³¹ L'FBI aveva richiesto alla Apple di realizzare una versione speciale del sistema operativo iOS da installare sul telefono al fine di aggirare il blocco. Ma un simile strumento, finito nelle mani sbagliate, avrebbe messo a repentaglio la sicurezza di milioni di utenti iPhone e per questo Apple si era opposta. In un messaggio ai propri clienti, il CEO di Apple, Tim Cook, aveva dichiarato che costruire una 'back door' per accedere ai dati criptati dell'iPhone di Syed Farook avrebbe costituito un precedente 'troppo pericoloso'. Cfr. l'articolo *Strage San Bernardino, Apple si oppone all'ordine del giudice di sbloccare dati iPhone del killer*, pubblicato da "Il fatto quotidiano" il 17 febbraio 2016 e disponibile all'indirizzo <<https://www.ilfattoquotidiano.it/2016/02/17/strage-san-bernardino-apple-si-oppone-allordine-del-giudice-di-sbloccare-dati-iphone>>.

³² Nel 2017, ad un anno dalla conclusione dello scontro legale tra Apple e l'FBI, la senatrice democratica Dianne Feinstein rivelò che il prezzo pagato dall'FBI per sbloccare l'iPhone 5C del terrorista Syed Farook era pari a 900.000 dollari. L'identità del soggetto che avrebbe aiutato l'FBI nelle operazioni di sblocco è stata mantenuta riservata, ma le indiscrezioni più accreditate hanno suggerito che la misteriosa "terza parte" fosse la Cellebrite, azienda israeliana che vende soluzioni per lo sblocco dei cellulari alle forze di polizia di tutto il mondo; altre fonti hanno suggerito che a collaborare con l'FBI sia stato invece un gruppo di hacker e non una specifica azienda. Cfr. l'articolo *Ecco quanto ha pagato l'FBI per sbloccare l'iPhone del terrorista San Bernardino*, pubblicato il giorno 8 maggio 2017 su La Stampa on-line, <<https://www.lastampa.it/tecnologia/news/2017/05/08/news/ecco-quanto-ha-pagato-l-fbi-per-sbloccare-l-iphone-del-terrorista-san-bernardi>>

l'FBI annunciò di aver provveduto allo sblocco del dispositivo e di aver recuperato i dati d'interesse investigativo e quindi, nello stupore generale, ritirò la richiesta nei confronti della Apple.

Merita una segnalazione il caso che si è concluso nel 2019, dopo quattro anni di battaglie legali che sono stati necessari alla londinese Rachel Thompson per costringere Apple a sbloccare l'iPhone del marito Matt morto suicida.³³ La storia di Rachel e Matt iniziò ai tempi dell'università, quando lei aveva 19 anni e lui 18. Nel 2019, dopo dieci anni di matrimonio, nacque la loro prima ed unica figlia Matilda. Matt era appassionato di fotografia e legatissimo a Matilda e le scattava foto e video in ogni circostanza e luogo: mentre era in braccio alla mamma, mentre muoveva i primi passi, mentre giocava. Con il tempo, l'iPhone di Matt si trasformò nell'album digitale di famiglia. Ma nel 2015, senza aver mai lasciato intendere alcunché, Matt decise improvvisamente di togliersi la vita a soli 39 anni. Nel dramma, Rachel e Matilda cercarono di trovare conforto nei ricordi catturati dalle fotografie e dalle registrazioni video del padre, ma tutti i loro ricordi di famiglia, 4.500 foto e 900 video, erano archiviati nell'iCloud di Matt, accessibile solo attraverso il cellulare del marito di cui, tuttavia, non conoscevano il codice necessario per poterlo sbloccare: il loro mondo era lì ma 'intrappolato' in una cassaforte inaccessibile. Rachel provò a chiedere lo sblocco dell'iPhone in un negozio Apple di Londra, ma senza successo. Scrisse allora direttamente alla Apple ma anche qui trovò un muro: l'azienda liquidò la faccenda dichiarando che avrebbe 'sbloccato' lo smartphone solo dietro un'ordinanza del tribunale. Rachel si rivolse allora all'autorità giudiziaria dando avvio ad una battaglia legale che si protrasse fino al 2019, quando un giudice della Central London County Court ordinò ad Apple di consegnarle i codici per consentire lo sblocco del cellulare del marito ed accedere finalmente alle foto ed ai video depositati sull'iCloud.

no-1.34596398>.

³³ La storia viene raccontata da "Il fatto quotidiano", <<https://www.ilfattoquotidiano.it/2019/05/16/dopo-anni-ottiene-lautorizzazione-a-sbloccare-liPhone-del-marito-morto-suicida-la-storia-di-rachel/5184207>>.

Quelle appena viste sono solamente alcune delle innumerevoli vicende che, nel corso degli ultimi anni, hanno costretto gli eredi ad affrontare lunghi e costosi iter legali nel tentativo, non sempre fruttuoso, di veder riconosciuto il loro diritto di accesso all'eredità digitale. Tuttavia, una recente sentenza del 2021 ha aperto nuove prospettive per quanto riguarda la trasmissione dell'eredità digitale, almeno in Italia. Tutto è nato dalla vicenda di un giovane, chef di professione, deceduto nel 2020 in un incidente stradale. Lo smartphone del giovane, un iPhone X, era andato distrutto nello schianto, ma le foto e i video sincronizzati on-line e conservati nell'iCloud risultavano comunque recuperabili; quest'ultimo, infatti, aveva un account ID Apple e utilizzava costantemente sistemi di sincronizzazione tra il dispositivo ed il *cloud*. I genitori, distrutti dal dolore per la tragica perdita del figlio, avevano espresso la volontà di recuperare i dati ivi archiviati, consistenti non solo in fotografie e video ma anche in ricette di cucina, anche allo scopo di realizzare un progetto dedicato alla sua memoria (ad esempio, un libro di ricette). Per tale motivo avevano più volte contattato Apple, ma la società, invocando le norme sulla privacy, si era rifiutato di fornirli ai familiari pretendendo, per consentire l'accesso ai dati contenuti dell'ID Apple, un ordine del Tribunale con determinati requisiti.³⁴ I genitori avevano allora adito le vie legali, presentando un ricorso d'urgenza ex artt. 669 bis e 700 c.p.c. Il Tribunale di Milano - prima Sezione Civile, con la sentenza del 9 febbraio 2021, riteneva la

³⁴ Come emerge dalla lettura delle sentenza, al fine di concedere l'accesso Apple aveva richiesto un ordine del tribunale che specificasse: 1) che il defunto era il proprietario di tutti gli account associati all'ID Apple; 2) che il richiedente fosse l'amministratore o il rappresentante legale del patrimonio del defunto; 3) che, in qualità di amministratore o rappresentante legale, il richiedente agisse come "agente" del defunto e la sua autorizzazione costituisse un "consenso legittimo", secondo le definizioni date nell'*Electronic Communications Privacy Act*; 4) che il tribunale ordinasse ad Apple di fornire assistenza nel recupero dei dati personali dagli account del defunto (che potrebbero contenere anche informazioni o dati personali identificabili di terzi). Cfr. la sentenza disponibile all'indirizzo <<https://www.iurishub.it/wp-content/uploads/2021/02/Apple-eredità-digitale-Tribunale.pdf>>.

domanda dei genitori meritevole di accoglimento, «stante la volontà degli stessi di realizzare un progetto a fini commemorativi del ragazzo, il legame esistente tra genitori e figli e l'assenza di un divieto espresso dell'interessato defunto»³⁵ ed ordinava in via cautelare d'urgenza ad Apple di fornire ai genitori i contenuti digitali dall'account del figlio. In questo modo il Tribunale ravvisava l'esistenza delle "ragioni familiari meritevoli di protezione" richieste dall'art. 2-terdecies del Codice in materia di protezione dei dati personali.³⁶ Merita notare che la vicenda evidenzia, come si è già auto modo di far notare, la necessità di agire al più presto per il recupero dei fondi personali digitali, pena la loro 'cancellazione'; infatti, il giudice ha riconosciuto la sussistenza del cd. *periculum in mora* (il pericolo cioè di un danno derivante da un ritardo nella decisione), rappresentato dal sistema informatico utilizzato dalla stessa Apple che – dopo un periodo di inattività prolungata di un account – avrebbe proceduto in automatico alla cancellazione definitiva di tutti i contenuti digitali.

La trasmissione dell'eredità digitale

La trasmissione dell'eredità digitale costituisce un problema serio, che sta assumendo progressivamente rilevanza. Oggi la situazione sta lentamente migliorando: alcuni fornitori di servizi on-line stanno correndo ai ripari e prevedono nei loro contratti soluzioni adeguate per soddisfare le esigenze degli eredi e, allo stesso tempo, preservare la riservatezza del *de cuius*. Anche dal punto di vista normativo, grazie all'intervento della Corte Europea e ai provvedimenti in materia di

³⁵ Cfr. Arezzo – Adamo 2021.

³⁶ Dal disposto del citato art. 2-terdecies appare evidente come i ricorrenti siano comunque legittimati ad esercitare il diritto di accesso ai dati personali del proprio figlio improvvisamente deceduto, legittimazione desumibile dal fatto che, oltre ad essere eredi dello stesso, agiscono in ogni caso a tutela dell'interessato, per ragioni familiari meritevoli di protezione.

privacy (da ultimo: il Regolamento Europeo n. 679/2016) in particolare, si sono registrati sviluppi significativi nel contesto giuridico sia italiano che europeo.

Purtroppo la legge italiana non è sempre applicabile. Molti fornitori di servizi digitali, infatti, hanno sede negli Stati Uniti o, comunque, in Stati extraeuropei che hanno una legislazione differente ed hanno adottato leggi sulla privacy molto diverse da quelle europee. A questo si aggiunga il fatto che le condizioni di utilizzo dei servizi – che l'utente accetta con noncuranza, a volte senza nemmeno leggerle – rinviano nella quasi totalità dei casi ad una legislazione e ad un Tribunale straniero. Generalmente le condizioni generali del servizio dichiarano applicabile le leggi della California, sotto la giurisdizione esclusiva della Contea di Santa Clara, nella Silicon Valley in California (U.S.A.), rinviando ad un diritto ignoto e la cui applicazione contempla dei costi insostenibili per chi non conosce quella legge e si trova al di qua dell'oceano.³⁷ Si comprendono, perciò, le difficoltà alle quali possono andare incontro gli eredi allorquando, dopo la morte del titolare dell'account, soprattutto se le credenziali (username e password) non sono note, si trovino a richiedere tutti i beni digitali del *de cuius*. Gli eredi dovranno contattare il fornitore di servizi e dimostrare il proprio diritto all'accesso secondo una normativa profondamente diversa da quella italiana. La stessa giurisdizione, in caso di controversia, non è quella italiana, ma quella dello Stato in cui è domiciliato il prestatore del servizio web. Già la distanza, da sola, rappresenta un serio problema, per non parlare della necessità di rivolgersi a un avvocato del posto per far valere i propri diritti.

Il rischio concreto è quello di non riuscire a far valere i propri diritti e non riuscire ad accedere ai beni digitali, e semmai di riuscirci dopo lunghe e faticose battaglie legali, quando ormai i beni saranno già stati cancellati in automatico dai server per 'inattività'. Sotto questo pun-

³⁷ Generalmente, le filiali italiane dei grandi operatori negano qualunque competenza sui servizi offerti su Internet. Questi vengono presentati come insediati in Paesi stranieri scelti soprattutto per il loro fisco favorevole. Cfr. Argella 2017.

to di vista occorre precisare che ogni 'social network' ha un modo diverso di gestire la morte di un utente, ma nella quasi totalità dei casi viene prevista la cancellazione dell'account e di tutto il materiale digitale in esso contenuto dopo un certo periodo di inattività; inoltre, viene sistematicamente esclusa la possibilità per gli eredi di ottenere le informazioni di accesso all'account della persona scomparsa.³⁸

Come scrive Ziccardi, autore tra l'altro di una delle prime opere italiane dedicate al tema, «le grandi aziende tecnologiche mirano, di solito, ad anticipare la volontà dell'utente medio, dando la possibilità ai loro clienti di nominare, tramite 'finti testamenti' (che, in realtà, sono semplici atti privati), degli eredi digitali».³⁹

Ad esempio, Facebook consente ai parenti o agli amici del defunto di chiedere che il profilo del *de cuius* venga trasformato in un 'account commemorativo', nel quale solo gli amici possono aggiungere commenti. In alternativa si può chiedere la cancellazione dell'account o la sua disattivazione. Nel secondo caso l'account viene bloccato, ma rimane sui server di Facebook, pur non essendo accessibile, e può essere eventualmente riattivato.⁴⁰ La piattaforma social rende noto in maniera esplicita che le credenziali di accesso non saranno fornite a nessuno – neanche agli eredi – perché ciò viola le regole di Facebook:⁴¹

Gli account commemorativi permettono ad amici e familiari di raccogliere e condividere ricordi di una persona che è venuta a mancare. Quando un

³⁸ Cfr. Carraffa 2016.

³⁹ Cfr. Ziccardi 2017, p. 16.

⁴⁰ I profili "commemorativi" prevedono l'inserimento della frase "In memoria di" prima del nome del defunto. Le impostazioni sulla privacy determinano se su questa pagina del profilo possano essere pubblicati dei post e condivisi dei contenuti. Gli account commemorativi non appaiono più tra i suggerimenti di amicizia. Allo stesso modo non è più possibile accedere all'account, a meno che non si diventi un 'contatto erede'. Oltre alle pagine commemorative Facebook raccomanda di creare un gruppo per la condivisione del dolore e di invitarvi le persone che potrebbero essere interessate.

⁴¹ Cfr. <<https://www.facebook.com/help/requestmemorialization>>.

account viene reso commemorativo, ne preserviamo la sicurezza impedendo a chiunque di accedervi. La nostra normativa prevede di rendere commemorativo l'account di una persona che è venuta a mancare se ci viene richiesto da un familiare o da uno degli amici più stretti. Tieni presente che nemmeno in queste circostanze possiamo fornire le informazioni di accesso all'account di un'altra persona. Le normative di Facebook non consentono di accedere all'account di un altro utente.

Tuttavia, sin dal 2011 Facebook consente al proprietario di un profilo di indicare un 'contatto erede' il quale possa, successivamente alla sua scomparsa, succedergli nella gestione del profilo digitale.

Twitter chiede di essere contattato direttamente in caso di decesso, rimandando alle norme generali in materia di successione. Inoltre, Twitter ha fatto la scelta di permettere la cancellazione delle informazioni di un utente dopo sei mesi d'inattività del profilo associato. Utilizzando il modulo di contatto per l'informativa sulla privacy è possibile, non senza complicazioni, avviare la cancellazione dell'account, procedura che può durare fino a sei mesi. Su Twitter è anche consuetudine annunciare la morte della persona con un ultimo *tweet*; tuttavia questo richiede i dati di accesso, che Twitter non rilascia facilmente; infatti anche le policy di Twitter precisano che le credenziali di accesso non vengono fornite a nessuno:⁴²

Non siamo in grado di fornire le credenziali di accesso dell'account a nessuno, indipendentemente dal rapporto tra il defunto e la persona che fa la richiesta.

Instagram si comporta in maniera simile a Facebook, facendo d'altronde parte dello stesso gruppo. L'assistenza fornisce moduli di contatto per modificare un profilo Instagram in stato 'commemorativo' o per cancellarlo completamente. Instagram richiede di dimostrare che il proprietario dell'account sia effettivamente deceduto e non ri-

⁴² Cfr. <<https://help.twitter.com/it/managing-your-account/contact-twitter-about-a-deceased-family-members-account>>.

lascia in nessun caso i dati di accesso. Un profilo Instagram che viene trasformato 'in memoria di' non sarà più accessibile. Visivamente gli account commemorativi non differiscono da quelli convenzionali, ma non sono più 'pubblici', ovvero non appaiono nelle ricerche. Tutte le foto e i commenti rimangono però a disposizione della comunità e continuano a essere interattivi.⁴³

Nel caso di Google, invece, ciascun utente può decidere preventivamente dopo quanto tempo di inattività dell'account si deve presumere la morte dell'utente, da 3 a 18 mesi. Un mese prima dello scadere del tempo prefissato, Google prova a contattare più volte, tramite e-mail e SMS, il proprietario dell'account, e se non riceve alcuna risposta, l'account diventa 'inattivo'. Ciò può comportare la cancellazione dell'account e di tutti i servizi ad esso associati (ad esempio, le e-mail su Gmail, i contenuti caricati su Drive, i video su YouTube, i blog su Blogger, gli appuntamenti su Calendar, le fotografie su Google Foto, la cronologia delle posizioni in Maps, i libri in Google Play Libri, etc.) o l'invio di una notifica ad un contatto di fiducia al quale sarà consentito di scaricare quella porzione dell'archivio personale che si è scelto di condividere con lui.⁴⁴ Quest'ultimo avrà tre mesi di tempo per farlo prima che l'account venga eliminato. Per quanto riguarda l'accesso, neanche Google fornisce password o altri dettagli di accesso:⁴⁵

Ci rendiamo conto del fatto che molte persone non lasciano istruzioni chiare per la gestione dei loro account on-line prima di passare a miglior vita. Possiamo collaborare con parenti stretti e rappresentanti per chiudere in alcuni casi gli account on-line di utenti deceduti. In alcune circostanze, possiamo fornire i contenuti dell'account di un utente deceduto. In ogni caso, la nostra responsabilità principale è tenere al sicuro e private le infor-

⁴³ Cfr. la *Guida all'eredità digitale* disponibile sul sito del provider di servizi *hosting* e *cloud* Ionos, <<https://www.ionos.it/digitalguide/siti-web/diritto-informativo/eredita-digitale>>.

⁴⁴ È possibile utilizzare la pagina di "Gestione account inattivo" per specificare quali diritti di accesso dei vari servizi di Google garantire agli eredi.

⁴⁵ Cfr. <<https://support.google.com/accounts/troubleshooter/6357590>>.

mazioni dei nostri utenti. Non possiamo fornire password o altri dettagli di accesso. Qualsiasi decisione di soddisfare una richiesta relativa a un utente deceduto verrà presa soltanto in seguito a un attento esame.

Ove sia necessario accedere all'account del *de cuius*, in conformità ai relativi termini di servizio, sarà necessario “fornire un’ingiunzione del tribunale emessa negli Stati Uniti”.

Nel caso di Apple, dopo un determinato periodo di inattività dell'account iCloud, viene avviata normalmente la distruzione dei dati ivi contenuti.

Stante le difficoltà, sia tecniche che giuridiche, che si incontrano nella trasmissione dell'eredità digitale, risulta indiscutibile come la prima forma di acquisizione dei beni digitali custoditi all'interno degli account del *de cuius* debba essere l'accesso attraverso lo stesso (o gli stessi) dispositivi tecnologici da lui utilizzati mentre era in vita. In altre parole, gli eredi possono tentare di accedere agli account del defunto utilizzando il suo personal computer, il suo tablet o il suo smartphone, sfruttando il fatto che gli elaboratori elettronici in generale e i programmi di navigazione (browser) in particolare memorizzano le credenziali di accesso ai diversi servizi in rete anche al fine di agevolare l'utente nell'accesso ai propri account.

La questione della posta elettronica merita un approfondimento. Secondo la legge italiana, gli eredi hanno il diritto di ricevere la corrispondenza del defunto, e questa regola vale anche per le email. Con i provider italiani, dunque, non ci dovrebbero essere – almeno in teoria – problemi di sorta. Ad esempio, il noto provider italiano Libero.it consente agli eredi di ottenere le credenziali di accesso alla casella di posta elettronica del defunto con una procedura tutto sommato molto semplice:⁴⁶

Per ottenere l'accesso all'account (casella di posta) di una persona deceduta,

⁴⁶ Cfr. <<https://aiuto.libero.it/articolo/sicurezza/richiesta-della-password-per-accedere-alla-casella-di-posta-di-una-persona-deceduta>>.

in base alle normative vigenti l'erede o gli eredi dovranno fornire:

- certificato di morte del titolare della casella
- documento di identità del deceduto
- documento di identità dell'erede
- dichiarazione sostitutiva di atto di notorietà che certifichi il nome dell'account oggetto della richiesta e il ruolo di erede del richiedente.

Le difficoltà sorgono con i provider stranieri, che sono i più numerosi, perché, come si è visto, la legislazione italiana non è più applicabile. A complicare il quadro giuridico contribuisce il fatto che mancano regole internazionali comuni, per cui per gli eredi può essere anche molto difficile accedere alla posta elettronica del defunto se non si conoscono le credenziali di accesso.

Ad ogni modo non si dimentichi mai il problema costituito dallo scorrere del tempo. Come già detto, dopo un lasso di tempo più o meno lungo – che può andare da qualche mese fino al più ad un paio di anni – l'intero contenuto della casella di posta elettronica viene cancellato 'per inattività' dell'account; quindi ogni richiesta che venga rivolta al provider del servizio di posta elettronica (anche italiano) una volta trascorso quel lasso di tempo non porterà ad alcun risultato.

Eredità digitale e biblioteche personali

Un caso particolare è quello rappresentato dalla trasmissione dei libri digitali (eBook). Coloro che 'acquistano' libri digitali sono spesso assillati da domande del tipo: potrò leggere gli eBook su un dispositivo diverso rispetto a quello su cui li ho 'scaricati' la prima volta? Che succederà se il dispositivo dovesse rompersi? Posso 'rivendere' l'eBook? Potrò trasferire i libri digitali agli eredi? Che fine farà la mia biblioteca digitale personale? Sono dubbi del tutto legittimi e rivelano come le modalità di fruizione dei libri digitali non siano ancora ben conosciute, forse anche per la loro complessità.

Per rispondere a queste domande occorre, innanzitutto, chiarire

che i libri digitali rientrano nella categoria dei cosiddetti *beni digitali concessi in licenza*. A questa categoria appartengono i beni digitali che non sono «assistiti da un diritto esclusivo ed assoluto di proprietà in capo al titolare»⁴⁷, come i brani musicali, i film, gli eBook, i periodici, le fotografie, le banche dati, i font tipografici, i programmi per elaboratore, i beni digitali compravenduti attraverso siti web o piattaforme dedicate, etc. Infatti, molto spesso «il negozio giuridico sotteso alla trasmissione *on-line* di beni digitali non è un contratto di vendita che comporta il trasferimento in capo all'acquirente di un diritto assoluto ed esclusivo di proprietà della copia 'acquistata', bensì un contratto di licenza, in forza del quale l'utente può utilizzare il bene oggetto dell'accordo a determinate condizioni e per un periodo di tempo determinato, mai comunque superiore alla sua vita».⁴⁸ Ad esempio, le condizioni d'uso degli eBook in formato Kindle acquistati su Amazon specificano chiaramente che i contenuti vengono resi disponibili non in virtù di un contratto di vendita ma in virtù di un contratto di licenza:⁴⁹

Con il download o l'accesso del Contenuto Kindle e con il pagamento dei relativi corrispettivi (comprese le tasse applicabili), il Fornitore di Contenuti ti concede il diritto non esclusivo di vedere, usare e visualizzare tale Contenuto Kindle per un illimitato numero di volte [...], esclusivamente sul dispositivo Kindle o sull'Applicazione Kindle, oppure con le diverse modalità previste per il tipo di Servizio, unicamente sul numero di dispositivi Kindle o di Dispositivi Supportati specificati nel Kindle Store ed esclusivamente per tuo uso personale e non commerciale. Il Contenuto Kindle ti viene concesso in licenza d'uso e non è venduto dal Fornitore di Contenuti.

In sostanza, quando affermiamo semplicisticamente di aver 'comprato' un libro digitale (e ne effettuiamo il *download* sul nostro computer) in realtà abbiamo acquistato una licenza d'uso, con un con-

⁴⁷ Cfr. D'Arminio Monforte 2020a, p. 74.

⁴⁸ *Ivi*, pp. 74-75.

⁴⁹ Cfr. le *Condizioni d'uso del Kindle Store* di Amazon disponibili all'indirizzo <<https://www.amazon.it/gp/help/customer/display.html?nodeId=201014950>>.

tratto che può essere anche estremamente complesso. Solitamente la licenza d'uso specifica che «il diritto di accedere alla piattaforma non è trasmissibile agli eredi, ma non è illecita la lettura dei libri già scaricati su memorie locali. In sostanza, ciò che viene ereditato è il dispositivo (computer, smartphone o eBook reader) e, con esso, i libri ivi contenuti».⁵⁰ Se, però, il dispositivo si rompe, non è possibile rivendicare alcun diritto su quanto era in esso memorizzato. A ben vedere, la situazione non sembra molto diversa da quella di un libro tradizionale: una volta rovinato (ad esempio, perché finito in un lavandino pieno d'acqua) non si può più leggere e, certamente, non rientra tra i diritti dell'acquirente quello di farselo sostituire dal negoziante che gliel'ha venduto.⁵¹

Questa precisazione non è di poco conto dal momento che i beni digitali concessi in licenza non possono (normalmente) essere oggetto di trasferimento né *inter vivos* né *mortis causa* e, dunque, non entrano a far parte dell'eredità digitale «a meno di non riuscire a dimostrare che in realtà l'alienazione era idonea ad integrare una vera e propria compravendita e, in quanto tale, attributiva di un diritto di proprietà sulla copia, come tale trasmissibile *mortis causa*»⁵².

Sotto il profilo tecnico, questo genere di beni è spesso protetto mediante sistemi di gestione dei diritti digitali (*Digital Rights Management*, DRM)⁵³, che, grazie all'utilizzo di meccanismi di cifratura, vincolano la fruizione del bene all'identità dell'utente, impedendo la diffusione di copie non autorizzate o l'utilizzo improprio e consentendo così di proteggere il diritto d'autore. Essi limitano il numero di copie e/o trasferimenti degli eBook e definiscono per ogni eBook le

⁵⁰ Cfr. Arcella 2017.

⁵¹ *Ibidem*.

⁵² Cfr. D'Arminio Monforte 2020, p. 75

⁵³ La locuzione *Digital Rights Management* (DRM), il cui significato letterale è "gestione dei diritti digitali", indica i sistemi tecnologici mediante i quali i titolari di diritto d'autore (e dei diritti connessi) possono tutelare, esercitare ed amministrare tali diritti nell'ambiente digitale.

possibili azioni effettuabili dall'acquirente. Normalmente tali sistemi consentono sempre almeno il trasferimento dal PC a un lettore eBook portatile e viceversa e, salvo eccezioni, non è consentita la stampa.

La scelta dell'utilizzo o meno del DRM, così come la tipologia di DRM da applicare ai beni è a discrezione dei singoli fornitori di contenuti. Sebbene i DRM possano essere utilizzati per proteggere il diritti d'autore per beni digitali di qualsiasi categoria (brani musicali in formato MP3, film in formato MP4, eBook in formato ePub o PDF, etc.), sono conosciuti soprattutto per il loro impiego nei libri digitali. In quest'ultimo caso, sono due i formati elettronici più utilizzati: l'ePub (estensione: .epub) e il PDF (estensione: .pdf).⁵⁴ Il primo rappresenta lo standard mondiale per gli eBook. Si tratta del formato che consente la massima personalizzazione dell'esperienza di lettura perché permette la paginazione dinamica (il testo presente nelle pagine si adatta al dispositivo con il quale si sta leggendo l'eBook) e la possibilità di modifica del carattere, della sua dimensione, dei margini e dell'interlinea. È compatibile con la maggior parte degli eReader e dei programmi di lettura digitale presenti sul mercato. Il formato PDF, invece, è caratterizzato dalla paginazione fissa e pertanto è utilizzato soprattutto quando nell'eBook è presente non solo contenuto testuale ma anche immagini e tabelle (che sarebbero difficilmente ridimensionabili a seconda del dispositivo con il quale si legge l'eBook) e con alcuni eReader questa funzione potrebbe dare dei problemi. Esiste anche un terzo formato, il Mobi (estensione: .mobi), il formato proprietario utilizzato da Amazon per distribuire sulle sue piattaforme i libri digitali; solo gli eReader Kindle e le relative applicazioni mobili sono in grado di leggere questo formato. Per leggere gli eBook è necessario un eReader o un programma di lettura digitale compatibile con l'estensione del file.

⁵⁴ I sistemi di DRM più utilizzati per i formati ePub e PDF sono il DRM di Adobe e il Social DRM. Il DRM di Adobe è compatibile con la maggior parte dei lettori di eBook, ma non con il Kindle di Amazon; il Social DRM invece è molto più flessibile: consente all'utente le operazioni di trasferimento, copia e stampa e anche di convertire l'epub nel formato .mobi, compatibile con il Kindle.

La presenza dei DRM implica sempre delle limitazioni alle modalità di fruizione del libro digitale. Vi sono eBook protetti da DRM che possono essere utilizzati solo sul computer/dispositivo sul quale sono stati 'aperti' per la prima volta: è questo il caso degli eBook protetti dal DRM di FileOpen. Infatti:⁵⁵

Un documento protetto da DRM può essere utilizzato solo sul computer/dispositivo sul quale è stato aperto per la prima volta. Il DRM impedisce di aprire il medesimo documento su un altro computer, come ad esempio un server di rete. Prima di aprire un documento assicurarsi di averlo salvato sul computer sul quale dovrà essere utilizzato.

In altri casi le condizioni di utilizzo sono meno restrittive. Ad esempio, il DRM Adobe, uno dei più utilizzati, consente la lettura degli eBook acquistati su un massimo di sei dispositivi autorizzati dallo stesso ID Adobe. Inoltre, gli eBook protetti da DRM Adobe non consentono la stampa, la copia o la modifica del contenuto. Esistono anche sistemi di DRM meno invasivi, come il 'Social' DRM (detto anche 'Light' o 'Soft' DRM): si tratta di un sistema di protezione degli eBook realizzato mediante l'apposizione di una marcatura (*watermark*) che incorpora all'interno dell'eBook (in maniera visibile o invisibile all'utente) alcune informazioni su chi lo ha acquistato (nome, indirizzo, e-mail), in maniera da identificarlo in caso di diffusione illegale del bene. L'eBook con questo tipo di protezione può essere letto su tutti gli eReader, tablet, smartphone e computer e non esiste alcun limite al suo trasferimento; può anche essere copiato, stampato e convertito in altri formati per eBook.⁵⁶

⁵⁵ Cfr. <<http://store.uni.com/catalogo/fileopen>>. Il DRM FileOpen è utilizzato dall'UNI (Organismo Italiano di Unificazione) per la vendita sul proprio sito di e-commerce delle norme UNI in formato digitale. I libri protetti da questo genere di DRM possono essere letti utilizzando Adobe Reader dopo aver installato l'apposito plugin FileOpen.

⁵⁶ Quando si acquista un eBook protetto da Social DRM, una volta scaricato esso si presenta solitamente nel formato .epub o .pdf (in base a quale formato si è

In generale, il problema del trasferimento degli eBook agli eredi non sembra essere preso in considerazione e le condizioni d'uso delle varie piattaforme non dicono nulla in merito a cosa succeda ai libri digitali nel caso di decesso dell'utente. Ad esempio, sul Kindle Store di Amazon le condizioni d'utilizzo dei libri in formato Kindle specificano quanto segue:⁵⁷

Salvo diversa specifica indicazione, non potrai vendere, dare in noleggio o affitto, distribuire, trasmettere, concedere in sublicenza o altrimenti trasferire qualsiasi diritto relativo al Contenuto Kindle o qualsiasi parte dello stesso a terzi, e non potrai togliere o modificare alcuna informazione o etichetta circa la proprietà riportata sul Contenuto Kindle. Inoltre, non potrai bypassare, modificare, annullare o eludere i dispositivi di sicurezza che proteggono il Contenuto Kindle.

In questo caso, le limitazioni sembrano proibire la rivendita dei contenuti, non tanto il loro passaggio agli eredi. In teoria, anche quello ereditario è un trasferimento, ma il contesto sembra affermare il divieto dei trasferimenti volontari, non di quelli che avvengono a causa del decesso del titolare dell'account.⁵⁸

In conclusione, la presenza di DRM costituisce certamente un grande ostacolo alla trasmissione dell'eredità digitale. Infatti, i libri digitali sono associati all'identità del soggetto produttore, il quale solo conosce le credenziali per avere accesso ai libri 'scaricati' sul suo com-

scelto di acquistare). È leggibile sin da subito con qualsiasi programma di lettura digitale, come Calibre, Adobe Digital Editions o l'estensione Readium per Google Chrome. Quando, invece, si acquista un eBook protetto da Adobe DRM e lo si scarica sul proprio personal computer, il formato del file non è né .epub, né .pdf, bensì .acsm (acronimo di Adobe Content Server Manager). Per poterlo leggere è necessario associare questa licenza a un account Adobe (ID Adobe), la società che gestisce il sistema di protezione dei contenuti digitali. Per farlo è necessario aprire il file .acsm con il programma Adobe Digital Editions e autorizzarlo con un ID Adobe.

⁵⁷ Cfr. le *Condizioni d'uso del Kindle Store* di Amazon, cit.

⁵⁸ Cfr. Argella 2017.

puter o depositati sui suoi spazi virtuali. Alla sua morte, l'apertura degli eBook protetti da DRM risulta difficile e potrebbe risultare addirittura impossibile. Viene da domandarsi: le biblioteche personali riusciranno a superare la prova dei DRM?

Una considerazione particolare va fatta relativamente agli spazi di archiviazione delle biblioteche digitali personali. Oggi la modalità di fruizione dei libri (e non solo quelli) si sta sempre più spostando dal dispositivo locale (computer, tablet, smartphone) al *cloud*: questa tendenza vale anche per i libri 'acquistati' che non è più necessario scaricare sui dispositivi in uso ma è possibile lasciare su una delle piattaforme che offrono questo servizio e dove rimarranno disponibili fino a quando sarà attivo il contratto. Una delle più conosciute è la piattaforma dell'azienda tedesca "Tolino media GmbH" che consente di salvare permanentemente nello spazio d'archiviazione *tolino cloud* tutti gli eBook acquistati presso il proprio rivenditore. In questo modo è possibile accedere ai propri libri digitali anche quando si è fuori casa.⁵⁹

Il *tolino cloud* ti garantisce la massima libertà, flessibilità e sicurezza nella lettura e nel salvataggio degli eBook. Lo spazio di archiviazione online è sempre disponibile e ti garantisce l'accesso alla tua biblioteca digitale anche quando sei fuori casa o in viaggio. Non importa quindi se vuoi leggere i tuoi eBook su un eReader toline, su un tablet, tramite la App di lettura toline, oppure direttamente tramite il browser web, utilizzando il Webreader toline. Grazie al *tolino cloud* potrai passare semplicemente da un dispositivo di lettura all'altro, senza dover mai rinunciare al tuo romanzo preferito. L'ecosistema toline ti garantisce sempre una lettura confortevole, sia che utilizzi un eReader, un tablet, uno smartphone o un computer.

Quindi, anche nel mondo dei libri (e degli audiolibri) si comincia a prefigurare quella transizione verso il *cloud* che già è diventata la norma in altri domini, come, ad esempio, quello della musica (ormai la musica è diventata 'liquida' e non occorre scaricare in locale alcunché, perché i brani musicali acquistati sono disponibili sul *cloud*) e dei film (anche

⁵⁹ Cfr. <<https://mytolino.it/vantaggi/tolino-cloud>>.

in questo caso i film 'acquistati' non vengono più scaricati in locale ma rimangono sul server del fornitore del servizio, come – PrimeVideo, Netflix, etc – dove rimarranno disponibili per tutto il periodo stabilito dall'accordo di licenza). Le conseguenze per la trasmissione agli eredi delle biblioteche personali sono facilmente immaginabili.

Il testamento digitale

Come si è visto, entrare in possesso dei fondi personali digitali potrebbe diventare un'impresa di non poco conto. Per evitare problemi agli eredi, la soluzione migliore sarebbe quella di lasciare a disposizione un vero e proprio 'testamento', contenente l'elenco analitico di tutti i beni componenti il patrimonio digitale e, per tutti quei beni (e sono la maggioranza) che non sono accessibili senza la conoscenza delle credenziali di accesso, anche le relative credenziali. Un siffatto documento servirebbe anche ad individuare i vari spazi virtuali su cui sono 'dislocati' i fondi personali, consentendo di entrare in possesso dei beni ereditari con più rapidità e risparmiare tempo e denaro. Dello stesso parere è il Consiglio nazionale del Notariato, che con lungimiranza ha iniziato a studiare il fenomeno sin dal 2007 (le prime istruzioni in materia diramate ai notai italiani risalgono al 2007) ed ha redatto nel 2014 una sorta di 'decalogo dell'eredità digitale' che evidenzia l'importanza di affidare le credenziali di accesso ad una persona fidata che provvederà a consegnarle agli eredi dopo la morte del titolare:⁶⁰

Affidate a una persona di fiducia le vostre credenziali d'accesso (username e password per es.) con istruzioni chiare su cosa fare in caso di decesso: distruggere i dati in tutto o in parte, o consegnarli a soggetti indicati da voi. Si chiama mandato *post mortem* ed è ammesso dal nostro diritto. Se cambiate le password, come è buona regola di sicurezza, ricordate di aggiornare le istruzioni.

⁶⁰ Cfr. Bechini 2014.

Se una volta i documenti venivano conservati nelle casseforti e per recuperarli si faceva ricorso a un fabbro, oggi, allo stesso modo, ci si può comportare per i dati conservati sotto password in risorse fisiche, come computer, tablet, smartphone, chiavette USB, dischi esterni. Se nessuno dispone delle password, ci si può rivolgere a servizi specializzati che possono tentare di violare le protezioni e accedere ai dati. L'inconveniente è che questo tipo di servizi è molto costoso. Meglio affidare questi dati a una persona di fiducia.

Questa persona può essere nominata esecutore testamentario, oppure mandatario *post mortem*, con un documento ufficiale redatto da un notaio.

Il testamento dovrebbe contenere innanzitutto l'inventario dei beni digitali che si vuole trasmettere agli eredi, che, nel caso della trasmissione dei fondi digitali personali, potrebbe essere articolato come segue:⁶¹

- *dispositivi tecnologici*: deve comprendere la lista dei dispositivi fisici (telefoni cellulari, tablet, computer, fotocamere e videocamere digitali, eReader, router, etc.) e tutte le informazioni necessarie per accedervi (comprese le username, il PIN, i segni grafici utilizzati per l'accesso agli smartphone, etc.) che sono indispensabili per concedere a terzi il primo accesso al fondo personale della persona;

- *supporti di archiviazione*: deve contenere l'elenco dei supporti utilizzati (chiavette USB, memory card, dischi fissi o dischi SSD esterni, NAS, DAS, etc.) insieme con la loro collocazione e, nel caso siano protetti da meccanismi di controllo dell'accesso, anche le modalità per 'sbloccarli';

- *account per l'accesso agli spazi di archiviazione personali*: si tratta dei servizi che offrono spazi di archiviazione sul *cloud* (Google Drive, Dropbox, Microsoft Onedrive, etc.) sui quali il soggetto produttore potrebbe aver depositato una parte considerevole (se non tutta) della sua produzione; sono compresi in questa sezione anche gli account

⁶¹ L'inventario è stato elaborato a partire da quello proposto da Giovanni Ziccardi (Ziccardi 2017).

per l'accesso alle piattaforme che consentono di creare le proprie biblioteche digitali personali on-line (come *tolino cloud*);

- *account di posta elettronica*: sarebbe opportuno indicare tutti gli account e-mail che si vogliono mantenere pubblici e conosciuti, con le relative credenziali aggiornate nel caso si voglia dare l'accesso agli eredi. Si può anche specificare la volontà di cancellare gli account in caso di morte (a meno che non siano condivisi o, per esempio, di proprietà del datore di lavoro);

- *account per l'accesso ai social network*: deve comprendere l'elenco degli account su social network e simili (Facebook, Twitter, Instagram, LinkedIn, etc.), indicando chiaramente o gli estremi delle credenziali nel caso vi sia l'intenzione di far continuare la gestione da un erede, o la volontà di chiudere l'account o, infine, il desiderio di convertirlo in una pagina commemorativa;

- *account per l'accesso ai siti web, ai blog, chat, etc.*: deve comprendere l'elenco dei siti web personali, dei blog curati, delle chat e di qualsiasi altro servizio web, indicando anche in questo caso in maniera chiara se si vuole che un erede se ne prenda cura o se si preferisce chiederne la chiusura;

- *beni e servizi digitali*: deve contenere l'elenco dei beni e servizi digitali (brani musicali, fotografie, libri, film e video, software, servizi, etc.) che nel corso degli anni si sono accumulati; come si è già avuto modo di evidenziare, da un punto di vista giuridico gran parte di questi beni non sono 'realmente' acquistati ma sono concessi in licenza fino a quando l'utente è vivo o sono collegati inscindibilmente a un account o a un indirizzo di posta elettronica. C'è quindi un rischio concreto di perdere e non poter trasmettere tutte queste informazioni, a meno che non si raggiungano accordi particolari con i provider per risolvere amichevolmente situazioni specifiche. Nel caso, invece, sia possibile trasferire la licenza, è necessario indicare le credenziali di accesso al servizio e illustrare, a chi verrà, questa possibilità.

Lo schema indicato poco sopra è solo d'esempio, e può essere personalizzato a seconda delle proprie esigenze. Come osservato lucida-

mente da Ziccardi, i due elementi che non dovrebbero mai mancare sono «l'indicazione completa dei servizi e delle relative credenziali e dell'azione che si vuole fare al termine della vita (cancellare e chiudere l'account, rendere commemorativo un profilo, continuare a mantenerlo in vita)»⁶².

Oltre ai fondi personali veri e propri, tra i beni digitali conservati dal *de cuius* potrebbero esserci conti correnti on-line, portafogli finanziari, *wallet* Bitcoin, fondi sugli account PayPal o di trading on-line, giacenze sui cassetti tributari, etc.); quindi questo elenco, ancorché non esaustivo, andrebbe completato con le informazioni necessarie per accedere a tali beni di natura patrimoniale (o, almeno, per far sapere agli eredi della loro esistenza).⁶³

In ogni caso, le password devono sempre essere contenute in un documento separato dal testamento, perché questo, per legge, diventa pubblico dopo la morte del testatore. Le password, comunque, devono sempre essere destinate agli eredi, oppure a chi è destinatario di un lascito specifico (legato). Questo è un aspetto che va sempre tenuto presente quando si tratta di beni patrimoniali. Il caso più importante è quello delle credenziali che permettono di gestire un conto corrente on-line (on-line banking). La semplice consegna delle password a una persona non equivale alla nomina di un erede, quindi chi riceve le password senza un'investitura ufficiale non può legittimamente utilizzarle, e se lo fa può essere accusato di truffa.⁶⁴ Non è pleonastico ricordare che, stante la natura mutevole delle informazioni (si pensi alle password che devono essere cambiate con regolarità), il testamento andrà aggiornato con una certa costanza, pena la sua inservibilità.

⁶² Cfr. Ziccardi 2017.

⁶³ Si fa presente che a partire dal 30 settembre 2021 l'accesso ai servizi forniti dalle pubbliche amministrazioni dovrà essere consentito solo attraverso l'identità SPID (Servizio Pubblico di Identità Digitale) o la CIE (Carta d'Identità Elettronica).

⁶⁴ Cfr. la pagina dal titolo "L'eredità digitale" sul sito del notaio Paolo Tonalini, <<https://www.tonalini.it/eredita/ereddig.html>>.

Riflessioni conclusive

Le considerazioni espresse nei paragrafi precedenti mostrano indiscutibilmente come le nuove tecnologie, se da una parte hanno per sempre mutato il rapporto tra l'identità personale e la morte, dall'altra hanno fatto nascere nuovi problemi per quanto riguarda la trasmissione di archivi e biblioteche personali. Di fronte alle criticità delineate, possiamo essere certi che, così come siamo stati in grado di conservare fino ai nostri giorni i fondi di persona del passato, sarà possibile conservare quelli che si stanno formando oggi? La risposta non è delle più confortanti: archivi e biblioteche di persona corrono il rischio, tutt'altro che irrealistico, di andare perduti⁶⁵; anzi, è molto probabile che buona parte dei fondi personali che si sono formati in questi anni siano già andati perduti. Molto significative sono, a questo proposito, le riflessioni del linguista Raffaele Simone che già nell'anno 2000 a proposito della transizione dalla tradizionale lettera cartacea ad altre forme di comunicazione come la posta elettronica e gli SMS scriveva:⁶⁶

La posta elettronica e, più recentemente, gli SMS [...] hanno modificato in profondità il concetto stesso di 'lettera' e il modo di scrivere epistolare. Abbreviazioni più o meno scherzose, simboli, formule fisse hanno preso ormai piede tra le usanze linguistiche. [Tutto ciò] ha reso immateriale un immenso materiale comunicativo, che una volta si sarebbe depositato su carta o su altri supporti stabili. I filologi di domani troveranno ben poche lettere negli archivi di uomini e donne notevoli...

Come sapientemente hanno scritto Weston, Carbé e Baldini, «pre-

⁶⁵ Purtroppo, gli archivi e le biblioteche personali rappresentano una categoria di beni culturali decisamente più a rischio rispetto a quelli appartenenti ad enti ed "organizzazioni" più o meno complesse che, per tutta una serie di motivi (interessi di studio, prescrizioni legislative, rilevanza economica, etc.), ricevono tradizionalmente l'attenzione degli archivisti e dei bibliotecari. Cfr. Vettore 2014.

⁶⁶ Cfr. Simone 2000, p. 124.

servare a lungo termine le memorie collettive e personali degli ultimi decenni è un'impresa resa particolarmente complessa dalla necessità di integrare competenze appartenenti ad ambiti considerevolmente diversi: discipline letterarie, tecniche archivistiche, tecnologia dell'informazione, questioni giuridiche, aspetti amministrativi»⁶⁷. Per riuscire in questa impresa occorre abbattere le barriere e le divisioni che a volte vi sono tra i vari settori scientifici e mettere a fattor comune le varie competenze, perché «in questa fase di importante trasformazione tecnologica, la produzione e la memorizzazione personali in ambiente digitale e/o di insiemi di documenti e libri digitali sono affrontabili ancora più da un punto di vista tecnico e informatico, piuttosto che da quelli bibliografico e archivistico tradizionali».⁶⁸

Inoltre, «nel caso di documenti personali nuovi aspetti vanno considerati, tra cui ad esempio il problema della gestione dei diritti *post mortem* (ovvero della cosiddetta eredità o testamento digitale)».⁶⁹ Se è vero, infatti, che gli eredi «sono quindi investiti, più o meno consapevolmente, dalla responsabilità di tramandare la memoria del defunto alla posterità»,⁷⁰ è altrettanto vero che nel passaggio dal mondo analogico a quello digitale una buona parte della responsabilità finisce con il ricadere sui soggetti produttori. Se questi ultimi non acquisiscono la consapevolezza di quanto sia importante il loro ruolo nella trasmissione dei fondi personali e non si rendono conto dell'importanza di mantenere un inventario, costantemente aggiornato, di tutti i beni digitali che compongono il loro patrimonio digitale, vani saranno i tentativi degli eredi.⁷¹ Dal canto loro gli eredi devono acquisire la percezione di

⁶⁷ Cfr. Weston – Carbé – Baldini 2017.

⁶⁸ Cfr. Sabba 2020.

⁶⁹ Cfr. Guercio 2016.

⁷⁰ Cfr. Cardinale 2019.

⁷¹ Si tenga presente che la scomparsa di una persona può avvenire in qualsiasi momento e, non sempre, questa può aver avuto la lungimiranza o sentito l'esigenza di pianificare la propria successione. La questione successoria, tuttavia, con lo sviluppo delle tecnologie ha assunto (e assumerà in futuro) un interesse che non riguarda più solo le persone anziane, poco avvezze all'utilizzo degli strumenti in-

quanto debba essere tempestivo il loro intervento, dal momento che i beni digitali possono 'scompare' anche nel giro di pochi mesi o qualche anno al massimo, come si è avuto modo di mettere in evidenza in precedenza. Allo stesso modo i fornitori di servizi on-line devono acquisire una maggiore consapevolezza sull'importanza di questi temi: anche se la sensibilità comincia ad aumentare, sono ancora numerosi i provider che non hanno neanche vagamente iniziato a porsi il problema dell'eredità digitale, ad esempio predisponendo meccanismi adeguati per l'accesso degli eredi e/o per la predisposizione di un 'testamento digitale', in armonia con i diritti nazionali ed internazionali.

Per quanto riguarda la situazione italiana, sebbene l'interesse verso questi temi sia cresciuto notevolmente proprio negli ultimi anni, come dimostrano le numerose pubblicazioni che sono state recentemente date alle stampe⁷², le associazioni nazionali degli archivisti e dei bibliotecari non hanno ancora sviluppato una riflessione su questi temi che interessano congiuntamente tanto i primi che i secondi. Ad esempio, le recenti *Linee guida sul trattamento dei fondi personali* dell'Associazione Italiana Biblioteche, che costituiscono una guida di riferimento preziosissima per il trattamento dei materiali analogici, sembrano non aver minimamente sfiorato il problema del trattamento dei fondi per-

formatici, bensì tutti coloro che sfruttano quotidianamente le nuove tecnologie. I casi giurisprudenziali che hanno portato alla nascita della c.d. eredità digitale dimostrano, del resto, che protagonisti del fenomeno successorio digitale sono (state) persone giovani, fruitrici indefesse di smartphone, tablet, social network, account ed Internet. Cfr. D'Arminio Monforte 2020b.

⁷² A titolo esemplificativo: Aurora Vesto, *Successione digitale e circolazione dei beni on-line. Note in tema di eredità digitale*, Napoli, Edizioni Scientifiche Italiane, 2020; Alessandro D'Arminio Monforte, *L'amministrazione dei beni ereditari. Chiamato all'eredità, curatore dell'eredità giacente ed esecutore testamentario*, Pisa, Pacini Giuridica, 2019; Alessandro D'Arminio Monforte, *La successione nel patrimonio digitale*, Pacini Giuridica, 2020; *Identità ed eredità digitali. stato dell'arte e possibili soluzioni al servizio del cittadino*, a cura di Oreste Pollicino, Valerio Lubello, Marco Bassini, Roma, Aracne, 2016.

sonali digitali che si stanno formando in questi anni.⁷³

È necessario, dunque, affrontare con urgenza queste problematiche, mettendo in campo interventi di sensibilizzazione per aumentare il livello di consapevolezza su queste tematiche e, si badi bene, non solo da parte degli specialisti del settore (ad esempio, gli archivisti, i bibliotecari, gli informatici, etc.) ma anche dalle persone comuni, che potrebbero diventare un giorno quei «soggetti significativi per la comunità»⁷⁴ su cui si concentra tradizionalmente l'interesse di archivisti e bibliotecari. Solo cercando di suggerire soluzioni concrete ed operative per assicurare la conservazione dei patrimoni digitali personali di tutte le persone, potremo evitare che di essi non rimanga alcuna traccia.⁷⁵ A questo proposito un aiuto concreto potrebbe venire dal Centro di ricerca *Personal Digital Memories*, costituitosi all'inizio del 2019 presso l'Università degli Studi di Bologna con l'obiettivo di fornire una soluzione – non solo sotto il profilo teorico ma anche dal punto di vista pratico – ai problemi che affliggono le memorie personali digitali e ne rendono difficile la conservazione a lungo termine.⁷⁶ In questo modo si potrà forse evitare che ci si incammini verso quel

⁷³ Cfr. AIB 2019.

⁷⁴ *Ibidem*, p. 2. Si fa riferimento, in particolare, alla definizione di *biblioteche d'autore e di persona* come «raccolte di libri accorpate in maniera funzionale alla propria attività da un soggetto significativo per la comunità culturale».

⁷⁵ Negli ultimi anni sono state sviluppate anche alcune soluzioni on-line per la gestione e la tutela dell'eredità digitale. In Italia meritano una segnalazione: eMemory, che si definisce come «la tua casa digitale con cui costruire, avere cura e far crescere ogni giorno il tuo patrimonio digitale in totale privacy: ricordi, documenti e memoria» (<http://www.ememory.it>) e eLegacy, che si definisce come «la soluzione leader in Italia per scoprire, ordinare e trasmettere ciò che conta della tua vita online» (<http://www.elegacy.app>).

⁷⁶ Partendo da uno studio serio e sistematico delle questioni di particolare complessità teorica e tecnica legate alle attività di formazione, gestione e conservazione dei fondi personali in ambiente digitale, il Centro intende proporre linee guida, indicazioni operative, soluzioni concrete che andranno a beneficio di tutte le persone che, a vario titolo, si trovano a dover governare le proprie memorie digitali personali, sia in ambito lavorativo che personale.

digital dark age – il medioevo digitale che qualcuno ha già cominciato a prefigurare⁷⁷ – e si potrà assicurare un futuro a quella parte del patrimonio personale, sempre più rilevante, che abbiamo racchiuso all'interno della memoria di un telefono, di un tablet, di un personal computer o che abbiamo affidato ad uno degli innumerevoli servizi *cloud* che sono ormai diventati 'estensioni' irrinunciabili nella nostra esistenza digitale.

⁷⁷ Di questo avviso è Vint Cerf, vice capo di Google nonché uno dei padri di Internet, il quale nel 2015 ha stupito tutti quando nell'incontro annuale dell'*American Association for the Advancement of Science* ha dichiarato che «se non si trova una soluzione, il Ventunesimo secolo sarà un enorme buco nero», un vero e proprio *digital dark age*. Il consiglio che Cerf ha dato sembra a prima vista sconcertante: «se avete una foto alla quale tenete davvero, stampatela». Cfr. Belardelli 2005.

Bibliografia

- AIB 2019 = Associazione italiana biblioteche - Commissione nazionale biblioteche speciali, archivi e biblioteche d'autore, *Linee guida sul trattamento dei fondi personali* (versione 15.1 – 31 marzo 2019), <<https://www.aib.it/struttura/commissioni-e-gruppi/gbaut/strumenti-di-lavoro/linee-guida-sul-trattamento-dei-fondi-personali>>.
- Allegrezza 2018 = Stefano Allegrezza, *L'impatto del digitale negli archivi privati: quale futuro per gli archivi di persona?*, «Atlanti», Volume 28(2018), Numero 1, p. 79-90.
- Allegrezza 2020 = Stefano Allegrezza, *Biblioteche e archivi personali in ambiente digitale: le sfide che si profilano all'orizzonte*, in *Il privilegio della parola scritta. Gestione, conservazione e valorizzazione di carte e libri di persona*, a cura di Giovanni Di Domenico e Fiammetta Sabba, Roma, Associazione italiana biblioteche, 2020.
- Arcella 2017 = Gea Arcella, *Che ne sarà dei miei e-Book?*, pubblicato nel blog di Social News il 30 gennaio 2017, <<https://www.socialnews.it/blog/2017/01/30/che-ne-sara-dei-miei-e-book>>.
- Arezzo - Adamo 2021 = Eliana Arezzo - Giovanni Adamo, *Eredità digitale e GDPR*, 12 febbraio 2021, <<https://www.studiolegaleadamo.it/eredita-digitale-e-gdpr-come-recuperare-i-dati-del-defunto>>.
- Bechini 2014 = Ugo Bechini, *Eredità digitale: le 10 cose da sapere*, disponibile all'indirizzo <<https://www.notariato.it/it/news/eredita-digital-e-le-10-cose-da-sapere>>, 2014.
- Belardelli 2005 = Giulia Belardelli, *Google, Vint Cerf lancia l'allarme: "Dietro di noi un deserto digitale, un altro Medioevo. Se tenete a una foto, stampatele"*, «L'Huffington Post», 13 febbraio 2005 <www.huffingtonpost.it/2015/02/13/vint-cerf-google-deserto-digitale_n_6677452.html>.
- Cardinale 2019 = Eleonora Cardinale, *Il ruolo degli eredi nella trasmissione dell'archivio*, «JLIS, Italian Journal of Library and Information Science», Vol. 10, No. 3 (2019), <<https://www.jlis.it/article/view/12567>>, DOI:

- <http://dx.doi.org/10.4403/jlis.it-12567>>
- Carrarra 2016 = Renato Carrarra, *Eredità digitale: cosa succede in caso di morte di una persona?*, <<https://www.notaiocarrarra.it/eredita-digitale>>.
- Cau 2019 = Eugenio Cau, *Gli ebook sono comodi ed economici, ma non eterni*, «Il Foglio quotidiano», 7 luglio 2019, <<https://www.ilmfoglio.it/tecnologia/2019/07/07/news/gli-ebook-sono-comodi-ed-economici-ma-non-eterni-263780>>.
- D'Arminio Monforte 2017 = D'Arminio Monforte, *L'eredità digitale*, Altalex editore, 2017, <<https://www.altalex.com/documents/news/2017/11/06/eredita-digitale>>.
- D'Arminio Monforte 2018 = Alessandro D'Arminio Monforte, *L'amministrazione dei beni ereditari. Chiamato all'eredità, curatore dell'eredità giacente ed esecutore testamentario*, Pisa, Pacini Editore, 2018.
- D'Arminio Monforte 2020a = Alessandro D'Arminio Monforte, *La successione nel patrimonio digitale*, Pisa, Pacini Editore, 2020.
- D'Arminio Monforte 2020b = Alessandro D'Arminio Monforte, *Accedere ai dati del defunto quando non si conosce la password*, «NetworkLex», 25 mar 2020, <<https://www.networklex.it/post/accedere-ai-dati-del-defunto-quando-non-si-conosce-la-password>>.
- eLegacy 2020 = *L'eredità digitale: un nuovo diritto da tutelare*, 2020, opuscolo realizzato da eLegacy.it <https://escamotages.com/wp-content/uploads/2020/06/Libretto_eLegacy.pdf>.
- Guercio 2016 = Mariella Guercio, *Archivi personali: la sfida del digitale. Una riflessione*, in *Gli archivi di persona nell'era digitale. Il caso dell'archivio di Massimo Vannucci*, a cura di Stefano Allegrezza e Luca Gorgolini, Bologna, Il Mulino, 2016, pp. 133-148.
- Jarre - Bottino = Pietro Jarre - Federico Bottino, *Sloweb: piccola guida all'uso consapevole del web*, Torino, Edizioni Golem, 2018.
- Maniaci - D'Arminio Monforte 2020 = Arturo Maniaci, Alessandro D'Arminio Monforte, *Eredità digitale: cos'è e come si può trasmettere*, «Altalex», Quotidiano on-line di informazione giuridica, pubblicato il 18/06/2020, <<https://www.altalex.com/guide/eredita-digitale-cos-a-e-come-si-puo-trasmettere>>.

Sabba 2020 = Fiammetta Sabba, *Riflessioni sui fondi d'autore e di persona tra tradizione e modernità, eredità e cultura, a margine del convegno "Il privilegio della parola scritta"*, in *Il privilegio della parola scritta. Gestione, conservazione e valorizzazione di carte e libri di persona*, a cura di Giovanni Di Domenico e Fiammetta Sabba, Roma, Associazione italiana biblioteche, 2020.

Simone 2000 = Raffele Simone, *La Terza Fase. Forme di sapere che stiamo perdendo*, Roma, Laterza, 2000.

Vettore 2014 = Simone Vettore, *Gestione degli archivi digitali di persona: strategie e problematiche*, «Il mondo degli Archivi», Sezione Studi, 4 febbraio 2014, <mda2012-16.ilmondodegliarchivi.org/index.php/primo-piano/item/283-gestione-degli-archivi-digitali-di-persona-strategie-e-problematiche>.

Weston - Carbé - Baldini 2017 = Paul Gabriele Weston - Emanuela Carbé - Primo Baldini, *Se i bit non bastano: pratiche di conservazione del contesto di origine per gli archivi letterari nativi digitali*, «Bibliothecae.it», 6 (2017), 1, 155-177.

Ziccardi 2017 = Giovanni Ziccardi, *Il libro digitale dei morti. Memoria, lutto, eternità e oblio nell'era dei social network*, Torino, UTET, 2017.

Tutti gli indirizzi internet sono stati controllati in data 26 marzo 2021.

Abstract

La rivoluzione digitale che da almeno un paio di decenni sta trasformando radicalmente ogni settore della società non ha tralasciato di operare dei profondi mutamenti anche nella vita personale di ciascuno – che sta diventando sempre più ‘digitale’ – e nella produzione e fruizione dei documenti. Tramite il personal computer, il tablet e lo smartphone si redigono documenti, si prendono appunti e note personali, si scrivono testi letterari, si elaborano studi e progetti, si scattano fotografie, si leggono libri, si interagisce sui social network, etc. In questo modo una grande quantità di materiali documentari si forma direttamente in formato digitale e sempre più spesso le riviste ed i libri vengono acquistati e letti in formato digitale. La conseguenza di tutto ciò è che la componente digitale negli archivi di persona sta aumentando sempre di più (e questi si stanno trasformando in “archivi digitali di persona”) e le biblioteche personali si stanno ‘popolando’ di libri digitali e quindi anch’esse stanno diventando digitali. In molti casi, poi, il materiale digitale viene archiviato sugli spazi virtuali messi a disposizione dai fornitori di servizi *cloud* e diventano accessibili solo a chi conosce (o possiede) le necessarie credenziali. Ma di fronte a questa trasformazione in molti cominciano a domandarsi: cosa accadrà a questi fondi personali digitali dopo la morte dei soggetti produttori o dei proprietari? Gli eredi saranno in grado di accogliere questa eredità? Per rispondere a queste domande occorre affrontare il problema della trasmissione dell’eredità digitale, comprendendo fino in fondo quali siano le implicazioni che derivano dall’aver affidato i fondi personali a sistemi spesso protetti da impenetrabili meccanismi di accesso e cercando di individuare le soluzioni che potrebbero consentire di assicurare loro un futuro, evitando di andare incontro a quel *digital dark age* che più di qualcuno ha già cominciato a prefigurare.

fondi personali; archivi di persona; biblioteche d’autore; biblioteche personali; eredità digitale

The digital revolution that for at least a couple of decades has radically transformed every sector of society has not neglected to make profound changes also in the personal life of each one – which is becoming more and more ‘digital’ – and in the production and use of documents. Through personal computers, tablets and smartphones, we draw up documents, take notes and personal notes, write literary texts, develop studies and projects, take photographs, read books, interact on social networks, etc. In this way, many documents are created in digital format and many magazines and books are purchased and read in digital format as well. As a consequence, the digital part in personal archives is increasing more and more (and these are turning into “digital personal archives”); in the same way, personal libraries increasingly consist of digital books and magazines and therefore they are becoming ‘personal digital libraries’ too. In many cases digital material is stored on virtual spaces made available by cloud service providers and become accessible only to those who know (or have) the necessary credentials. But faced with this transformation, many people begin to ask themselves: what will happen to these personal digital fonds after the death of the producers or owners? Will the heirs be able to accommodate this legacy? To answer these questions, we need to face the problem of the transmission of the digital legacy, fully understanding the implications that derive from having entrusted personal fonds to systems often protected by inscrutable access mechanisms and trying to identify the solutions that could allow them to secure their future, avoiding falling into that ‘digital dark age’ that more than someone has already begun to foreshadow.

personal fonds; personal records; personal archives; personal libraries; digital legacy