Luglio 2020

Firma elettronica avanzata ed "onboarding" della clientela bancaria nel decreto semplificazioni

Massimiliano Nicotra, Senior Partner, Qubit Law Firm

Il recente decreto semplificazioni (decreto legge 16 luglio 2020 n. 76 pubblicato sulla G.U. n. 178) contiene all'art. 27 rubricato "Misure per la semplificazione e la diffusione della firma elettronica avanzata e dell'identità digitale per l'accesso ai servizi bancari" alcune specifiche previsioni volte a semplificare per banche, istituti di pagamento ed altri intermediari bancari e finanziari, gli adempimenti relativi alla stipulazione dei contratti per l'erogazione dei prodotti e servizi nonché all'identificazione della clientela con riferimento, in particolare, alle operazioni che vengono condotte on-line o in multicanalità.

Al fine di comprendere la portata di tali previsioni appare utile illustrare brevemente l'attuale disciplina normativa applicabile, così da poter meglio apprezzare le modifiche apportate dal decreto legge.

Com'è noto l'art. 117 del Testo Unico Bancario richiede, in via generale, la forma scritta per la stipulazione dei contratti tra banche e clienti, requisito ribadito dall'art. 120 *noviesdecies* relativo al credito immobiliare ai consumatori, dall'art. 125 bis inerente al credito al consumo, dall'art. 126 *quinquies* per i contratti quadro relativi ai servizi di pagamento e dall'art. 126 *quinquiesdescies* per la forma dell'autorizzazione del trasferimento tra i conti di pagamento.

Il provvedimento del 29 luglio 2009 della Banca d'Italia in materia di "Trasparenza delle operazioni e dei servizi bancari e finanziari", come da ultimo modificato in seguito al recepimento della direttiva 2014/92 UE (PAD), prescrive in ciascuna delle sezioni in cui vengono rispettivamente trattate le disposizioni sopra richiamate che "*il documento informatico soddisfa i requisiti della forma scritta nei casi previsti dalla legge*" e che "*l'idoneità del documento informatico a soddisfare il requisito della forma scritta è disciplinata dagli articoli 20 e 21 del decreto legislativo 7 marzo 2005, n. 82*".

Il mancato rispetto della forma scritta determina la nullità del contratto, la quale può essere fatta valere solo dal cliente.

Le disposizioni così richiamate del d.l.vo n. 82/2005, cd. Codice dell'Amministrazione Digitale (di seguito "CAD") - che durante gli anni ha subito numerose modifiche anche in conseguenza dell'entrata in vigore del Regolamento (UE) n. 910/2014 (cd. eIDAS) - stabiliscono i requisiti di validità ed efficacia del documento informatico e devono essere lette anche alla luce del DPCM 13 novembre 2014 in materia di "*Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonche' di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005*", nonché del DPCM 22 febbraio 2013 che reca regole tecniche per la generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ed, infine, degli ulteriori provvedimenti adottati dall'Agenzia per l'Italia Digitale (AgID).

L'attuale disciplina del documento informatico, dettata in particolare dall'art. 20 del CAD, prevede che il medesimo soddisfa il requisito della forma scritta ed ha l'efficacia dell'art. 2702 del codice civile quando:

- vi è apposta:
  - una firma digitale;
  - una firma elettronica qualificata;
  - una firma elettronica avanzata;
- oppure se formato previa identificazione informatica del suo autore attraverso un processo individuato da AgID che renda inequivoca e manifesta la riconducibilità del documento all'autore e tale comunque da garantire i requisiti di sicurezza, integrità ed immodificabilità del documento stesso.

La disposizione determina direttamente il requisito di validità ed efficacia del documento informatico, non lasciando quindi spazi di interpretazione a coloro che ne devono valutare la conformità rispetto alle eventuali prescrizioni normative.

In tutte le altre ipotesi, ossia qualora non venga utilizzato uno degli strumenti sopra indicati, l'idoneità del documento a soddisfare il requisito della forma scritta ed il suo valore probatorio è liberamente valutabile dal giudice, tenuto conto delle caratteristiche di sicurezza, integrità ed immodificabilità che la tecnologia utilizzata conferisce al documento informatico stesso.

Per terminare questa breve disamina introduttiva appaiono necessarie alcune ulteriori precisazioni.

Le firme elettroniche qualificate, di cui la firma digitale costituisce un sottoinsieme caratterizzato dall'adozione di un meccanismo di cifratura a chiavi asimmetriche, fondano la loro sicurezza su una struttura pubblica di certificazione, al cui vertice è posta l'Autorità di controllo, che vigila sui prestatori di servizi fiduciari, i quali provvedono a rilasciare i certificati elettronici qualificati con cui vengono identificati i titolari delle chiavi di sottoscrizione accertandosi altresì del rispetto dei requisiti di sicurezza dei dispositivi utilizzati per l'apposizione delle sottoscrizioni sui documenti informatici.

Le firme elettroniche avanzate, d'altro canto, disciplinate dall'art. 26 del Regolamento eIDAS, possono essere basate su requisiti di sicurezza differenti e, soprattutto, non è richiesto alcun provvedimento autorizzatorio preventivo per la loro realizzazione né che siano predisposte necessariamente da un un prestatore di servizi fiduciari potendo essere erogate anche direttamente da coloro che intrattengono il rapporto giuridico con la propria controparte contrattuale.

Infine, con riferimento all'ulteriore processo di formazione idoneo a soddisfare il requisito della forma scritta di cui all'art. 20, comma 1 bis, del CAD, è opportuno evidenziare che recentemente l'Agenzia per l'Italia Digitale ha adottato la determinazione n. 157/2020 con cui sono state emanate le Linee Guida che disciplinano la possibilità di utilizzare una particolare procedura, avvalendosi di SPID e dei sigilli elettronici qualificati (i cd. QSeal), per la creazione di un documento informatico attribuibile al soggetto identificato tramite il sistema di identità digitale.

Le semplificazioni per il rilascio della firma elettronica avanzata (art. 27, commi 1° e 2° d.l. 76/2020)

Definito il contesto delle norme che disciplinano la stipulazione dei contratti degli operatori bancari e degli strumenti che la normativa attuale fornisce per l'imputazione della paternità dei documenti informatici, è possibile esaminare la portata delle nuove disposizioni di semplificazione adottate con il d.l. n. 76/2020.

Secondo l'art. 57 del DPCM 22 febbraio 2013 il soggetto che eroga un servizio di firma elettronica avanzata ha l'obbligo "*a) identificare in modo certo l'utente tramite un valido documento di riconoscimento, informarlo in merito agli esatti termini e condizioni relative all'uso del servizio, compresa ogni eventuale limitazione dell'uso, subordinare l'attivazione del servizio alla sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente*".

In base a tale disposizione l'identificazione del soggetto a cui è rilasciata una firma elettronica avanzata deve avvenire necessariamente tramite l'acquisizione di un documento di riconoscimento e l'attivazione del servizio richiede la necessaria accettazione da parte dell'utente dei termini e condizioni di servizio.

E' evidente che, nell'ambito dei servizi erogati online, la necessità di ottenere una copia dei documenti di identità può essere di ostacolo alla speditezza del processo di rilascio

della firma elettronica avanzata, soprattutto in considerazione del fatto che in alcuni casi l'utente è già cliente dell'operatore ed è dotato di strumenti che consentono di identificarlo univocamente.

In tal senso, il primo comma della disposizione in esame individua i seguenti processi alternativi con cui è possibile identificare un utente ai fini del rilascio della firma elettronica avanzata.

Identificazione tramite credenziali di strong authentication

La prima modalità di identificazione riguarda la possibilità di identificare l'utente tramite una procedura elettronica basata su credenziali conformi al Regolamento delegato (UE) 2018/389 della Commissione, di cui il medesimo sia stato già munito dal soggetto che eroga il servizio di firma elettronica avanzata.

In sintesi l'utente, già identificato dall'operatore ai sensi del dl.vo n. 231/2007 e munito di credenziali di strong authentication, potrà essere identificato ai fini del rilascio di una firma elettronica direttamente tramite l'utilizzo di dette credenziali, così potendo procedere all'accettazione dei termini e condizioni d'uso e stipulare i contratti con l'operatore utilizzando tale firma elettronica avanzata.

L'ambito di applicazione della semplificazione attiene ai rapporti tra la banca o, in generale, l'operatore bancario, ed i suoi clienti ai quali siano state previamente rilasciate credenziali forti di autenticazione per l'accesso ai servizi o il compimento di operazioni.

Identificazione tramite SPID

La lettera b) del 1° comma dell'art. 27 prevede la possibilità di identificare l'utente che richiede una firma elettronica avanzata tramite il Sistema Pubblico d'Identità Digitale (SPID) di cui all'art. 64 del CAD.

La portata innovativa della disposizione risiede nel porre quale requisito per la valida identificazione informatica dell'utente un livello di sicurezza delle credenziali SPID pari al secondo, ossia basato su due fattori.

Occorre sottolineare, infatti, che la previsione del d.l.vo n. 231/2007 (art. 19, 1° comma, lett. a) n. 2)) antecedente alla modifica apportata dal decreto legge in commento, richiedeva l'utilizzo di un'identità digitale del "livello massimo di sicurezza", con ciò rendendo praticamente inutilizzabili a tali fini le credenziali SPID più ampiamente diffuse in Italia, che sono invece basate sul secondo livello.

In considerazione di ciò la norma, in combinato disposto con le ulteriori semplificazioni in materia di identificazione della clientela introdotte dal terzo comma della stessa, è in grado di avere un forte impatto sui processi di onboarding online della clientela da parte degli intermediari.

L'applicazione, infatti, non è limitata a coloro che siano già clienti dell'intermediario, trovando applicazione per qualsiasi utente che sia dotato di SPID e che intenda instaurare un rapporto con l'operatore. Inoltre, consentendo il rilascio di una firma elettronica avanzata al soggetto identificato con tale modalità si semplificano i processi di stipulazione dei contratti dato che, successivamente alla prima fase di riconoscimento dell'utente tramite SPID, si potrà procedere senza soluzione di continuità alla sottoscrizione del contratto che disciplina il singolo rapporto (o il contratto quadro in caso di servizi di pagamento) con uno strumento idoneo a soddisfare il requisito della forma scritta richiesto dalle norme del Testo Unico Bancario citate in apertura del presente scritto.

Identificazione tramite CIE e sistemi di identificazione notificati

Il terzo comma estende la possibilità di identificare gli utenti utilizzando sistemi di identificazione informatica basati su credenziali di livello almeno significativo, nell'ambito di quei sistemi di notificazione notificati in sede europea con esito positivo.

Tale ulteriore previsione estende le considerazioni già svolte in merito all'utilizzo di SPID a tutti i sistemi di identificazione che siano stati notificati alla Commissione Europea, secondo la procedura stabilita dall'art. 9 del Regolamento eIDAS, basati su credenziali di livello almeno "significativo", corrispondente al secondo livello del Sistema Pubblico di Identità Digitale. In forza di tale disposizione si potrà procedere all'identificazione dell'utente anche attraverso identità digitali eventualmente rilasciate in altri Stati membri dell'Unione Europea[1]. Sarà inoltre possibile rilasciare una firma elettronica avanzata riconoscendo l'utente attraverso un'identificazione informatica a mezzo di una Carta d'Identità Elettronica, la quale, è opportuno ricordarlo, costituisce l'ulteriore sistema di identità digitale - con livello di sicurezza "avanzato" - già notificato dall'Italia in Commissione Europea.

Il 2° comma dell'art. 27, precisa che in caso di riconoscimento dell'utente con una delle modalità indicate al 1° comma sarà necessario che il soggetto erogatore del servizio conservi per almeno 20 anni "*le evidenze informatiche del processo di autenticazione*" in base a cui è stata rilasciata la firma elettronica avanzata, così sostituendo in tali ipotesi l'obbligo di conservazione del documento di riconoscimento stabilito all'art. 57, comma 1, lett. b), del DPCM 22 febbraio 2013.

Le semplificazioni in materia di identificazione a distanza della clientela

Il 3° comma dell'art. 27 introduce alcune modifiche sulle modalità di identificazione della clientela ai fini della disciplina in materia di prevenzione dell'uso del sistema finanziario

[1] L'elenco dei sistemi notificati e dei livelli di sicurezza garantita è disponibile nel sito della Commissione Europea al link https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS?replyToComment=62885725&#comment-62885725

a fini di riciclaggio o finanziamento del terrorismo (d.l.vo n. 231/2007 come modificato dalle disposizioni di recepimento delle direttive IV e V AML).

L'identificazione del cliente è notoriamente un obbligo che grava su tutti gli operatori ed intermediari bancari e che incide, pertanto, nella definizione del processo di onboarding della clientela quando effettuato con modalità telematiche.

La prima sostanziale modifica riguarda **la soppressione dell'obbligo di acquisizione di un documento identificativo del cliente**, così evitando la trasmissione online di copia dei documenti e lasciando l'operatore libero di effettuare il riscontro dell'identità del cliente tramite fonti affidabili ed indipendenti.

La lett. c) del comma 3° contiene a sua volta rilevanti modifiche della disciplina per l'identificazione a distanza della clientela, allineando così le modalità di riconoscimento agli strumenti più diffusi sul territorio nazionale ed anche ai sistemi introdotti in seguito all'evoluzione dei servizi basati sul Regolamento eIDAS.

Come già innanzi accennato, l'art. 19 del d.l. n. 231/2007, comma 1, lett. a) n. 2) consentiva di ritenere assolto l'obbligo di riconoscimento anche senza la presenza fisica del cliente qualora l'identità fosse stata riscontrata tramite un'identità digitale SPID di livello massimo di sicurezza, o tramite un'identità digitale o un certificato per la generazione di una firma digitale rilasciati nell'ambito di un sistema di identificazione elettronica notificato ai sensi dell'art. 9 del Regolamento eIDAS.

Le difficoltà applicative derivanti dalla formulazione di detta previsione erano di due ordini: innanzitutto, come chiarito, la scarsa diffusione di credenziali SPID con livello massimo di sicurezza, dato che la quasi totalità delle identità digitali rilasciate in Italia (ad oggi oltre 8 milioni) utilizzano un livello di sicurezza significativo e non elevato.

Inoltre, la seconda parte della disposizione appariva mal formulata, sia in quanto la firma digitale è definita solo in Italia come particolare tipologia di firma elettronica qualificata sia perchè essa non rientra nei sistemi di identificazione digitale notificati ex art. 9 del Regolamento eIDAS, ma è autonomamente disciplinata dal medesimo regolamento quale servizio fiduciario.

Con la lett. c), n. 1) del 3° comma in esame si interviene quindi sull'art. 19, comma 1, lett. a) n. 2) del d.l.vo n. 231/2007, prevedendo la possibilità di soddisfare gli obblighi di identificazione previsti dalla disciplina cd. antiriclaggio attraverso:

- un'identità digitale SPID di cui all'art. 64 del CAD di livello almeno significativo;
- un'identità digitale sempre di livello almeno significativo, rilasciata nell'ambito dei servizi di identificazione elettronica nazionali di cui all'art. 9 del Regolamento eIDAS, tra cui la Carta d'Identità Elettronica;
- un certificato per la generazione di una firma elettronica qualificata;

- una procedura di identificazione elettronica sicura e regolamentata ovvero autorizzata o riconosciuta dall'Agenzia per l'Italia Digitale.

L'operatore, pertanto, in seguito alla semplificazione apportata dalla norma in commento, potrà procedere con tali strumenti all'identificazione del cliente utilizzando le numerose identità digitali SPID già diffuse sul territorio o certificati qualificati associati alle firme elettroniche con cui possono essere sottoscritti i contratti (strumenti che consentono di soddisfare la forma scritta ex art. 20, comma 1-bis, CAD).

A parere di chi scrive, inoltre, appare rilevante l'ulteriore possibilità di individuare procedure di identificazione sicure e regolamentate. In tal senso l'ultimo periodo della disposizione prevede due tipologie di procedure: quelle "*autorizzate o riconosciute dall'Agenzia per l'italia Digitale*" ovvero, con formulazione disgiuntiva, quelle "*sicure e regolamentate*". Tali ultime procedure potrebbero essere individuate dalla Banca d'Italia, attraverso le disposizioni di adeguata verifica della clientela - da ultimo aggiornate con provvedimento del 30 luglio 2019 - o da organismi sovranazionali nell'ambito dell'attuazione dei provvedimenti europei, consentendo quindi un'applicazione della norma in linea con l'evoluzione della tecnologia.

Infine, una particolare semplificazione è stabilita per i rapporti relativi alle carte di pagamento e dispositivi analoghi, nonché strumenti di pagamento basati su servizi di telecomunicazione, digitali o informatici (con esclusione dei casi in cui tali carte, dispositivi o strumenti sono utilizzabili per generare l'informazione necessaria a effettuare direttamente un bonifico o un addebito diretto verso e da un conto di pagamento).

L'art. 27, 3° comma, lett. c), n. 2) prevede che l'obbligo di riconoscimento ai fini antiriciclaggio potrà essere assolto per tali servizi tramite un bonifico bancario da parte degli utenti verso un conto di pagamento intestato al soggetto tenuto al riconoscimento, purchè gli utenti si siano identificati tramite credenziali di strong authentication conformi ai requisiti dell'art. 4 del Regolamento delegato (UE) 2018/389.

Considerazioni conclusive

Le disposizioni esaminate ed introdotte al fine di semplificare l'accesso ai servizi bancari tramite un più ampio utilizzo degli strumenti più diffusi sul territorio italiano (come SPID) e di quelli di più semplice attivazione, quali le firme elettroniche avanzate, potranno sicuramente portare dei benefici in termini di speditezza e sicurezza delle procedure di onboarding online della clientela da parte degli operatori bancari e degli intermediari.

Per consentire un più ampio utilizzo degli stessi sarebbe però necessario che in sede di conversione vengano chiariti alcuni ulteriori limiti dell'attuale normativa, soprattutto in tema di firme elettroniche avanzate, ancora cristallizzata alla formulazione del 2013.

Il primo è relativo alla presunzione di utilizzo del dispositivo da parte del titolare di firma elettronica, stabilita dall'art. 1-ter unicamente per la firma elettronica qualificata o digitale. La presunzione determina processualmente un'inversione dell'onere della prova in base alla quale colui che risulta firmatario di un documento informatico, in caso di firma digitale o qualificata, non può limitarsi a contestare l'utilizzo del dispositivo, ma deve fornire prova che detto utilizzo non sia a lui riconducibile (e quindi, stante gli obblighi di custodia su di lui gravanti, che sia stato fraudolentemente utilizzato a sua insaputa).

Tale meccanismo non opera per la firma elettronica avanzata, molto probabilmente per ragioni storiche legate alle principali soluzioni tecnologiche esistenti al momento in cui furono introdotte tali disposizioni (periodo in cui il concetto di firma elettronica avanzata il più delle volte coincideva con quello di firma grafometrica).

L'assenza della presunzione per la firma elettronica avanzata rende in realtà più agevole il disconoscimento di un documento informatico da parte di colui che ne risulti firmatario, in quanto la prova dell'utilizzo del dispositivo, e quindi dell'apposizione della firma elettronica avanzata e della sua riconducibilità al titolare, dovrà essere resa dal soggetto che intende avvalersi del documento stesso.

Tale differente regime processuale non sembra avere più alcuna giustificazione in seguito all'entrata in vigore del Regolamento eIDAS, in quanto l'art. 26, 1° comma lett. c) stabilisce, tra i requisiti che una firma elettronica avanzata deve soddisfare, quello di essere creata con strumenti che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo. E' proprio il controllo esclusivo dello strumento, quindi, che caratterizza la firma elettronica avanzata e non appare quindi essere ulteriormente giustificabile la così ampia possibilità di contestarne l'uso da parte di colui che ne risulta titolare, gravando la controparte che fa affidamento sulla validità del contratto intercorso dell'onere di dover provarne l'utilizzo effettivo.

Infine, un ulteriore limite al più ampio utilizzo della firma elettronica avanzata nell'ambito dei contratti stipulati dagli operatori bancari e dagli intermediari è costituito dall'art. 60 del DPCM 22 febbraio 2013.

La norma stabilisce che la firma elettronica avanzata è utilizzabile limitatamente ai rapporti giuridici intercorrenti tra il sottoscrittore e il soggetto di cui all'art. 55, comma 2, lettera a), ossia a colui che eroga la soluzione per motivi istituzionali, societari o commerciali.

Ebbene, anche tale limitazione sembra non aver più molto senso nel nostro ordinamento, in quanto motivata ai tempi della sua introduzione da motivazioni prettamente tecnologiche (relative, principalmente, alla mancanza di interoperabilità tra le varie soluzioni).

E’ noto infatti che, soprattutto nel contesto dei gruppi bancari, i servizi tecnologici vengono erogati da una delle società del gruppo ed utilizzati poi dalle altre società nell’ambito dell’erogazione dei propri servizi. In alcuni casi, inoltre, l’intermediario colloca prodotti o servizi di altri soggetti (soluzioni assicurative, carte di pagamento, etc.) ed i contratti intercorrono direttamente tra il cliente della banca ed il soggetto terzo. In forza della limitazione contenuta nell’art. 60 del DPCM 23 febbraio 2013 non sarebbe possibile utilizzare, ai fini della stipulazione del contratto, una soluzione di firma elettronica avanzata erogata dalla banca, in quanto la stessa non risulterebbe essere parte del rapporto giuridico da instaurare.

Nel solco della volontà di semplificazione e di maggior diffusione degli strumenti digitali per l’accesso ai servizi bancari, sarebbe pertanto opportuno eliminare anche tale limitazione, la quale non ha più ragione di esistere non essendo più attuali quei limiti tecnologici originali, consentendo al soggetto erogatore di far utilizzare una firma elettronica avanzata non solo per i rapporti di cui è direttamente parte, ma anche per quelli instaurati nell’ambito del gruppo di societario di appartenenza ovvero dei quali venga promossa, in fase precontrattuale, la stipulazione verso propri clienti anche se intercorrenti poi con un soggetto diverso.