Norme sulle firme elettroniche a confronto: UE, Italia e Cina

Giusella Finocchiaro, Hu Guiping*

Abstract

Con il presente contributo si intende offrire una prospettiva comparata della normativa sulle firme elettroniche, ponendo a confronto la disciplina dettata dall'UNCITRAL, dal legislatore europeo e da quello italiano rispetto a quanto stabilito dalla normativa cinese. Partendo dalla genesi legislativa, si indagano gli aspetti essenziali dei testi normativi, traendo convergenze e divergenze legislative tra i due contesti: europeo e cinese. Laddove tutti i testi legislativi condividono i principi cardine e i concetti di base, le differenze possono incunearsi nelle pieghe dei dettagli esecutivi. Nell'approfondire in chiave comparata le disposizioni della normativa sulle firme elettroniche, si delinea un panorama differenziato relativo anche all'evoluzione di sistema giudiziale. Infine si pone in evidenza la criticità comune dei testi legislativi in esame: il rischio di venire meno della sovranità del titolare delle firme. Il surrogato tecnologico della firma autografa sembra inevitabile in ossequio del principio cardine della libera circolazione di beni.

This contribution is intended to offer a comparative perspective of the legislation on electronic signatures, comparing the discipline dictated by UNCITRAL, the European and Italian legislators with respect to the provisions of Chinese legislation. Starting from the legislative genesis, the essential aspects of the normative texts are investigated, drawing the convergences and divergences between the two contexts: European and Chinese. Where all legislative texts share the cardinal principles and basic concepts, the differences can be wedged in the folds of the executive details. In examining the provisions of the legislation on electronic signatures from a comparative point of view, a differentiated panorama emerges also relating to the evolution of the judicial system. Finally, the common criticality of the legislative texts in question is highli-

* Le opinioni espresse nel presente contributo sono frutto della collaborazione e della riflessione congiunta degli autori. La Prof.ssa Finocchiaro ha sviluppato l'ideazione e la struttura del contributo curandone il coordinamento ed elaborando i par. da 1 a 4, limitatamente alle parti relative alla disciplina internazionale, europea e italiana, mentre la Dott.ssa Hu Guiping ha curato in particolare le parti concernenti la disciplina cinese nei par. da 1 a 4, nonché il par. 5.
Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

ghted: the risk of losing the sovereignty of the electronic signer. The technological substitute of handwritten signature seems inevitable in compliance with the cardinal principle of the free movement of goods.

Sommario

Keywords

firme elettroniche – UNCITRAL – Unione europea – Italia - Cina

1. Sull'approccio normativo

Con il presente contributo si intende offrire una prospettiva comparata della normativa sulle firme elettroniche, ponendo a confronto la disciplina dettata dall'UNCITRAL (la Commissione delle Nazioni Unite per il diritto commerciale internazionale), dal legislatore europeo e da quello italiano rispetto a quanto stabilito dalla normativa cinese.
Partendo dall'azione dell'UNCITRAL, la Commissione delle Nazioni Unite ha disciplinato il fenomeno delle transazioni elettroniche a livello internazionale adottando il *Model Law On Electronic Commerce* (di seguito, per brevità, "MLEC") nel 1996 e il *Model Law On Electronic Signature* (nel prosieguo, per brevità, "MLES") nel 2001, svolgendo così un ruolo di armonizzazione e di uniformazione del diritto[1].
I principi su cui si basa l'azione dell'UNCITRAL sono quelli dell'autonomia contrattuale delle parti, della non discriminazione, della neutralità tecnologica e dell'equivalenza funzionale[2]. Mentre il principio dell'autonomia contrattuale non richiede ulteriori illustrazioni, occorre soffermarsi brevemente sugli altri principi.
Secondo il principio di non discriminazione, non si può negare validità giuridica ed

[1] L'UNCITRAL (United Nations Commission of international trade law), istituita nel 1966 e composta da una parte dei Paesi che siedono all'Assemblea generale delle Nazioni Unite, svolge da sempre un ruolo essenziale di armonizzazione del diritto commerciale internazionale, predisponendo strumenti di *hard law* e *soft law*. Cfr. G. Herrmann, *Establishing a legal framework for electronic commerce: the work of the United Nations Commission on International Trade Law (UNCITRAL)*, in *World Trade and Arbitration Materials*, 11, 1999, 45 ss. Inoltre, per una completa analisi sul MLEC e al MLES, si rinvia a: E.A. Caprioli- R. Sorieul, *Le commerce international électronique: vers l'émergence de règles juridiques trasnationales,* in *Journal du droit international*, 1991, 323 ss.; R. Sorieul, *The UNCITRAL Model Law and the modernization of legislation to facilitate electronic commerce,* in *Electronic commerce initiatives of ESCAP: business facilitation needs/ Economic and Social Commission for Asia and the Pacific*, 1998, 59 ss.; R. Sorieul, *The UNCITRAL's Model Law on Electronic Signatures,* in G. Chatillon (a cura di), *Internet International Law. International and European studies and comments*, Bruxelles, 2005, 389 ss.

[2] Per approfondimenti cfr. G. Finocchiaro, *Il ruolo dell'UNCITRAL nello sviluppo della disciplina sul commercio elettronico*, in F. Delfini - G. Finocchiaro (a cura di), *Diritto dell'informatica*, Torino, 2014, 64 e H.D. Gabriel, *The United Nations Convention of the use of electronic communications in international contracts: an overview and analysis*, in *Uniform Law Review/Revue de droit uniforme*, 11, 2006, 288.

efficacia probatoria alle informazioni generate, trasmesse e registrate su un supporto non cartaceo unicamente in ragione della loro forma elettronica.

Il principio della neutralità tecnologica invece sancisce che le disposizioni di legge devono essere tecnologicamente neutre rispetto alla tecnologia, senza riconoscere o privilegiare una soluzione tecnologica specifica per implementare i principi giuridici affermati. In altri termini, la norma giuridica non dovrebbe riferirsi a un livello di sicurezza predeterminato o a una tecnologia specifica, bensì dovrebbe limitarsi a dettare lo scopo da raggiungere senza indicare le modalità tecniche per il suo perseguimento.

Il principio di equivalenza funzionale poi si fonda sull'analisi delle funzioni che svolge il documento cartaceo, al fine di determinare in che modo tali funzioni possano essere ugualmente soddisfatte attraverso gli strumenti elettronici. In particolare, il MLEC fissa criteri e requisiti volti a determinare se le funzioni svolte dalla scrittura[3], dalla firma[4] e dall'originale[5] possano essere ugualmente assicurate attraverso determinate tecniche elettroniche, ogniqualvolta la normativa nazionale prescriva l'uso di documenti "cartacei", "firmati" o "originali". Secondo questa logica, la normativa sulle firme elettroniche, anziché disciplinare la firma elettronica, mira a creare un equivalente che soddisfi le funzioni svolte dalla firma. Ne consegue che la firma elettronica sarà destinata a produrre gli stessi effetti giuridici della firma autografa, qualora sia idonea ad assolvere tutte le funzioni svolte da quest'ultima. Il compito del legislatore diventa allora quello di definire i requisiti che la firma elettronica deve rispettare affinché possano dirsi assolte le funzioni a cui questa è preordinata, producendo conseguentemente i corrispondenti effetti giuridici.

L'UNCITRAL, inoltre, ha stabilito alcuni criteri di affidabilità per l'equivalenza tra firme elettroniche e firme autografe, introducendo in particolare un modello a doppio livello (*two-tier approach*)[6]. Secondo quanto disposto dall'art. 6, c. 1, MLES, in via generale ("primo livello") il *data message*[7] e la firma autografa sono considerati funzionalmente equivalenti «se la firma elettronica offre un livello di affidabilità adeguato allo scopo per cui il messaggio di dati è stato generato o trasmesso, alla luce delle circostanze, incluse le pattuizioni contrattuali»[8]. Inoltre, ai sensi dell'art. 7 del MLES, qualsiasi metodo – purché conforme agli standard internazionali riconosciuti e compatibile con le *rules of private international law*[9] – può essere utilizzato per soddisfare il requisito di firma autografa. Al secondo livello, l'affidabilità della firma elettronica è presunta se tale firma soddisfa i requisiti fissati dall'art. 6, c. 3, MLES, tra cui la corrispondenza

---

3 Art. 6, MLEC.

4 Art. 7, MLEC.

5 Art. 8, MLEC.

6 Cfr. U. Draetta, *Internet et le commerce électronique en droit international des affairs,* in *Recueil des cours de l'Académie de Droit International de la Haye*, Dordrecht, 314, 2005, 125; J. Penadés, *Firma electrónica y comercio electrónico. Regulación en España y en la Unión Europea*, in F.J. Orduña – G.A. Aguilera (a cura di), *Comercio, administraciòn y registros electrònicos*, Cizur Menor, 2009, 547 ss., spec. 567 ss.

7 Giova precisare che il MLES non si riferisce al documento informatico, ma al "*data massage*", che definisce quale «*information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy*» (art. 2, c. 1, lett. *c*), MLES).

8 Art. 6, c. 1, MLES.

9 Art. 7, c. 2 e 3, MLES.

esclusiva dei dati per la formazione della firma al firmatario e il controllo esclusivo del firmatario sui dati. La norma contempla altresì metodi di firma elettronica che possono essere riconosciuti *ex ante* da un'autorità statale, da un ente privato accreditato o dalle parti stesse, quali metodi che soddisfano criteri di affidabilità tecnica stabiliti nella legge modello[10].

Il MLEC e il MLES rappresentano dunque i principali strumenti di *soft law*[11] di riferimento per le legislazioni nazionali di oltre sessanta paesi del mondo, fra cui la Cina.

L'approccio legislativo cinese prevede una fedele riproduzione delle prescrizioni dettate dal *Model Law* elaborato dall'UNCITRAL. In vigore dal 1° aprile 2005, la legge sulle firme elettroniche della Repubblica Popolare della Cina si pone l'obiettivo di disciplinare la firma elettronica, determinarne gli effetti giuridici[12], chiarire lo *status* giuridico e le procedure di certificazione del prestatore del servizio di certificazione e, infine, stabilire le misure di sicurezza per l'utilizzo di firme elettroniche. Vengono anche richiamati alcuni principi fondamentali, tra cui quello di autonomia contrattuale[13], di non discriminazione[14], di neutralità tecnologica e di equivalenza funzionale[15]. Con la riforma del 2015, il legislatore cinese ha poi introdotto il meccanismo del doppio livello di verifica dell'affidabilità e della validità della firma, mentre la riforma dell'aprile 2019 ha esteso l'ambito di applicazione della normativa alla sottoscrizione degli atti aventi ad oggetto i beni immobili.

Per quanto riguarda, invece, il panorama italiano, occorre anzitutto chiarire l'approccio che sta a fondamento della disciplina in materia di firme informatiche[16], basato sullo strumento cognitivo della metafora[17]. Sebbene si tratti di entità ontologicamente diverse, il legislatore italiano ha infatti posto in relazione la sottoscrizione autografa e le firme informatiche. Non si tratta tuttavia di un rapporto di identità ma solo di una associazione terminologica sotto il profilo cognitivo. In altre parole, si tratta di una relazione basata sul "come se" e non, invece, sull'"uguale", che consente di stabilire che le firme informatiche sono come la firma autografa[18]. Tale disciplina ha subito, nel

---

[10] Cfr. L.G. Castellani, *I testi dell'UNCITRAL in materia di diritto del commercio elettronico*, in F. Delfini – G. Finocchiaro (a cura di), *Diritto dell'informatica*, cit., 46 ss.

[11] Sulla distinzione tra *soft law* e *hard law* si rinvia a: J.H. Dalhuisen, *Custom and its revival in transnational private law*, in *Duke Journal of Competitive & International Law*, 399, 2008, 355: «*Soft law means rules that do not emerge from an autonomous source of law and are not law in that sense. In the international commercial and financial sphere, soft law often means proposals or sets of principles from Unidroit, Uncitral or other such organizations, or from think-tanks that aspire to reflect the living law particularly at the transnational level. […] To repeat, short of soft law emerging as custom or general principle, it is not law, and therefore not a norm that must be applied, although it may provide guidance (usually supplementary to hard law or as some manifestation thereof)*».

[12] Art. 1 della legge cinese sulle firme elettroniche.

[13] Art. 3 della legge cinese sulle firme elettroniche.

[14] Art. 3, c. 2, legge cinese sulle firme elettroniche.

[15] Artt. 4-8 e 13 della legge cinese sulle firme elettroniche.

[16] Si precisa che la dicitura "firme informatiche" viene impiegata in senso a-tecnico e comprensivo di tutte le firme elettroniche.

[17] Il tema della metafora nel diritto viene illustrato con la consueta ricchezza culturale e profondità di analisi da F. Galgano, *Le insidie del linguaggio giuridico. Saggio sulle metafore nel diritto*, Bologna, 2010, 22-23.

[18] G. Finocchiaro, *La metafora e il diritto nella normativa sulla cosiddetta "firma grafometrica"*, in *Dir. Inf.*, 1, 2013, 3.

corso dell'ultimo ventennio, ripetuti interventi legislativi che hanno progressivamente portato alla definizione dell'attuale quadro costituito dall'adeguamento al regolamento (UE) 910/2014 (nel prosieguo, per brevità, "Reg. e-IDAS") e dal Codice per l'amministrazione digitale di cui al d.lgs. 7 marzo 2005, n. 82, come successivamente modificato e integrato (di seguito, per brevità, "CAD")[19]. La ragione di questa continua opera di affinamento compiuta dal legislatore italiano è, in gran parte, riconducibile alla necessità di coordinarsi con le scelte operate a livello europeo.

In sede europea, l'*iter* legislativo ha visto l'adozione, in un primo momento, della direttiva 1999/93/CE e, in un secondo momento, del Reg. e-IDAS. La *ratio* alla base del primo intervento era quella di superare gli ostacoli che le normative dei diversi Stati membri ponevano alla libera circolazione dei beni e dei servizi nel mercato interno. Il legislatore ha tentato quindi di creare un quadro giuridico europeo armonizzato per la fornitura dei servizi di firma elettronica e di certificazione, al fine di favorire lo sviluppo nel mercato interno del commercio elettronico. Questo proposito continua ad essere perseguito, divenendo ancor più concreto, grazie al Reg. e-IDAS che, proprio in virtù della sua natura di regolamento, detta una disciplina generale direttamente applicabile in tutti gli Stati membri dell'Unione europea. L'obiettivo del Reg. e-IDAS è infatti quello di fornire una base giuridica comune che consenta di «garantire il buon funzionamento del mercato interno perseguendo al contempo un adeguato livello di sicurezza dei mezzi di identificazione elettronica e dei servizi fiduciari»[20]. La previsione di una base giuridica condivisa permette altresì di assicurare l'interoperabilità giuridica e tecnica tra gli Stati membri in relazione agli strumenti di identificazione elettronica, di autenticazione e di firma elettronica. Perseguendo tale finalità, l'art. 6 del Reg. e-IDAS introduce l'obbligo di riconoscimento reciproco transfrontaliero dei mezzi di identificazione *on line* nel settore pubblico. In altri termini, il Reg. e-IDAS prevede a favore degli Stati membri la facoltà di notificare i loro sistemi di identificazione elettronica alla Commissione europea, qualora tali sistemi soddisfino le condizioni relative ai livelli di garanzia previsti dall'art. 7 del Reg. e-IDAS. Una volta accertato il soddisfacimento di tali condizioni, la Commissione pubblica i regimi di identificazione elettronica notificati in un apposito elenco nella Gazzetta Ufficiale dell'UE[21] e, a partire da questo momento ed entro 12 mesi, gli altri Stati membri sono obbligati a riconoscere il sistema di identificazione elettronica notificato. In questo modo, viene consentito a cittadini, imprese, amministrazioni pubbliche o organismi dello Stato membro notificante di accedere ai servizi in rete dei soggetti pubblici di un altro Paese dell'Unione, a condizione che il sistema di identificazione notificato abbia un livello di sicurezza pari o superiore a quello richiesto dal servizio offerto. L'interoperabilità tecnica dei sistemi elettronici all'interno dell'Unione è poi garantita dall'attuazione del già citato principio di neutralità tecnologica che impone requisiti minimi tecnici d'in-

[19] Il CAD è stato, negli anni, oggetto di molteplici interventi legislativi volti a realizzare un apparato normativo organico. In particolare, tra le riforme più recenti, occorre segnalare il d.lgs. 26 agosto 2016, n. 179, che ha provveduto a raccordare la normativa nazionale al Reg. e-IDAS e il d.lgs. 13 dicembre 2017, n. 217 che ha modificato la disciplina probatoria del documento informatico e ha previsto un nuovo processo di firma elettronica avanzata. Cfr. G. Finocchiaro, *Diritto di Internet*, cit., 85.

[20] Art. 1 del Reg. e-IDAS.

[21] Art. 9, par. 2, Reg. e-IDAS.

teroperabilità e di sicurezza per l'identificazione elettronica.
Sempre con riferimento al quadro normativo europeo, appare opportuno sottolineare come il Reg. e-IDAS se, da un lato, mantiene sostanzialmente invariata la normativa previgente relativa alle firme elettroniche, dall'altro, introduce e disciplina anche nuovi strumenti, quali: sigilli elettronici, che garantiscono la provenienza e l'integrità del documento; validazioni temporali elettroniche, che forniscono prova della data e dell'ora del documento opponibile a terzi; servizi elettronici di recapito certificato, che permettono di dare prova dell'invio e dell'avvenuta ricezione dei dati, riducendo rischi di perdita, danneggiamento, furto e modifica non autorizzata di questi; servizi riguardanti i certificati di autenticazione dei siti web, che consentono di dimostrarne l'affidabilità, collegando il sito alla persona fisica o giuridica a cui viene rilasciato il certificato.

2. Prestatore di servizi fiduciari vs certificatore di firme elettroniche

Sempre in prospettiva comparata, giova esaminare la figura del prestatore di servizi fiduciari.
Una compiuta definizione di prestatore di servizi fiduciari non appare né nella direttiva 1999/93/CE né nel *Model Law* dell'UNCITRAL. Entrambi, infatti, si limitano a prevedere la figura del prestatore di servizi di certificazione, descrivendola come l'entità o la persona fisica o giuridica che rilascia certificati o fornisce altri servizi connessi alle firme elettroniche[22]. Una scelta differente viene, invece, compiuta dal legislatore europeo nel Reg. e-IDAS tramite l'introduzione di un'espressa definizione di prestatore di servizi fiduciari che consente, se adeguatamente interpretata, di ricomprendere al suo interno anche la figura del prestatore di servizi di certificazione. Ciò è possibile muovendo dal combinato disposto delle norme del Reg. e-IDAS che definiscono rispettivamente il prestatore di servizi fiduciari e il servizio fiduciario. Il primo è quella «persona fisica o giuridica che presta uno o più servizi fiduciari come prestatore qualificato o non qualificato»[23]. Per servizio fiduciario, si intende invece «un servizio elettronico fornito normalmente dietro remunerazione e consistente nei seguenti elementi: a) creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi; oppure b) creazione, verifica e convalida di certificati di autenticazione di siti web; o c) conservazione di firme, sigilli o certificati elettronici relativi a tali servizi»[24].
Alla luce di tali definizioni, come anticipato, la figura del prestatore di servizi di certi-

[22] All'art. 2, par. 1, n. 11, direttiva 1999/93/CE. In maniera analoga, l'art. 1, c. 1, lett. e), MLES, definisce il "certification service provider" come «person that issues certificates and may provide other services related to electronic signatures».

[23] Art. 3, n. 19, Reg. e-IDAS.

[24] Art. 3, n. 16, Reg. e-IDAS. La normativa europea distingue tra servizi fiduciari qualificati e non qualificati, a seconda che questi soddisfino i requisiti fissati dal Regolamento e che garantiscano un maggiore livello di sicurezza e di affidabilità nelle transazioni elettroniche. Cfr. L. Greco, *Articolo 3. Definizioni*, in F. Delfini -G. Finocchiaro (a cura di), *Diritto dell'informatica,* cit., 48.

ficazione, disciplinata dalla previgente Direttiva e dal *Model Law*, pare rientrare di fatto in quella del prestatore di servizi fiduciari, che, al pari del primo, fornisce servizi come quelli di creazione, verifica e convalida di firme elettroniche, nonché di rilascio del certificato delle firme. Il legislatore europeo non opera dunque alcuna distinzione di ruolo tra prestatore di firme elettroniche e certificatore, salvo quella relativa allo svolgimento di un servizio "qualificato". Tale attributo, una volta riconosciuto dall'organismo di vigilanza in capo al prestatore di servizi fiduciari, consente a quest'ultimo – tra le altre cose – di rilasciare il certificato della firma elettronica qualificata[25].

Superata tale questione definitoria, è possibile esaminare la disciplina prevista dal Reg. e-IDAS per tutti i prestatori di servizi fiduciari, i quali sono soggetti ai medesimi requisiti ed obblighi.

In primo luogo, il Reg. e-IDAS conferma i principi cardine relativi alla protezione dei dati personali stabiliti dal regolamento (UE) 679/2016, imponendo ai prestatori di servizi fiduciari di rispettare gli obblighi e i principi generali in materia di protezione dei dati personali e, in particolare, quelli inerenti alla sicurezza del trattamento dei dati e alla necessità e finalità del trattamento, secondo cui i dati devono essere adeguati, pertinenti e non eccedenti rispetto alle finalità del trattamento.

In secondo luogo, la normativa europea stabilisce per tutti i prestatori di servizi fiduciari requisiti, specificamente in materia di sicurezza e responsabilità, tali da garantire la dovuta diligenza, trasparenza e attendibilità delle loro operazioni e dei loro servizi[26].

Il Reg. e-IDAS istituisce poi per tutti i prestatori di servizi fiduciari un regime di vigilanza in grado di assicurare parità di condizioni per la sicurezza e l'attendibilità dei loro servizi, in un'ottica di tutela degli utenti e del funzionamento del mercato interno.

L'unica differenza si riscontra nella sorveglianza sui prestatori di servizi fiduciari qualificati e sui prestatori privi di qualifica che, per i primi, avviene *ex ante* e per i secondi *ex post*[27]. A ciò si aggiunga che, nel Reg. e-IDAS, i prestatori qualificati sono soggetti a requisiti e obblighi più stringenti, sempre nella prospettiva di garantire un elevato livello di sicurezza di tutti i servizi fiduciari qualificati offerti. Il medesimo intento emerge dal disposto dell'art. 13, par. 2, Reg. e-IDAS, in cui si afferma che i prestatori qualificati possono stabilire limiti all'uso dei servizi forniti, a condizione che i clienti ne siano debitamente e anticipatamente informati e che tali limiti siano conoscibili a terzi. Il rispetto di tale previsione giova altresì al prestatore qualificato, il quale, adeguando il proprio comportamento a quanto prescritto, potrà mitigare la possibilità di essere chiamato a rispondere per responsabilità legate ad un uso dei servizi eccedente il limite fissato[28].

Con riferimento al quadro normativo italiano, emerge come, sotto il profilo dell'accreditamento e della qualificazione del prestatore di servizi fiduciari, il legislatore abbia

[25] Art. 3, n. 15, Reg. e-IDAS. Ulteriori differenze tra prestatori di servizi fiduciari qualificati e non emergono, come vedremo di seguito, in riferimento ai requisiti e agli obblighi previsti dal Reg. e-IDAS per questi soggetti.

[26] Considerando 35 del Reg. e-IDAS.

[27] Considerando 36 e art. 17, par. 3, Reg. e-IDAS.

[28] Considerando 37 del Reg. e-IDAS.

deciso di stabilire regole più restrittive rispetto a quelle del Reg. e-IDAS[29]. In Italia, infatti, il servizio di certificazione di firma elettronica qualificata può essere fornito solo da un soggetto pubblico o privato costituito nella forma di società di capitali[30].
Per quanto riguarda, invece, il quadro normativo cinese, occorre precisare sin da subito che il legislatore cinese, con la legge sulle firme elettroniche, non detta una disciplina specifica relativa ai prestatori di servizi fiduciari, ma si limita a definire i requisiti che il certificatore cinese deve soddisfare[31]. Il richiedente deve essere una persona giuridica costituita in forma societaria, dotata di sufficiente capitale e di personale tecnico e gestionale adeguato. Questi deve inoltre ottenere una doppia autorizzazione preventiva da parte della *State Cryptography Administration*, ai fini dell'utilizzo di chiavi crittografiche, e da parte del Ministero dell'Industria e dell'Informazione, ai fini dell'accreditamento[32]. Sebbene la legge cinese, diversamente dalla direttiva 1999/93/CE e dal *Model Law* dell'UNCITRAL, non fornisca una definizione di certificatore o di servizio di certificazione elettronica, tale lacuna è colmata dall'art. 2 del Decreto del Ministero cinese dell'Industria dell'Informazione del 28 gennaio 2005, n. 35, recante "Misure per l'amministrazione dei servizi di certificazione elettronica", in vigore dal 1° aprile 2005, ove il servizio di certificazione elettronica è definito come «il servizio pubblico di verifica sull'autenticità e affidabilità per le parti interessate delle firme elettroniche» [33]. Il certificatore, invece, è «un'istituzione di terza parte che presta servizi di certificazione elettronica ai firmatari elettronici e alle parti facenti affidamento sulla firma elettronica». Nel 2009, l'art. 2 del citato decreto ministeriale n. 35/2005[34] viene modificato tramite l'introduzione di un "servizio di certificazione elettronica al pubblico in generale"[35]. Questo servizio, così come chiarito dal decreto ministeriale

[29] Art. 29 del CAD.

[30] L'ultima modifica effettuata dal d.lgs. 217/2017 stabilisce, all'art. 29, c. 2, CAD che «il richiedente deve avere natura giuridica di società di capitali e deve disporre dei requisiti di onorabilità, requisiti tecnologici e organizzativi, nonché garanzie assicurative ed eventuali certificazioni adeguate al volume dell'attività svolta e alla responsabilità assunta nei confronti dei propri utenti e dei terzi. Tali requisiti sono individuati, nel rispetto della disciplina europea, con decreto del Presidente del Consiglio dei Ministri, sentita l'AgID. Il decreto in questione determina altresì i criteri per la fissazione delle tariffe dovute all'AgID per lo svolgimento di queste attività, nonché i requisiti e le condizioni per lo svolgimento delle attività di cui al comma 1 da parte di amministrazioni pubbliche».

[31] Art. 17 della legge cinese sulle firme elettroniche.

[32] Art. 18 della legge cinese sulle firme elettroniche.

[33] 2005年 "电子认证服务管理办法", 第二条 本办法所称电子认证服务，是指为电子签名相关各方提供真实性、可靠性验证的公众服务活动。
本办法所称电子认证服务提供者，是指为电子签名人和电子签名依赖方提供电子认证服务的第三方机构（以下称为"电子认证服务机构"）。

[34] 中华人民共和国工业和信息化部令第1号《电子认证服务管理办法自2009年3月31日起施行;
第二条 本办法所称电子认证服务，是指为电子签名相关各方提供真实性、可靠性验证的活动。
本办法所称电子认证服务提供者，是指为需要第三方认证的电子签名提供认证服务的机构（以下称为"电子认证服务机构"）。
向社会公众提供服务的电子认证服务机构应当依法设立。

[35] L'art. 2, c. 1, decreto ministeriale n. 35/2005 recita: «I servizi di certificazione per E-government rivolti agli organi pubblici, sono basati sulla tecnologia crittografica con certificati digitali. I servizi di certificazione elettronica dell'E-government comprendono i servizi di certificazione elettronica di

recante "Misure per l'amministrazione della certificazione elettronica per l'E-government", può essere fornito solamente da un'istituzione di certificazione elettronica (di seguito, per brevità, "CA", ossia *Certificate Authority*) costituita a norma di legge[36]. In particolare, ai sensi dell'art. 15, la CA deve essere «una persona giuridica di un'istituzione pubblica o una persona giuridica di società controllata dallo Stato, che ha ottenuto l'autorizzazione per i servizi di certificazione elettronica». Sono dunque previsti *ex lege* due requisiti. In primo luogo, la società di capitali, avente l'autorizzazione a fornire un servizio di certificazione elettronica, deve essere controllata dallo Stato per poter fornire i servizi all'*E-government* – in altre parole, la norma impone di fatto un regime di monopolio statale del servizio di certificazione riguardo agli affari governativi. In secondo luogo, le società di capitali a controllo statale devono presentare una richiesta di valutazione delle qualifiche alla *State Cryptography Administration* e, in caso di esito positivo, queste potranno essere accreditate ed incluse nell'elenco CA, reso pubblico sul sito di tale Amministrazione.

In definitiva, venendo, ancora una volta, all'analisi comparata delle norme, con riguardo alla definizione di prestatore del servizio di certificazione, occorre notare una differenza tra il Reg. e-IDAS e la legge cinese. Mentre il primo consente tanto ad una persona fisica quanto ad una giuridica di prestare i servizi di firma elettronica, la norma cinese esclude la persona fisica, assegnando tale attività solamente ad una persona giuridica. In aggiunta, se il Reg. e-IDAS fissa obblighi generali, requisiti e responsabilità dei prestatori di servizi fiduciari[37], la legge cinese li prevede solo nei confronti dei prestatori di servizi di certificazione di firma elettronica. Infine, sebbene la normativa cinese stabilisca in modo esplicito i requisiti che il certificatore deve soddisfare, rimane indefinita la questione relativa alla disciplina applicabile ai prestatori di firma elettronica. Di conseguenza, in mancanza di una precisa indicazione da parte del legislatore, i giuristi cinesi[38], sin dall'entrata in vigore della legge in commento, si sono interrogati su chi possa essere accreditato a fornire il servizio di firma elettronica. I principali interrogativi ruotano attorno alla *ratio* sottesa a tale scelta legislativa. Si tratta di una impostazione ereditata dal MLES oppure deriva dall'applicazione del principio di neutralità tecnologica? Al di là del dibattito dottrinale, dall'esame dei siti cinesi emerge come le piattaforme di *e-commerce* prestino servizi quasi onnicomprensivi che vanno dalla certificazione alla firma elettronica, dalla conservazione alla consulenza legale fino all'autenticazione e perizia giudiziaria e così via. A tal proposito giova

E-government per i dipartimenti governativi, per le imprese e le istituzioni, i gruppi sociali e il pubblico in generale».

[36] "电子政务电子认证服务管理办法" L'Annuncio della *State Cryptography Administration* n. 7/2009 sulla pubblicazione delle "Misure per l'amministrazione della certificazione elettronica per E-government", in vigore dal 1° novembre 2009. In questo atto si stabilisce che entro il 1° maggio 2010, il prestatore del servizio di certificazione elettronica, per avviare l'attività per l'*E-government*, deve presentare la richiesta di valutazione di qualifica alla *State Cryptography Administration*.

[37] Art. 19, "Requisiti di sicurezza relativi ai prestatori di servizi fiduciari"; Art. 20, "Vigilanza dei prestatori di servizi fiduciari qualificati"; Art. 21, "Avviamento di un servizio fiduciario qualificato"; Art. 24, "Requisiti per i prestatori di servizi fiduciari qualificati".

[38] Cfr.法制日报 , 作者: 路虹 ,"电子签名法"实施遭遇规章空白 配套机构欠缺, 2005年06月13日11:03

richiamare il caso del certificatore (CA) iTrusChina Co., Ltd.di Pechino[39], il quale offre servizi per autenticare l'identità del soggetto richiedente, servizi di firma elettronica e certificazione, di contratto elettronico e conservazione dei dati con metodi *blockchain*. Anche in virtù di questa situazione di fatto, nel 2019, anno in cui sono state adottate dall'UNCITRAL le *Draft provisions on the cross-border recognition of identity management and trust services*[40] in coordinamento con il Reg. e-IDAS, è entrata in vigore la legge sul commercio elettronico della Repubblica Popolare della Cina che ha permesso di annoverare i prestatori di firme elettroniche tra gli operatori delle piattaforme di *e-commerce*. In questo modo, i primi sono stati assoggettati ai medesimi obblighi generali previsti per i secondi, tra cui la tenuta di un registro dell'impresa[41] e l'ottenimento di una licenza[42] necessari ad avviare l'attività[43], la pubblicazione di specifiche informazioni[44] nonché l'obbligo di ottemperare ad alcuni adempimenti fiscali[45] e il divieto di abusare della propria posizione dominante[46].
Alla luce di questa ricognizione, si può concludere che sia il quadro normativo europeo sia quello cinese sembrano ammettere la prassi di considerare unitariamente i servizi di firma elettronica e quelli relativi alla loro certificazione.

3. Sulla responsabilità del prestatore di servizi fiduciari

Il Reg. e-IDAS disciplina il regime di responsabilità dei prestatori di servizi fiduciari. In particolare, l'art. 13, al par. 1, primo capoverso, prevede una forma di responsabilità extracontrattuale in capo al prestatore nei confronti di qualsiasi soggetto, persona fisica o giuridica, compreso il terzo che non sia legato al prestatore da alcun vincolo contrattuale. Il secondo capoverso pone a carico del danneggiato l'onere della prova del dolo o della negligenza che, tuttavia, subisce un'inversione al terzo capoverso, ove si afferma che il dolo o la negligenza di un prestatore qualificato sono presunti, a meno che questi non dimostri il contrario. La disposizione prosegue, prevedendo al par. 2 un'esenzione di responsabilità del prestatore di servizi fiduciari qualora il cliente utilizzi i servizi oltre i limiti indicati causando così un danno a terzi, a condizione che il prestatore abbia previamente informato, in modo adeguato e tempestivo, i propri clienti dell'esistenza delle

[39] https://www.itrus.com.cn/intro.html. La società ha fornito i suoi servizi di certificazione per quasi 500.000.000 di utenti provenienti da diversi settori, quale governo, banca, sicurezza, assicurazione, magistratura, offerte, finanza Internet, ecc.

[40] A/CN.9/WG.IV/WP.160 – *Draft Provisions on the Cross-border Recognition of Identity Mangement and Trust Services*, 16 September 2019.

[41] Art.10 della legge cinese sul commercio elettronico.

[42] Art.12 della legge cinese sul commercio elettronico.

[43] Si noti, perciò, che non essendoci requisiti a livello di norma ordinaria, le regole relative ai requisiti e alla licenza sono definite unicamente da norme secondarie e attuative.

[44] Artt. 15 e 16 della legge cinese sul commercio elettronico.

[45] Art. 11 della legge cinese sul commercio elettronico.

[46] Art.22 della legge cinese sul commercio elettronico. Si noti che, non essendovi requisiti fissati a livello di norma ordinaria, le regole relative ai requisiti e alla licenza sono dettate da norme secondarie e attuative.

limitazioni d'uso dei servizi da esso forniti e che tali limitazioni siano state rese conoscibili ai terzi[47]. Infine, il par. 3 stabilisce che l'applicazione dei commi precedenti deve avvenire nel rispetto delle norme di ciascuno Stato membro in materia di responsabilità[48]. Di conseguenza, la diretta applicabilità del Reg. e-IDAS non preclude al legislatore nazionale di precisare il regime di responsabilità dei prestatori di servizi fiduciari.

In Italia, diversamente da quanto previsto dal Reg. e-IDAS, la disciplina della responsabilità viene delineata dall'art. 30 del CAD solo con riferimento ai prestatori di servizi fiduciari qualificati che «cagionano danno ad altri nello svolgimento della loro attività» [49], imponendo loro un onere della prova più gravoso rispetto a quello della normativa europea. Si tratta dell'*onus probandi* previsto dall'art. 2050 c.c. per l'esercizio di attività pericolose, in base al quale i prestatori qualificati devono provare di avere adottato tutte le misure idonee ad evitare il danno. Tale disposizione ha suscitato numerosi rilievi critici in dottrina, non solo perché aggrava la posizione del prestatore qualificato rispetto alla norma europea, ma anche perché è riconducibile ad una responsabilità extracontrattuale di natura oggettiva[50].

Volgendo poi lo sguardo alla normativa cinese, come accennato in precedenza, la legge sulle firme elettroniche si occupa delle sole responsabilità del prestatore di servizi di certificazione di firme elettroniche, con particolare riferimento alla pubblicazione del *certificate practice statement* (di seguito, per brevità, "CPS"[51]), alla verifica dell'identità del destinatario del servizio[52], alla garanzia dell'autenticità e dell'integrità delle informazioni sulle firme elettroniche[53], alla tempestiva comunicazione[54] e conservazione di informazioni relative al certificato[55], senza invece prevedere limiti di responsabilità né obblighi sotto il profilo della protezione dei dati personali[56]. Le regole appena richiamate, se violate, comportano l'insorgere di responsabilità di natura civile[57], amministrativa[58] e penale[59].

L'art. 28 della legge cinese sulle firme elettroniche esclude poi la responsabilità del

---

[47] Cfr. F. Delfini, *Art. 13. Responsabilità e onere della prova*, in F. Delfini – G. Finocchiaro (a cura di), *Diritto dell'informatica,* cit., 153.

[48] Art. 13, par. 3, Reg. e-IDAS: «i paragrafi 1 e 2 si applicano conformemente alle norme nazionali in materia di responsabilità».

[49] Art. 30 del CAD.

[50] F. Delfini, *Art. 13*, cit., 156.

[51] Art. 19 della legge cinese sulle firme elettroniche.

[52] Art. 20 della legge cinese sulle firme elettroniche.

[53] Artt. 21 e 22 della legge cinese sulle firme elettroniche.

[54] Art. 23 della legge cinese sulle firme elettroniche.

[55] Art.24 della legge cinese sulle firme elettroniche.

[56] Solo nel 2018, lo *standard CPS for E-government* ha fissato gli obblighi e la responsabilità del certificatore sotto il profilo della riservatezza e della protezione dei dati personali, della proprietà intellettuale, della garanzia e del funzionamento del servizio. Queste responsabilità, insieme a quelle relative alla conservazione, sono inserite nell'accordo sui servizi di certificazione, sottoscritto dall'utente e dal certificatore o da un suo delegato.

[57] Art. 28 della legge cinese sulle firme elettroniche.

[58] Artt. 29, 30 e 31 della legge cinese sulle firme elettroniche.

[59] Artt. 32 e 33 della legge cinese sulle firme elettroniche.

prestatore qualora questi dimostri che il danno subito dal titolare della firma, o dalla parte facente affidamento sulla firma elettronica, non gli sia imputabile. Nello specifico, il prestatore deve dare prova che i servizi da esso prestati siano stati svolti in stretta osservanza della legge in commento e delle disposizioni dello Stato nonché del CPS depositato presso il Ministero dell'Industria dell'Informazione.

In ottica comparata, dunque, è possibile notare come, nonostante le differenze in materia di responsabilità dei fornitori di servizi, i testi normativi presi in considerazione presentino anche alcuni elementi comuni come la presunzione di dolo o negligenza del prestatore, la responsabilità contrattuale e l'inversione dell'onere della prova.

Un ulteriore tema che si presta ad essere analizzato in chiave comparata è quello delle sanzioni, rispetto alle quali il Reg. e-IDAS detta una norma generale: «Gli Stati membri stabiliscono norme relative alle sanzioni da applicare in caso di violazioni del presente regolamento. Le sanzioni previste sono effettive, proporzionate e dissuasive»[60].

In Italia, con gli interventi dettati dal d. lgs. 26 agosto 2016, n. 179 e dal d. lgs. 13 dicembre 2017, n. 217, il legislatore ha inasprito la pena per la violazione di obblighi previsti dal Reg. e-IDAS e dallo stesso CAD. Riguardo alle sanzioni amministrative inflitte a seguito di violazioni degli obblighi in generale, è stato introdotto un regime sanzionatorio differenziato a seconda della gravità della violazione. In particolare, sono aumentati i minimi e i massimi edittali delle sanzioni pecuniarie che ora possono essere irrogate da un minimo di 40 mila e ad un massimo di 400 mila euro, in base alla gravità della violazione accertata e all'entità del danno cagionato all'utenza. In caso di gravi violazioni del CAD[61], l'Agenzia per l'Italia digitale (nel prosieguo, per brevità, "AgID") può disporre, in aggiunta, la cancellazione del fornitore del servizio dall'elenco dei soggetti qualificati e il divieto di accreditamento o qualificazione per un periodo non superiore a due anni[62]. L'art. 32-*bis*, c. 2, CAD prende poi in considerazione le ipotesi di malfunzionamento nei servizi offerti dai prestatori qualificati tale da comportare l'interruzione del servizio oppure la mancata o intempestiva comunicazione del disservizio all'AgID e agli utenti. In questi casi, a meno che si provi la forza maggiore o il caso fortuito, l'AgID può irrogare sanzioni amministrative al prestatore qualificato. Si prevede altresì la cancellazione dall'elenco pubblico del prestatore qualificato in caso di reiterazione dell'inadempimento nel biennio successivo alla prima diffida dell'Autorità volta a richiedere il ripristino della regolarità dei servizi. Infine, le sanzioni di cui all'art. 32-*bis* sono aumentate fino al doppio in caso di violazioni degli obblighi del prestatore di servizi fiduciari qualificato relativi alla cessazione dell'attività, nonostante l'intimazione da parte dell'AgID ad ottemperarvi entro un termine non superiore a trenta giorni[63].

Muovendo alla legge cinese sulle firme elettroniche, questa riconosce una responsabilità civile in capo al certificatore nelle ipotesi di violazione degli artt. 19, 20, 21, 22 e

[60] Art. 16 del Reg. e-IDAS.

[61] Secondo quanto disposto dall'art. 32-*bis*, c. 1, CAD, si considerano gravi «le violazioni del presente Codice idonee a esporre a rischio i diritti e gli interessi di una pluralità di utenti o relative a significative carenze infrastrutturali o di processo del fornitore di servizio».

[62] Art. 32-*bis* del CAD.

[63] Art. 37, c. 4-*ter*, CAD.

24 per danni cagionati al firmatario e ai terzi che hanno fatto affidamento sulla firma. In particolare, agli artt. 29 e 30 della legge cinese sulle firme elettroniche sono sancite sanzioni di natura amministrativa per le ipotesi di violazione dell'obbligo di tempestiva comunicazione in caso di sospensione e cessazione dell'attività[64], e di esercizio del servizio senza licenza[65]. Nulla, invece, è previsto per i casi di disservizio o disfunzione emergenziale del sistema di certificazione.

Altre sanzioni sono previste per le violazioni degli obblighi relativi al CPS o per l'inadempimento relativo alla conservazione di informazioni, ma possono essere irrogate solamente se il soggetto intimato a porvi rimedio non ottempera all'obbligo prescritto[66]. In questa eventualità, le conseguenze consistono nella revoca della licenza e nel divieto, al dirigente direttamente responsabile e al diretto incaricato, di prestare servizio per un periodo di dieci anni.

Nel 2009, sono state introdotte ulteriori ipotesi di violazione, quali l'occultamento di informazioni[67], il rifiuto dell'obbligo di sostituire il prestatore che cessa l'attività, la mancata notifica di modifiche del CPS e di *policy* di certificato[68]. Nel caso in cui il prestatore di servizio commetta tali violazioni, il Ministero può intimargli di porvi rimedio entro un determinato termine e, in caso di inottemperanza, può irrogare una sanzione pecuniaria dai cinque mila ai dieci mila RMB. La sanzione pecuniaria inflitta per intempestiva comunicazione di sospensione o cessazione dell'attività[69] è, invece, di importo pari a 1.000-7.000€, cifra decisamente modesta se paragonata ai fatturati di prestatori come iTrust Co.ltd che rilascia 500.000 certificati all'anno.

Infine, non sono previste sanzioni pecuniarie per violazioni relative alla verifica dell'identità del destinatario del servizio, alle garanzie volte ad assicurare l'integrità e l'esattezza delle informazioni contenute nel certificato[70] e all'obbligo di conservazione[71]. Quanto invece al risarcimento del danno derivante dalla condotta inadempiente del certificatore, la prassi è quella di stabilirne l'ammontare all'interno dell'accordo contrattuale tra le parti e spesso questo è pari alle spese di rilascio del certificato. In questo modo, viene fissato, di fatto, un limite alla responsabilità del certificatore.

64 Art. 23 della legge cinese sulle firme elettroniche.

65 Ai sensi dell'art. 29 della legge cinese sulle firme elettroniche, per le attività illecite di prestazione di servizi di certificazione elettronica senza licenze, oltre all'immediata cessazione dell'attività, è prevista l'irrogazione di una sanzione pecuniaria di importo pari a 300 mila RMB. Per la violazione dell'obbligo di comunicare la sospensione dell'attività, entro il termine stabilito, la sanzione amministrativa prevista dall'art. 30 della legge cinese sulle firme elettroniche va da un minimo di 10.000 yuan ad un massimo di 50.000 yuan.

66 A questo proposito, si vedano gli artt. 31, 19 e 24 della legge cinese sulle firme elettroniche.

67 Art. 38 della legge cinese sulle firme elettroniche.

68 Art. 40 della legge cinese sulle firme elettroniche.

69 Art. 23 della legge cinese sulle firme elettroniche.

70 Artt. 21 e 22 della legge cinese sulle firme elettroniche.

71 Art. 24 della legge cinese sulle firme elettroniche.

4. Sul valore probatorio della firma qualificata

Nel seguente paragrafo sono esaminate le questioni connesse agli effetti giuridici della firma qualificata e all'efficacia probatoria del documento informatico a cui è apposta.
A tale proposito, giova innanzitutto richiamare l'art. 25 del Reg. e-IDAS che sancisce l'equivalenza degli effetti giuridici della firma elettronica qualificata rispetto a quelli di una firma autografa e stabilisce l'interoperabilità delle firme elettroniche qualificate basate su un certificato qualificato tra gli Stati membri.
Analogamente, il legislatore italiano attribuisce alla firma elettronica qualificata un valore giuridico più elevato e riconosce al documento informatico sottoscritto con tale firma un'efficacia probatoria rafforzata rispetto alle altre tipologie di firme informatiche, ossia quella semplice e quella avanzata[72]. L'art. 21, c. 2-*bis*, CAD riserva infatti alla firma elettronica qualificata e alla firma digitale la sottoscrizione degli atti di cui all'art. 1350, c. 1, numeri da 1 a 12, c.c., a pena di nullità. Sotto il profilo probatorio, invece, l'art. 20, c. 1-*bis*, stabilisce che il documento informatico sottoscritto con firma digitale, altro tipo di firma elettronica qualificata o firma elettronica avanzata[73], soddisfa il requisito della forma scritta e ha efficacia probatoria *ex* art. 2702 c.c., ossia fa piena prova fino a querela di falso della provenienza delle dichiarazioni da chi l'ha sottoscritta, a condizione che la sottoscrizione sia legalmente considerata come riconosciuta, o riconosciuta esplicitamente o tacitamente dall'apparente sottoscrittore[74].
Il rinvio all'art. 2702 c.c. consente di richiamare l'istituto del disconoscimento[75] della scrittura privata e della sottoscrizione[76]. Come è noto, il procedimento di disconoscimento della scrittura privata e della sottoscrizione autografa consiste in una formale negazione della paternità, tempestivamente avanzata in giudizio da parte di colui con-

[72] In dottrina sul tema, seppur antecedenti al CAD: A. Gentili, *Documento informatico e tutela dell'affidamento*, in *Riv. dir. civ.*, II, 1998, 163 ss.; A. Graziosi, *Premesse ad una teoria probatoria del documento informatico*, in *Riv. dir. proc. civ.*, 1998, 481 ss.; Id, voce *Documento informatico (diritto processuale civile)*, in *Enc. dir. Annali*, II, Milano, 2008, 492 ss.; M. Orlandi, *La paternità delle scritture: sottoscrizioni e forme equivalenti*, Milano, 1997; Id, *Il falso digitale*, Milano, 2003. Tra le opere monografiche: G. Navone, Instrumentum *digitale: teoria e disciplina del documento informatico*, Milano, 2012.

[73] Giova precisare che, a seguito della riforma operata dal d.lgs. 217/2017, è stato introdotto un ulteriore processo di firma consistente nel «processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore». Anche tale documento ha l'efficacia probatoria *ex* art. 2702 c.c. ed è ritenuto idoneo a soddisfare la forma scritta.

[74] Ai sensi dell'art. 20, c. 1-*bis*, CAD, il documento informatico non sottoscritto o sottoscritto con firma elettronica semplice, invece, è, sotto il profilo probatorio, liberamente valutabile dal giudice, tenuto conto delle sue caratteristiche oggettive di sicurezza, integrità e immodificabilità in concreto. Cfr. G. Finocchiaro, *Diritto di Internet*, cit., 87 e 88.

[75] Cfr. G. Buonomo, *La scrittura privata informatica: firme elettroniche, valore probatorio e disconoscimento in giudizio (alla luce delle modifiche introdotte dalla l. 221/2012)*, in *Dir. Inf.*, 2, 2013, 255 ss.

[76] Art. 214 c.p.c., rubricato "Disconoscimento della scrittura privata": «Colui contro il quale è prodotta una scrittura privata, se intende disconoscerla, è tenuto a negare formalmente la propria scrittura o la propria sottoscrizione. Gli eredi o aventi causa possono limitarsi a dichiarare di non conoscere la scrittura o la sottoscrizione del loro autore». Si veda anche l'art. 216 c.p.c., rubricato "Istanza di verificazione": «La parte che intende valersi della scrittura disconosciuta deve chiederne la verificazione, proponendo i mezzi di prova che ritiene utili e producendo o indicando le scritture che possono servire di comparazione».

tro il quale è prodotta la scrittura privata cartacea o la sottoscrizione autografa. La parte che voglia avvalersi della scrittura o sottoscrizione eventualmente disconosciuta dovrà esperire un procedimento di verificazione affinché il giudice disponga la comparazione di scrittura e di grafia, con l'eventuale supporto di una perizia grafologica[77], al fine di accertare la paternità della scrittura e della sottoscrizione autografa, intesa come diretta riferibilità di questi ultimi al sottoscrittore. La firma autografa è infatti un gesto fisico personale che imprime sulla carta un segno indelebile della volontà del sottoscrittore ed è, dunque, indissolubilmente legata al firmatario[78].

Alla luce di quanto appena esposto, appare inverosimile pensare di riferirsi al concetto di paternità – tradizionalmente inteso – anche in relazione alle firme informatiche apposte sul documento informatico. Invero, queste ultime non sono il risultato della mano che traccia, fissando la grafia su un supporto analogico. Si tratta piuttosto di un processo che il firmatario, avvalendosi di un dispositivo per la creazione di firma o di servizi offerti da soggetti terzi, realizza seguendo istruzioni ben precise. Il processo è impersonale, soprattutto quando vi è una scarsa consapevolezza da parte del firmatario o quando non si ha simultaneità tra il gesto manuale e la volontà, frammentando e segmentando così l'espressione di sovranità. In considerazione delle differenze di cui sopra, il disconoscimento della scrittura privata e della sottoscrizione autografa non sembra ammissibile in caso di firma elettronica qualificata e firma digitale[79]. Se lo fosse, il destinatario del documento informatico dovrebbe adempiere ad un *onus probandi* pressoché impossibile. Dal canto suo, invece, il titolare della firma potrebbe limitarsi a negare l'utilizzo della firma[80].

Nel tentativo di porre rimedio ai problemi di autenticità collegati all'uso della firma elettronica qualificata che non consente di individuare il soggetto che effettivamente utilizza il dispositivo di firma, ma solamente colui che ne è titolare[81], il legislatore italiano compie un passo ulteriore rispetto alla disciplina europea[82]. Infatti, grazie all'introduzione dell'art. 20, c. 1-*ter*, CAD, viene sancito che «l'utilizzo del dispositivo di firma

[77] Art. 216 del c.p.c.

[78] F. Carnelutti, *Studi sulla sottoscrizione*, in *Riv. dir. comm.*, I, 1929, 509.

[79] Trattano il tema del disconoscimento della firma: A. Gentili, *I documenti informatici: validità ed efficacia probatoria*, in *Dir. internet*, 2006, 308 e il Consiglio di Stato – Sezione Consultiva per gli Atti Normativi, nel parere reso in occasione dell'adunanza del 30 gennaio 2006, n. 31, avente ad oggetto la bozza di decreto legislativo recante disposizioni correttive e integrative al d.lgs. 7 marzo 2005, n. 82, entrambi ritenendolo come del tutto peculiare.

[80] Cfr. G. Finocchiaro, *La firma digitale. Formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici.,* in F. Galgano (a cura di), *Libro VI, Della tutela dei diritti, art. 2699-2720. Commentario del Codice Civile Scialoja-Branca*, Bologna, 2000, 127.

[81] G. Finocchiaro, *La firma digitale*, cit., 7.

[82] Gli artt. 29 e 30 del Reg. e-IDAS introducono alcuni importanti requisiti. In primo luogo, i dispositivi di creazione di firma qualificata devono essere muniti di certificazione di sicurezza. In secondo luogo, la firma elettronica qualificata deve essere munita di un certificato qualificato fornito da un prestatore di servizi fiduciari qualificato. Queste disposizioni – assieme ad altre – sono volte ad assicurare l'identificabilità del soggetto titolare del dispositivo per la creazione della firma. In particolare, il certificato qualificato ha una funzione identificativa del soggetto titolare della firma e del soggetto che l'ha certificata, nonché di affidabilità rispetto al registro su cui essa è stata pubblicata per la consultazione. La qualifica di titolare della firma, in questi casi, si riferisce al titolare del dispositivo per la firma, ossia della chiave privata certificata.

elettronica qualificata o digitale si presume riconducibile al titolare di firma elettronica, salvo che questi dia prova contraria». Si introduce, quindi, una presunzione di corrispondenza tra l'utilizzatore del dispositivo e la figura del firmatario, il quale è di norma il titolare legittimo del dispositivo, a meno che non ne perda il possesso.
Da tale presunzione relativa è possibile far discendere due corollari principali.
In primo luogo, il titolare del dispositivo è gravato dell'obbligo di diligenza nella custodia e nella cura del dispositivo di firma elettronica qualificata. Infatti, ai sensi dell'art. 32 del CAD, rubricato "Obblighi del titolare di firma elettronica qualificata e del prestatore di servizi di firma elettronica qualificata", «il titolare del certificato di firma è tenuto ad assicurare la custodia del dispositivo di firma o degli strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma da remoto, e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma». Tali obblighi non sono, invece, previsti dal Reg. e-IDAS.
In secondo luogo, il titolare del dispositivo è gravato dell'onere di fornire la prova contraria nel caso in cui intenda negare che si tratti della propria firma. Ciò comporta che questi, per vincere la presunzione, debba dimostrare che un terzo si sia servito della chiave privata dopo essersene indebitamente impossessato[83].
Ci si interroga, allora, riguardo al tipo di prova di cui il titolare del dispositivo può concretamente disporre per contestare la riferibilità della sottoscrizione di un documento informatico mediante una firma elettronica qualificata o digitale. A questo proposito occorre evidenziare che, diversamente dal disconoscimento previsto dall'art. 241 c.p.c., l'oggetto del disconoscimento di cui all'art. 20, c. 1-*ter*, CAD, da parte dell'apparente sottoscrittore non è la firma o la scrittura, bensì l'utilizzo del dispositivo di firma elettronica qualificata o digitale. Di conseguenza, il giudice valuterà il fatto in base ad un criterio di responsabilità alla luce dei criteri dell'art. 32 CAD già esaminati, e non invece sulla base di un criterio di paternità[84].
Dunque, in caso di utilizzo abusivo causato da perdita o furto del dispositivo di firma qualificata, il titolare del dispositivo può provare il falso, dimostrando: a) di non aver utilizzato il dispositivo in un dato momento, con l'allegazione attestante la perdita del dispositivo in un momento anteriore all'apposizione della firma (ad esempio, la denuncia di smarrimento del dispositivo); b) che la causa della perdita o del furto del dispositivo non gli è imputabile; c) di aver adottato tutte le misure tecniche e organizzative per

[83] A tal riguardo, il Consiglio di Stato, nel parere emesso il 30 gennaio 2006, ha affermato che «il documento informatico, munito di firma digitale, sembra porsi, per effetto dell'inversione dell'onere della prova in tema di disconoscimento, come una sorta di *tertium genus* tra la scrittura privata e l'atto pubblico, avendo in giudizio la stessa efficacia probatoria di una scrittura privata munita di sottoscrizione legalmente riconosciuta, ed essendo, in realtà, in nulla diverso da una scrittura privata munita di sottoscrizione non autenticata». Cfr. F. Delfini, *Documento informatico, forma analogica e forma elettronica: dalla scrittura privata autenticata all'atto pubblico informatico,* in F. Delfini – G. Finocchiaro (a cura di), *Diritto dell'informatica*, cit., 2014, 262.

[84] Il Consiglio di Stato, Sezione Consultiva per gli Atti Normativi, nell'Adunanza del 7 febbraio 2005, ha sottolineato l'importanza di «superare i vecchi concetti di falso, strettamente legati al principio di 'paternità' della firma e non a quello di 'responsabilità' per la firma». Si veda anche il parere del Consiglio di Stato emesso il 30 gennaio 2006. In questa occasione, il Consiglio di Stato ha affermato che «sarebbe (…) opportuno individuare il tipo di prova che consente il disconoscimento secondo un criterio di responsabilità nella conservazione e nell'utilizzo della chiave privata».

evitare i danni ai terzi, allegando la richiesta al prestatore di servizi fiduciari qualificato di revoca o sospensione del certificato[85] non appena sia venuto a conoscenza della perdita o della compromissione del dispositivo; d) di essere estraneo alle dichiarazioni emesse imputategli dalla firma digitale; e) di non conoscere il destinatario delle dichiarazioni firmate digitalmente. Tali prove sono finalizzate a sottrarre qualsivoglia valore giuridico al documento sottoscritto, eliminandone – oltre all'efficacia sua propria – qualsiasi ulteriore effetto attribuitogli dalla legge. Il titolare del dispositivo può, altresì, citare in giudizio il prestatore di servizio fiduciario qualificato, qualora si sia verificato un ritardo nella pubblicazione delle informazioni relative allo smarrimento del dispositivo, ossia un'anomalia del processo di firma. Come già accennato, l'apprezzamento del giudice si baserà sul criterio di responsabilità del titolare del dispositivo e del prestatore di servizi fiduciari qualificato. In particolare, in tema di responsabilità del prestatore di servizi fiduciari qualificato, si è precedentemente ricordato che l'art. 13, par. 1, Reg. e-IDAS dispone che «i prestatori di servizi fiduciari sono responsabili di danni causati, con dolo o per negligenza, a qualsiasi persona fisica o giuridica in seguito a un mancato adempimento degli obblighi di cui al presente regolamento». Al contrario, l'art. 30, c. 1, CAD attribuisce al prestatore di servizi fiduciari qualificato la responsabilità risarcitoria per il danno cagionato ad altri nello svolgimento della loro attività, a meno che non provi di aver adottato tutte le misure idonee ad evitare il danno. In conclusione, pare possibile individuare solo un limitato numero di mezzi di prova di cui il titolare della firma elettronica qualificata o digitale dispone per eccepire che la firma gli sia imputabile. Al fine di ovviare a tali criticità, sembra auspicabile affidarsi alla tecnologia, creando un meccanismo procedimentale che garantisca l'identificazione del soggetto nel momento di effettiva apposizione della firma da parte di questi.

Discorso diverso è invece quello relativo all'invalidità della firma digitale. In dottrina, sono state elaborate diverse ipotesi di invalidità della firma digitale, quali l'erronea attribuzione del certificato, l'utilizzo abusivo della chiave privata e così via. Nell'ipotesi di utilizzo abusivo della chiave privata in un rapporto giuridico contrattuale, ci si è domandati se la fattispecie sia riconducibile al riempimento non autorizzato del foglio firmato in bianco, *absque pactis*, o alla fattispecie del *falsus procurator* o *falsus dominus*[86]. Il primo caso ricorre quando l'autore del riempimento non sia stato autorizzato dal sottoscrittore con preventivo patto. Nel secondo caso, per *falsus procurator* si intende colui «che ha contrattato come rappresentante senza averne i poteri o eccedendo i limiti delle facoltà conferitegli dal rappresentato»[87], mentre con *falsus dominus,* ci si riferisce alla fattispecie generale della dichiarazione sotto falso nome o sotto nome altrui. La questione necessiterebbe di una trattazione più approfondita che esula tuttavia dallo scopo della presente analisi. In ogni caso, occorre sottolineare che, con riferimento all'efficacia probatoria e ai rimedi processuali, l'orientamento dottrinale prevalente riconosce l'applicabilità della disciplina del foglio firmato in bianco e della querela

[85] Art. 32, c. 3, lett. g), CAD.

[86] Cfr. G. Finocchiaro, *La firma digitale,* cit., 134 ss.

[87] Art. 1398 c.c., rubricato "Rappresentanza senza potere": «colui che ha contrattato come rappresentante senza averne i poteri o eccedendo i limiti delle facoltà conferitegli, è responsabile del danno che il terzo contraente ha sofferto per avere confidato senza sua colpa nella validità del contratto».

di falso al documento informatico firmato con chiave privata usata abusivamente[88]. Al contrario, si è respinta la possibilità di assimilare l'ipotesi di utilizzo abusivo della chiave privata, alle fattispecie del *falsus procurator* e del *falsus dominus* che presuppongono che l'autore dell'atto abusivo sia individuabile e sia conosciuto dal firmatario o dal *dominus*[89]. Nel contesto della sottoscrizione tramite firma elettronica qualificata o firma digitale, infatti, è assai improbabile che il legittimo titolare del dispositivo possa identificare l'utilizzatore abusivo dal momento che quest'ultimo non instaura alcun rapporto giuridico obbligatorio con il titolare legittimo della firma, ma solamente con il destinatario delle dichiarazioni, diretto beneficiario delle dichiarazioni emesse dall'apparente sottoscrittore. Di conseguenza, il criterio di responsabilità contrattuale tra il titolare del dispositivo e l'utilizzatore abusivo non sembra potersi applicare, a meno che l'utilizzatore abusivo sia egli stesso il destinatario delle dichiarazioni oggetto della controversia. Altrettanto inverosimile è la configurazione di una responsabilità di natura extracontrattuale: qualora l'utilizzo del dispositivo da parte dell'utilizzatore abusivo, in luogo del legittimo titolare, venga qualificato alla stregua di atto illecito, riconducibile all'art. 2043 c.c., il soggetto danneggiato finirebbe per dover produrre le prove del dolo o della colpa dell'utilizzatore abusivo, per giunta ignoto. Questo ragionamento non è condivisibile data la difficoltà per il danneggiato di adempiere a tale onere probatorio.
Sotto questi profili, la normativa cinese appare innovativa.
Nel 2015, infatti, la legge cinese sulle firme elettroniche ha introdotto l'art. 14, ai sensi del quale: «una firma elettronica affidabile ha i medesimi effetti giuridici di una firma autografa o di un sigillo». Per rendere effettiva la disposizione, il governo cinese ha adottato una strategia di ampio respiro. In primo luogo, al fine di assicurare l'affidabilità tecnologica e gestionale della firma, è stato ideato un progetto per la creazione di una rete fiduciaria basata sul *Public Key Infrastructure* (nel prosieguo, per brevità, "PKI") che si interfaccia con il sistema di autenticazione elettronica attraverso un processo gestionale di autorizzazione, valutazione e individuazione di responsabilità. In secondo luogo, sono state predisposte ingenti risorse da investire in ricerca e sviluppo dei prodotti crittografici insieme a sistemi gestionali, quale *core technology* della certificazione della firma elettronica[90]. Inoltre, occorre sottolineare che, sul versante tecnologico, il governo cinese ha designato le società, come E Sign, preposte a sviluppare prodotti crittografici per uso commerciale, prodotti e sistemi autonomi sviluppati in Cina, per assicurare la sicurezza di rete e di informazione[91]. La *State Cryptography Administration* ha

[88] Cfr. G. Finocchiaro*, La firma digitale,* cit., 142.

[89] Ivi, 136 e 139.

[90] Cfr. http://www.sca.gov.cn/sca/xwdt/2006-05/26/content_1002342.shtml国家密码管理局魏允韬副局长在“电子签名法” 实施一周年暨电子认证服务业发展研讨会”上的讲话. In un intervento del 26 maggio 2006, il vice direttore della *State Cryptography Administration* Wei Yuntao ha fatto un bilancio a distanza di un anno dall'entrata in vigore della legge cinese sulle firme elettroniche, ribadendo che il codice segreto è la *core* tecnologia per l'applicazione della legge. Lo stesso vice direttore ha dichiarato che è pronta una gamma di prodotti crittografici commerciali ormai consolidati per soddisfare le esigenze del settore dei servizi di certificazione elettronica.

[91] Cfr. https://baijiahao.baidu.com/ CA. Stando ai dati dell'Istituto di ricerca dell'industria dell'informazione, alla fine del 2017, vi erano 34 service *providers* di firme elettroniche da parte di terzi, di cui 7 affiliate a prestatori di certificazione elettronica (CA), mentre 22 dedicate prettamente ai contratti elettronici. Il volume di affari ha visto un incrementato del 200% dal 2015 al 2017 e ha raggiunto un

il compito di accreditare la CA che utilizza codici segreti per uso commerciale nei servizi di certificazione elettronica *e-government*, e di gestire insieme ai relativi dipartimenti le firme elettroniche e i messaggi di dati utilizzati in attività governative[92].

Sul versante della regolamentazione, invece, a partire dal 2016, è stata adottata una serie di norme tecniche volte a uniformare il format dello standard nazionale del documento elettronico[93] e il processo di apposizione di firma elettronica affidabile. In particolare, dal novembre 2016, è in vigore il National standard GB/15843.3-2016 per l'autenticazione di soggetti, che adotta il meccanismo di firma digitale[94], compatibile con lo standard ISO/IEC 9798-3:1998, IDT. Dal 2018, invece, è entrato in vigore lo standard nazionale GB/T 36651-2018 "Protocollo di tecnologia informatica della sicurezza per l'identificazione biometrica in ambiente attendibile"[95]. Si tratta di uno dei trentasei standard nazionali in vigore per l'identificazione biometrica che la Cina ha sviluppato dal 2012 al 2018 in tema di autenticazione dell'identità. Nello stesso anno, sono state adottate le "Specifiche tecniche generali della tecnologia informatica di sicurezza per la firma mobile"[96] e i "Requisiti tecnici per la creazione e verifica delle firme elettroniche affidabili basati sul certificato digitale con l'infrastruttura PKI"[97]. Questi ultimi mirano a colmare la lacuna legislativa relativa ai requisiti tecnici per la creazione e la verifica della firma affidabile. Inoltre, qualificando come affidabile la firma elettronica basata sul certificato digitale, il legislatore si pone in continuità con la prassi internazionale.

Infine, la strategia adottata dal governo cinese in materia di prove informatiche comprende numerosi interventi in ambito giudiziario. In particolare, a partire dalla metà del 2016, con l'avvento di *Internet Plus*, il sistema giudiziario cinese è diventato digitale e la tecnologia informatica sta trasformando i tribunali in luoghi virtuali ampiamente

miliardo di Yuan nel 2018. La piattaforma E-Sign (e签宝) ha superato i 100 milioni di yuan di fatturato nel 2019, con 400 mila utenti aziendali e 10 milioni di utenti individuali. Nel 2016, 10 aziende cinesi raggiungevano un fatturato di oltre 1 milione di yuan. Inoltre, sempre nel 2016, stando ai dati di Saizhiku citato dell'Istituto, 35 piattaforme di firma elettronica gestite da terzi hanno investito più di 100 milioni di yuan in ricerca e sviluppo tecnologico.

92 Cfr. Art. 29 della legge sulla crittografia della Repubblica Popolare della Cina, in vigore dal 1° gennaio 2020.
第二十九条　国家密码管理部门对采用商用密码技术从事电子政务电子认证服务的机构进行认定，会同有关部门负责政务活动中使用电子签名、数据电文的管理.

93 Si fa riferimento allo "Standard nazionale OFD per l'immodificabilità del documento elettronico". Tale standard si applica all'archiviazione, lettura, EDI e utilizzo di documenti standard, in ambiti *e-commerce*, *e-government*, EDI, rilascio di informazioni, pubblicazione digitale e gestione degli archivi.

94 "信息技术安全技术实体鉴别第3部分：采用数字签名技术的机制（补篇）", 2016年11月实施. 由国家质量监督检验检疫局与国家标准化管理委员会联合发布。pubblicato il 25 aprile 2016 dall'Amministrazione nazionale di supervisione, controllo e quarantena insieme alla Commissione di gestione in standardizzazione nazionale.

95 "信息安全技术基于可信环境的生物特征识别身份鉴别协议".

96 "信息安全技术移动签名通用技术规范". Il documento definisce i termini tecnici relativi alla firma mobile e specifica le regole sui dispositivi dotati di funzione di comunicazione mobile, sull'applicazione, progettazione, sviluppo e test dei sistemi di firma elettronica nei dispositivi di comunicazione.

97 "信息安全技术/公钥基础设施基于数字证书的可靠电子签名生成及验证技术要求" 2017年12月29日发布， 2018年7月1日实施. Adottato dalla Commissione nazionale di standardizzazione tecnica della sicurezza cibernetica, pubblicato il 29 dicembre 2017, in vigore dal 1° luglio 2018.

accessibili. La solennità del Palazzo di giustizia e del processo è stata sostituita dai colloqui informali via *Wechat* o *Skype*, con la possibilità di seguire le udienze in qualsiasi luogo fisico. Dal 2017, sono state istituite tre *Internet Court*[98]. Nel 2018, la Corte di Internet di Hangzhou[99] ha inaugurato la prima piattaforma[100] per l'acquisizione di prove informatiche basate sulla *blockchain*[101], con un *database* di oltre 1,95 milioni di prove, tra cui certificati notarili e prove peritali, prove di piattaforme da parte di terzi, prove di conservazione e di verifica, atti pubblici, prove di decisioni arbitrali. Nel giro di pochi anni, sono nati anche la piattaforma del sistema giudiziario nazionale per i servizi di iscrizione a ruolo di cause via *Wechat*[102] e il sistema *one-stop* di servizio di arbitrato *online* istituito da Fadada insieme all'arbitrato Guangzhong e il micro-tribunale mobile. Al fine di innovare il proprio sistema giudiziario, assicurando processi più semplici e ve-

[98] https://baike.baidu.com/item/杭州互联网法院. La Corte di Internet di Hangzhou è stata inaugurata il 18 agosto 2017, come la prima corte pilota nazionale che tratta controversie *online*. A settembre 2018, sono state istituite altre due corti a Pechino e Guangzhou. La Corte di Internet, ricorrendo alle tecnologie di rete, completa l'intero procedimento giudiziario *online*, dall'atto di citazione, iscrizione a ruolo, deposito di prove, udienza, al giudizio sino all'esecuzione. L'obiettivo è quello di facilitare il processo giudiziario civile per i cittadini, risparmiando risorse giudiziarie. L'innovazione del meccanismo è integrata tramite la predisposizione di molteplici e diversificati metodi di risoluzione delle controversie come quelli in via preventiva, mediazione di terze parti e processo. Grazie ad una gestione professionale, efficiente e conveniente delle controversie *online*, avvalendosi di tecnologie di analisi di *Big Data* e facendo un raffronto tra vari moduli, si cera di formulare regole strutturate e standardizzate di giudizio su Internet.

[99] In un anno, la Corte di Internet di Hangzhou ha trattato 12.103 casi concludendone 10.646.

[100] Cfr. https://www.8btc.com. La piattaforma è collegata a più interfacce di dati. La Corte può trasmettere, verificare e archiviare rapidamente, attraverso la piattaforma, i dati elettronici rilevanti. La Corte può altresì accedere direttamente alle piattaforme di *e-commerce* per ottenere informazioni sulla transazione relativa alla causa. Tutti i più importanti *service provider* come Taobao, JD.com e piattaforme *e-commerce*, di contratti elettronici e conservazione di certificati, possono diventare fornitori di prove informatiche per la piattaforma della Corte. Ciò significa che se le parti desiderano proporre le prove sulle transazioni attraverso la piattaforma *e-commerce*, possono semplicemente inserire nella piattaforma di contenzioso o nella piattaforma di prove informatiche il numero d'ordine per recuperare le informazioni rilevanti sulla transazione. Se i dati del caso sono conservati su un'altra piattaforma già connessa, le parti devono solo inviare il numero *hash* della conservazione di dati, mentre spetterà alla Corte di Internet il compito di completare la comparazione intelligente dei valori *hash* ed accedere ai dati attraverso la piattaforma di prove informatiche. Se i dati verificati risultano corrispondenti ai fatti, sono assunti nell'ambito della domanda giudiziaria.

[101] Cfr. https://www.chinacourt.org/article/detail/2018/10/id/3522776.shtml. La *blockchain* è strutturata in tre livelli. Il primo è il livello del programma di *blockchain*. L'utente può, tramite il programma, registrare direttamente nella *blockchain* tutte le sue operazioni ossia consegnare *online* le prove informatiche quali contratto elettronico, processo di tutela dei diritti e specifiche del processo di servizio. Il secondo è il livello di competenza di tutto l'itinerario della *blockchain*. In questa fase si forniscono servizi fiduciari affidabili quale l'autenticazione del nome reale, la firma elettronica, la marca temporale, la conservazione di dati. Il terzo è il livello di alleanza giudiziaria. Mediante la tecnologia *blockchain*, si possono connettere istituti notarili, CA/RA, il centro di valutazione giudiziario e i tribunali, ed ognuno rappresenta un nodo della catena. Con tale impalcatura, la *blockchain* giudiziaria è in grado di risolvere i problemi di affidabilità dei dati elettronici per tutto i loro ciclo di vita.

[102] Cfr. https://www.qianzhan.com. Il 25 dicembre 2017 è stata istituita la prima piattaforma nazionale del sistema giudiziario che offre servizi via *Wechat* di iscrizione a ruolo di cause. L'attore, in qualunque posto e qualsiasi momento, una volta ottenuto via *Wechat* il numero d'iscrizione a ruolo, può effettuare via telefono mobile tutto la procedura, tra cui l'invio di materiali di contenzioso, il deposito delle prove, l'autenticazione dei nomi reali e il pagamento di spese di giustizia. Si tratta di contenzioso amministrativo e civile in materia di commercio.

loci per i cittadini[103], il governo cinese ha saputo sfruttare al meglio l'incremento del livello tecnologico imprenditoriale delle firme elettroniche così come lo sviluppo di Internet mobile, *cloud computing*, *blockchain*, "*mobile phone shield*" – sistema di autenticazione mobile "sicuro e conveniente" –, sistemi di conservazione di firme elettroniche e sistemi di certificazione "blockchain".

Se in passato i professionisti facevano affidamento su autorità terze, come i notai, per acquisire e costituire le prove, oggi, il crescente ricorso a prove informatiche in giudizio ha determinato la nascita, in Cina, di molte piattaforme di dati elettronici gestite da soggetti terzi, tra cui Factom e E-Sign[104]. La piattaforma E-Sign, ad esempio, si coordina con le istituzioni di valutazione giudiziaria, gli istituti notarili, gli arbitrati, i tribunali e altre istituzioni considerate affidabili per costruire un'alleanza *blockchain*, ossia un *database* di prove congiunte, attraverso il sistema di archiviazione distribuita della *blockchain*, caratterizzata dall'immodificabilità dei *file* che, utilizzando l'algoritmo *hash* irreversibile, generano una catena di codici memorizzata sulla piattaforma. Il medesimo *file* viene contestualmente memorizzato presso istituzioni di valutazione giudiziaria, istituti notarili e arbitrali, realizzando una validazione incrociata delle prove. Così facendo, tali piattaforme hanno realizzato un modello di *business* costruito sulla base delle loro condizioni tecniche e dei loro obiettivi commerciali, diretto ad offrire servizi verso terzi di raccolta e acquisizione di prove informatiche.

Al fine di legittimare l'uso delle tecnologie disponibili, il 18 giugno 2018 sono state adottate "Le disposizioni della Corte suprema del popolo su alcune questioni processuali nella corte di Internet"[105] (di seguito, per brevità, "Disposizioni"). In particolare, l'art. 11[106] prevede che la Corte di Internet riconosca i dati elettronici presentati dalle parti, mediante mezzi tecnici di raccolta, acquisizione e antimanomissione di prove informatiche quali firme elettroniche, marcatempo affidabile, verifica sui valori dell'*hash* e della *blockchain*, oppure per mezzo di certificati rilasciati dalla piattaforma di costituzione e acquisizione di prove, che dimostrino la loro autenticità. Dunque, per la prima volta, la Cina ha riconosciuto, in via interpretativa, i mezzi di costituzione e acquisizione di prove come marca temporale e *blockchain*. Il primo caso di assunzione di prove informatiche acquisite con la tecnica della *blockchain* nell'ambito del primo grado di giudizio è stato presentato innanzi alla Corte di Internet di Hangzhou che ne ha confermato l'efficacia probatoria all'interno di un contenzioso civile[107]. A tal proposito, è stato tuttavia precisato che la Corte mantiene un atteggiamento aperto e neutro volto

[103] Giova sottolineare, al riguardo, che la durata media del processo *online* è di 28 minuti ed il termine di conclusione di una causa è di 41 giorni, con una riduzione rispettivamente di tre quinti e metà del tempo rispetto a un processo tradizionale. Il tasso di accettazione della sentenza di primo grado è del 98,59%.

[104] "云法通" "可信时间戳" "存证云" "安存语录""e签宝" 为第三方电子数据平台.

[105] 2018年9月6日最高院发布《最高人民法院关于互联网法院审理案件若干问题的规定》，9月17日实施。Le Disposizioni offrono per la prima volta una specifica interpretazione giudiziaria dei casi presentati alla corte di Internet.

[106] "互联网法院审理案件若干问题的规定" 第11条: "当事人提交的电子数据，通过电子签名、可信时间戳、哈希值校验、区块链等证据收集、固定和防篡改的技术手段或者通过电子取证存证平台认证，能够证明其真实性的，互联网法院应当确认"。

[107] Cfr. http://www.sohu.com/a/240775254_100130948.

a valutare, caso per caso, tutti gli elementi ai fini della decisione[108], lasciando con ciò intendere che il primo caso giurisprudenziale sulle prove informatiche ottenute con la tecnologia *blockchain* non possa costituire un precedente giudiziario vincolante.

Dal quadro appena tratteggiato, emerge come la tecnologia della *blockchain*[109] abbia avuto un ruolo centrale nel permettere di acquisire le prove informatiche imponendo una nuova prospettiva nella prassi giudiziaria[110].

Alla base della spinta propulsiva verso le nuove tecnologie, vi sono i sostenitori della costruzione di un'alleanza *blockchain* per tutta la rete di tribunali a livello azionale[111].

Nonostante gli entusiasmi, non mancano alcune voci che invitano alla prudenza evidenziando le criticità della tecnologia *blockchain*[112].

Tra i difetti della *blockchain* si annoverano l'impossibilità di garantire l'autenticità dei

[108] Ivi. Così dichiarava la vice presidente Wang Yifei della Corte di proprietà intellettuale presso l'Alta corte popolare della Provincia dello Zhejiang.

[109] La *blockchain* è essenzialmente una struttura di archiviazione di dati che ricorre ad un algoritmo distribuito e decentralizzato così da creare diversi valori di memorizzazione in più nodi, con l'effetto di migliorare l'integrità e l'immodificabilità dei dati. Il cuore della tecnologia di marca temporale, crittografia e *blockchain* è la verifica del valore *hash*. I dati elettronici possono essere calcolati per ottenere un'unica "carta d'identità" non modificabile per garantirne l'integrità (Cfr. https://www.fadada.com/notice/detail-1496.html, 19 settembre 2018). Ogni transazione forma una struttura di dati indipendente, memorizzata in blocco. Il blocco contiene una marca temporale, il numero del blocco precedente, il valore *hash* del blocco precedente, i dati del blocco corrente. La *blockchain* garantisce, attraverso un meccanismo POS (*Proof of Stake*) e DPOS (*Delegated Proof of Stake*), che solo una persona possa produrre e trasmettere lo stesso blocco, e che altre persone possano sincronizzare la copia, senza possibilità di effettuare nessuna modifica. Il tentativo di manomissione dei dati su un blocco implica due operazioni da compiere contestualmente: ricalcolare il blocco corrente e tutti i blocchi successivi e sincronizzare la propria *blockchain* con la maggior parte dei nodi in tutta la rete. Poiché i nodi sulla *blockchain* aumentano costantemente, modificare decine di migliaia di nodi sull'intera rete prima che venga generato il blocco successivo, richiede una potenza di calcolo del nodo superiore della somma di potenza di calcolo di tutti gli altri nodi (Cfr. https://www.jianshu.com/p/8f0906077d73). In tema di *blockchain*, cfr. G. Finocchiaro – C. Bomprezzi, *A legal analysis of the use of blockchain technology for the formation of smart legal contracts*, in *questa Rivista,* 2, 2020, 111 ss.

[110] A questo proposito, giova ricordare che l'art. 9 del MLEC, con riferimento alle prove informatiche, dispone che la loro valutazione da parte del giudice debba avvenire sulla base di alcuni parametri, quali la loro affidabilità, il modo in cui i dati sono stati generati, archiviati o comunicati nonché il modo in cui l'integrità delle informazioni è garantita e in cui il mittente è stato identificato.

[111] Cfr. https://www.8btc.com/article. Secondo tal proposta, ogni tribunale, basandosi sul sistema processuale esistente, costituisce un nodo dell'alleanza della *blockchain* che ha il compito di verificare, firmare e supervisionarsi a vicenda tra più di 3.500 tribunali in Cina. Nella catena dell'alleanza giudiziaria applicata alla struttura gerarchica di corte suprema, provinciale, media, fino alla corte di base, si impiegherebbero tra gli 8 e i 10 minuti per sincronizzare tutti nodi utilizzando il meccanismo del consenso. Per costruire il sistema nazionale di acquisizione di prove informatiche con tecnica di *blockchain*, si calcola che la rete di 3.500 tribunali richiede la configurazione di circa 5.000 *server*. Si prevede un investimento iniziale di circa 20 milioni di yuan, ed un successivo costo annuo di circa 700 mila-10 milioni di yuan. In questo modo, con un modesto investimento, si potrebbe risolvere il problema della fiducia nelle prove informatiche e del controllo giudiziario su di esse, se si affida all'ordinamento giudiziario la direzione della "catena di alleanze" di prove informatiche, così da tutelare anche la sovranità giudiziaria della Cina.

[112] Cfr. http://www.nbd.com.cn/articles/2018-09-10. Il consigliere Xiao Feng dell'Associazione di ricerca giuridica della Bank of China rileva che i fatti del mondo reale non possono essere registrati meramente dalla tecnologia *blockchain*, come nel caso delle controversie concernenti i sinistri assicurativi aerei. In diverse occasioni, sono le registrazioni manipolate sulla catena a provocare il meccanismo di consenso. Il consigliere ritiene che per provare che i fatti siano effettivamente avvenuti, sia necessario verificare le prove documentali tradizionali, i messaggi di dati e le prove materiali.

dati aggiunti fuori dalla *blockchain* e l'incapacità di tenere il passo con la rapida evoluzione tecnologica. Infine, vi sono problemi di protezione dei dati personali e di sicurezza. Richiedendo impianti ad alta tecnologia per assicurare adeguate risorse computazionali, vi è soprattutto il rischio di dispersione, incompletezza o perdita di prove. Inoltre, le prove memorizzate nella piattaforma possono essere falsificate o manomesse e l'arco temporale a cui risale la prova elettronica può essere modificata in base ad una nuova impostazione della macchina, causando perdita di effetti giuridici e così via. A tal proposito, occorre rilevare che lo stesso art. 11 delle Disposizioni non precisa il controllo dello standard sul *software* applicativo e la validazione legale dei mezzi di costituzione e acquisizione delle prove[113].

Un'ulteriore questione critica riguarda la tendenza a concentrare il settore in esame nelle mani di pochi prestatori di firme elettroniche che detengono le tecnologie più avanzate. Ad esempio, la già citata E-Sign (e-签宝), una società di servizi di firme elettroniche fondata nel 2002, è l'unica del settore ad aver ottenuto i tre certificati rilasciati dalla *State Cryptography Administration*: il certificato del modello di dispositivo crittografico commerciale, il certificato di azienda designata per produrre i dispositivi crittografici commerciali, la licenza commerciale per prodotti crittografici. Nel 2018, la società è entrata a far parte dell'alleanza di tecnologie e industrie affidabili. I suoi prodotti alimentano tutti i sistemi domestici, quali *chip*, sistemi operativi, *database*, *middleware* e *file*, capaci di fornire servizi anche a clienti con elevate esigenze di sicurezza, quali *E-government* e alta finanza. Attraverso tale meccanismo di certificazione, una volta valutata l'affidabilità della tecnologia utilizzata, questa viene automaticamente riconosciuta anche alla firma elettronica derivata, senza necessità di una valutazione da parte del giudice.

Tuttavia, lo stretto connubio tra tecnologia e giustizia comporta il rischio di una potenziale ingerenza, in campo giudiziario, dei detentori di competenze tecnologiche. Nell'ordinamento giudiziario, tali soggetti, invece di essere sottoposti a sorveglianza, finiscono per dettare le regole sull'affidabilità, mentre gli interpreti del diritto sono relegati al ruolo di "apprendisti" delle regole tecniche. I protagonisti che partecipano alla redazione di standard nazionali sono le società di *software*. I *service provider* di dimensioni gigantesche hanno propri centri di ricerca e sviluppo e immettono sul mercato nuovi prodotti che vengono in seguito disciplinati dagli interpreti del diritto. La catena di alleanze tra l'apparato giudiziario, centri di valutazione giudiziaria, centri di certificazione e *service provider* presenta pertanto un altissimo grado di interdipendenza al punto di rendere molto difficile districarne le relazioni interne per rivendicare la terzietà e l'indipendenza della giustizia.

5. Questione sulla sovranità del firmatario elettronico

Le criticità connesse all'implementazione della firma elettronica erano ben note al le-

[113] Cfr. https://www.jianshu.com/p/8f0906077d73. È auspicabile che vengano stabilite al più presto norme uniformi per l'acquisizione di prove, comprese regole di implementazione procedurali e tecniche in conformità con le Disposizioni.

gislatore europeo sin dall'inizio della rivoluzione digitale. Difatti, la direttiva 1999/93/CE avvertiva della possibilità di registrazione e copia di dati per creare firme elettroniche che avrebbe potuto «costituire una minaccia per la validità giuridica delle firme elettroniche»[114].

La sicurezza rappresenta le fondamenta su cui regge l'intero impianto normativo e caratterizza, dall'inizio alla fine, il processo delle firme elettroniche. Non solo, la sicurezza riguarda tutta l'infrastruttura della comunicazione e delle transazioni economiche[115]. Da qui l'esigenza che sistemi come quello di PKY, dove i prestatori di certificazione delle firme elettroniche forniscono chiave privata e pubblica, garantiscano un elevato livello di sicurezza. Tuttavia, è altresì cruciale, ad esempio, che il firmatario possa mantenere un esclusivo controllo sui dati utilizzati per la creazione della firma elettronica. In questo scenario, dove l'interesse a tutelare la sicurezza potrebbe porsi in conflitto con quello di protezione dei dati personali, occorre operare un bilanciamento.

In Cina, tale operazione risulta alquanto problematica dal momento che, diversamente da quanto accade nell'Unione europea, la legge cinese sulle firme elettroniche non fa alcun espresso rinvio alla normativa a tutela dei dati personali. Solamente la legge sulla tutela dei diritti dei consumatori della Repubblica Popolare della Cina stabilisce[116] che «l'operatore della piattaforma non può divulgare né vendere i dati personali dei consumatori e deve adottare misure tecniche per impedire la divulgazione o la perdita delle informazioni personali del consumatore"[117]. La stessa legge, però, non prevede disposizioni specifiche relative all'attribuzione di responsabilità al prestatore di servizi[118].

Alla luce del quadro delineato, emerge una differenza, anche culturale, tra il contesto normativo europeo e quello cinese. In Europa, vi è una consolidata disciplina a tutela dei consumatori, sintetizzabile nell'espressione "circolazione sicura dei dati". Al contrario, in Cina, il meccanismo di tutela è stato appena costruito e necessita di un collaudo giurisprudenziale. Per questo motivo appare utile, soprattutto in ottica comparata, formulare alcune considerazioni sul sistema giudiziario cinese, il quale presenta alcune sostanziali differenze con quello italiano. L'analisi comparata dei due sistemi infatti mette in luce l'esistenza di una radicale differenza. In Italia, il processo giudiziario è lento e fondato su un rito processuale ormai consolidato, in cui la "nuova" norma

---

114 Considerando 18 della direttiva 99/93/CE.

115 Si noti come nei servizi di *E-government*, i governi designano le aziende preposte alla ricerca e allo sviluppo di prodotti sicuri nell'ambito del sistema crittografico a chiave pubblica, e confidano nella affidabilità della firma elettronica da questi fornita (ad esempio, in Cina, l E-sign).

116 "中华人民共和国消费者权益保护法" 第二十九条 经营者收集、使用消费者个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意。经营者收集、使用消费者个人信息，应当公开其收集、使用规则，不得违反法律、法规的规定和双方的约定收集、使用信息。

经营者及其工作人员对收集的消费者个人信息必须严格保密，不得泄露、出售或者非法向他人提供。经营者应当采取技术措施和其他必要措施，确保信息安全，防止消费者个人信息泄露、丢失。在发生或者可能发生信息泄露、丢失的情况时，应当立即采取补救措施。

经营者未经消费者同意或者请求，或者消费者明确表示拒绝的，不得向其发送商业性信息。

117 Art. 29 della legge cinese sulla tutela dei diritti dei consumatori.

118 Si noti tuttavia che tale vuoto normativo viene colmato dalla legge cinese sul commercio elettronico con gli artt. 23, 25, 32, 79 e 87.

deve armonizzarsi con l'ordinamento giuridico esistente. In Cina, invece, il processo è improntato all'innovazione ed è rimesso alla valutazione del giudice speciale: l'intero impianto giuridico sembra doversi adeguare alla legge cinese sulle firme elettroniche eretta sulla base dell'architettura delineata dal modello UNCITRAL e non il contrario. Il principio del giudice naturale, tutelato dalla Costituzione italiana[119], si contrappone all'istituzione del giudice cinese nato nel 2017 per la giurisdizione delle controversie *online*. Considerando che i rapporti negoziali *online* sono destinati a crescere, ci si domanda se il tribunale "ordinario" cinese sia contestualmente destinato a scomparire, sostituito dalla Corte di Internet.

In conclusione, le questioni di cui si è dato conto nel presente contributo sembrano potersi ricondurre al tema della sovranità. Un tempo l'uomo era sovrano della propria mano, la mano esprimeva la sovranità dell'uomo capace di agire. Oggi, l'impianto giuridico sulle firme elettroniche riflette una separazione tra la mano e il corpo, creando un surrogato tecnologico che assicura il coordinamento tra la mano e la mente. Nel momento in cui la legge vieta al prestatore di servizi di firma elettronica qualificata di copiare la chiave privata, ammette la possibilità che quest'ultimo la copi. La mano che non si stacca dal corpo è la vera e unica garanzia della propria sovranità, mentre la garanzia del surrogato tecnologico è imposta dal legislatore che deve misurarsi con il potere tecnologico esercitando il potere coercitivo sanzionatorio. A tale proposito, emerge una certa debolezza del legislatore cinese. Il *vulnus,* creato dall'adozione da parte del legislatore italiano dello strumento cognitivo del modello e della metafora per la disciplina delle firme informatiche, si palesa nell'inapplicabilità dell'istituto ideato per la tutela della firma autografa. Le firme informatiche non sono come la firma autografa, proprio in ragione della progressiva perdita della sovranità dei titolari di queste firme. Questi sono trascinati nel mondo virtuale dove la firma si compone di numeri, codici, segni irriconoscibili e dove spesso il sottoscrittore perde consapevolezza dell'atto stesso della firma. Una firma autografa è riconoscibile dal suo autore che, in caso di falsificazione della firma, può avvalersi dell'istituto del disconoscimento. L'onere di presentare l'istanza di verificazione e produrre le prove grava sulla parte che intende fare valere la firma. In mancanza di tale istanza oppure di esito positivo, il documento firmato non può essere utilizzato nel processo. Diversamente, per le firme informatiche, non potendo essere riconosciute ad occhio nudo dai propri titolari, non è possibile ricorrere all'istituto della verificazione di cui all'art. 216 c.p.c. Per ovviare a tale problema è stata introdotta la presunzione, ai sensi dell'art. 20, c. 1-*ter*, CAD, dell'utilizzo del dispositivo in capo al titolare del medesimo. Tuttavia, ciò comporta un aggravamento dell'onere della prova in capo al titolare del dispositivo di firma (si pensi, ad esempio, al caso di furto o di smarrimento di questo).

In Cina, gli effetti giuridici delle firme elettroniche sono riconosciuti in via automatica in presenza dei requisiti previsti dalla legge e, di fronte allo strapotere dei prestatori delle firme elettroniche, ci si domanda quale sia il mezzo di cui potrebbe disporre il titolare del dispositivo nell'ipotesi di copia della chiave privata, oppure di creazione o manomissione di prova da parte del certificatore. L'evoluzione del diritto civile attorno

[119] Art. 25, c. 1, Costituzione italiana: «Nessuno può essere distolto dal giudice naturale precostituito per legge».

al principio cardine della circolazione di beni permette che questi circolino inarrestabilmente ad un ritmo sempre più veloce. Contemporaneamente, l'uomo accetta – spesso inconsapevolmente – di perdere la propria sovranità, travolto dalla crescita esponenziale dei prodotti della potente macchina dei *Big Data* e dell'intelligenza artificiale. L'uomo alimenta la macchina immettendovi i propri dati, finendo però per essere privato dalla stessa della propria indipendenza e della propria dignità. Le informazioni che, mai come oggi, l'uomo concede volontariamente (o meno) ai *service provider*, fanno sorgere sempre più robot di intelligenza artificiale, che torneranno a spogliarlo fino all'ultimo velo della sua essenza.