Il Delegato

Londra, 12 maggio 2020

Prot. 26
Fasc. H.1

Oggetto: la creazione di una *open data platform* per facilitare l'accesso al credito da parte delle PMI.[1]

***Sintesi**:* A seguito della pubblicazione del rapporto "Future of Finance", la Bank of England ha identificato cinque obiettivi prioritari per favorire lo sviluppo dell'industria finanziaria britannica, nell'ottica di svolgere un ruolo di *leadership* globale nella creazione di nuovi *standard* nell'ambito dello sviluppo tecnologico. In particolare, la creazione di una *open platform* per facilitare l'accesso al credito da parte delle PMI rappresenta una importante opportunità per risolvere gli squilibri di crescita delle PMI britanniche e permetterne uno sviluppo equilibrato e al passo coi tempi. Nel Regno Unito vi sono 5,9 milioni di PMI. Esse impiegano il 60% della forza lavoro del settore privato e contribuiscono al 50% del PIL nazionale. Al momento molte PMI incontrano difficoltà nell'accedere al credito di cui hanno bisogno e si calcola che esista un *funding gap* pari a 22 miliardi di sterline. I dati a disposizione dimostrano che nel Regno Unito solo il 36% delle PMI fa uso di finanziamenti esterni. Il modello presentato nel documento "Open data for SME finance" propone un sistema basato su una rete decentralizzata di data *providers* che utilizzano una serie standardizzata di APIs per mettere a disposizione i dati all'interno del sistema finanziario in tempo reale, a richiesta delle PMI stesse. L'esperienza internazionale dimostra come un ruolo propositivo da parte delle autorità centrali, legato a un corretto utilizzo dell'identità digitale e nel rispetto della tutela della *privacy*, possa consentire un rapido sviluppo di quella *data portability* necessaria ad implementare un sistema in grado di aprire nuovi orizzonti.

La Bank of England (BoE) prosegue l'articolazione della propria visione strategica sul futuro dell'industria finanziaria attraverso la pubblicazione di un nuovo documento "***Open data for SME finance***"[2], che fa il punto della situazione e detta le linee guida per la creazione di una *open data platform* al fine di facilitare l'accesso al credito da parte delle PMI. Inoltre, questo documento costituisce uno degli *input* su cui si concentrerà il lavoro

[1] A cura di Riccardo Tordera.
[2] https://www.bankofengland.co.uk/paper/2020/open-data-for-sme-finance (Marzo 2020).

della Smart Data Review del governo e costituirà uno dei punti di partenza della Digital Markets Taskforce (la cui creazione è stata annunciata dal Budget 2020), nonché dell'iniziativa Open Finance della Financial Conduct Authority (FCA).

Come già riferito da questa Delegazione con l'appunto 20/H.1 del 14 aprile u.s. "L'approccio della BoE e dell'FCA per strutturare la raccolta dei dati e la digitalizzazione dell'attività di *reporting*", nel mese di giugno 2019 la BoE ha pubblicato una risposta al rapporto "Future of Finance"[3] dal titolo "New economy, new finance, new Bank"[4] in cui, partendo dai suggerimenti indicati nel rapporto stesso, ha indicato cinque obiettivi da perseguire:

1. Favorire lo sviluppo di un migliore sistema dei pagamenti.
2. Sostenere la creazione di una *open platform* per facilitare l'accesso al credito delle PMI.
3. Favorire la transizione a una *carbon-neutral economy*.
4. Realizzare una *world-class regtech* e una *data strategy*.
5. Migliorare la *resilience* del sistema finanziario tramite l'adozione del *cloud* e di altre tecnologie.

Questo appunto vuole esporre come la BoE stia agendo nell'ambito del secondo dei cinque obiettivi sopra elencati, nell'intento di colmare il *funding gap* di 22 miliardi di sterline che le PMI britanniche si trovano a fronteggiare, come esplicitato nel documento sopra menzionato.

Il *funding gap* e la situazione delle PMI nel Regno Unito

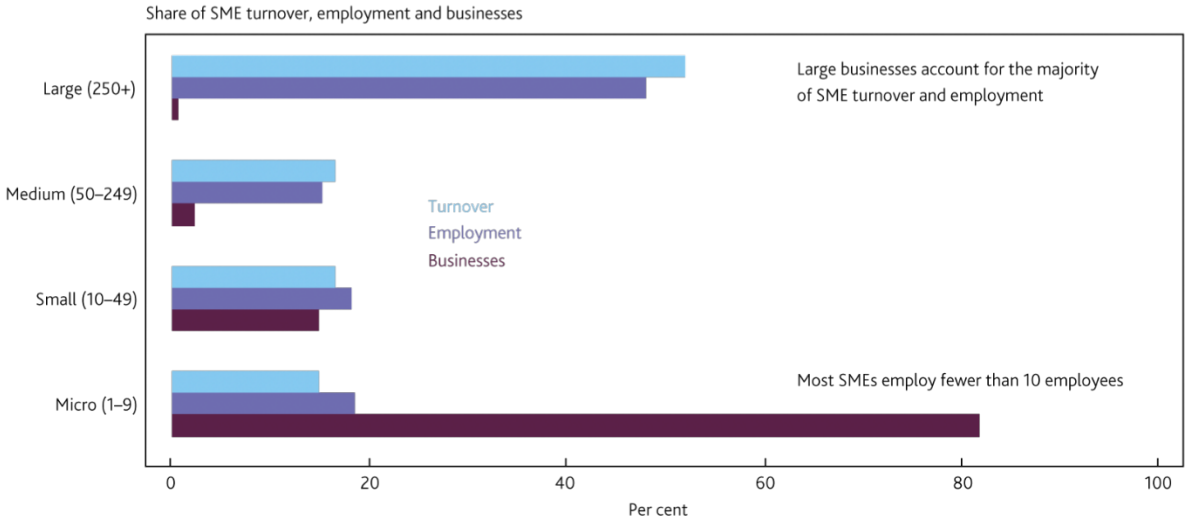
La natura mutevole del commercio e le innovazioni tecnologiche che stanno cambiando l'economia richiedono una maggiore attenzione alla gestione dei dati, che vengono continuamenti generati dal sempre crescente utilizzo di piattaforme *online* e dal commercio digitale. Proprio le piattaforme *online*, alla base della diffusione della c.d. *sharing economy*, hanno portato a un sempre più visibile declino dell'*asset ownership*, riducendo la capacità di determinati gruppi di accedere ad alcuni servizi finanziari, quali ad esempio il *secured lending*, vista l'impossibilità di fornire i collaterali necessari. Un'economia sempre più *capital light*, flessibile e dinamica comporta che il sistema finanziario dipenda maggiormente da *asset* di natura intangibile.

[3] Il rapporto "*Future of Finance*", commissionato nel 2018 dall'ex governatore Carney al consulente esterno Huw van Steenis e presentato nel giugno 2019, identifica le forze propulsive dei cambiamenti in atto nell'economia, le conseguenze di questi mutamenti per il sistema finanziario e le linee direttrici secondo le quali la BoE dovrebbe agire al fine di (i) favorire l'innovazione nella *financial infrastructure*, (ii) l'adozione di *standard* adeguati a livello sia nazionale che globale, (iii) guidare la transizione ad una *low-carbon economy,* (iv) proteggere il sistema finanziario dal *cyber risk* e infine (v) adottare una regolamentazione digitale.
[4] https://www.bankofengland.co.uk/-/media/boe/files/report/2019/response-to-the-future-of-finance-report.pdf

La digitalizzazione dell'economia sta inoltre producendo notevoli cambiamenti nel mercato del lavoro. Nel 2019, un lavoratore britannico su dieci ha lavorato nella c.d. *gig economy* ed uno su sei è *self-employed*. Questo comporta che il lavoratore che fa utilizzo di piattaforme *online* abbia un reddito variabile, di fatto diventando meno appetibile per il creditore tradizionale, a fronte di una minore capacità di offrire le usuali garanzie. Di conseguenza, forme di credito alternative vanno sempre più diffondendosi. Nel 2017, ad esempio, il *peer-to-peer lending* (P2P) ha visto un incremento del 10% rispetto all'anno precedente. A livello globale, il *fintech* si sta mostrando capace di offrire soluzioni nuove in grado di garantire un maggiore sviluppo della *financial inclusion*, rendendo possibile l'accesso al credito a quei settori dell'economia che ne sono rimasti esclusi.

Nel Regno Unito vi sono 5,9 milioni di PMI. Esse impiegano il 60% della forza lavoro del settore privato e contribuiscono al 50% del PIL nazionale. Le PMI britanniche costituiscono un gruppo eterogeneo: se per definizione le PMI del Regno Unito sono quelle imprese private che hanno meno di 250 dipendenti e un fatturato annuo inferiore a 25 milioni di sterline, in realtà la maggioranza di esse ha meno di 10 dipendenti. Nel loro insieme queste piccole imprese rappresentano il 19% dell'occupazione complessiva del settore ed il 15% del fatturato totale, con forti squilibri di distribuzione regionale tra Londra e il ricco sud ovest e le altre zone del paese (cfr. Figura 1).

Figura 1: SMEs are a heterogeneous group.



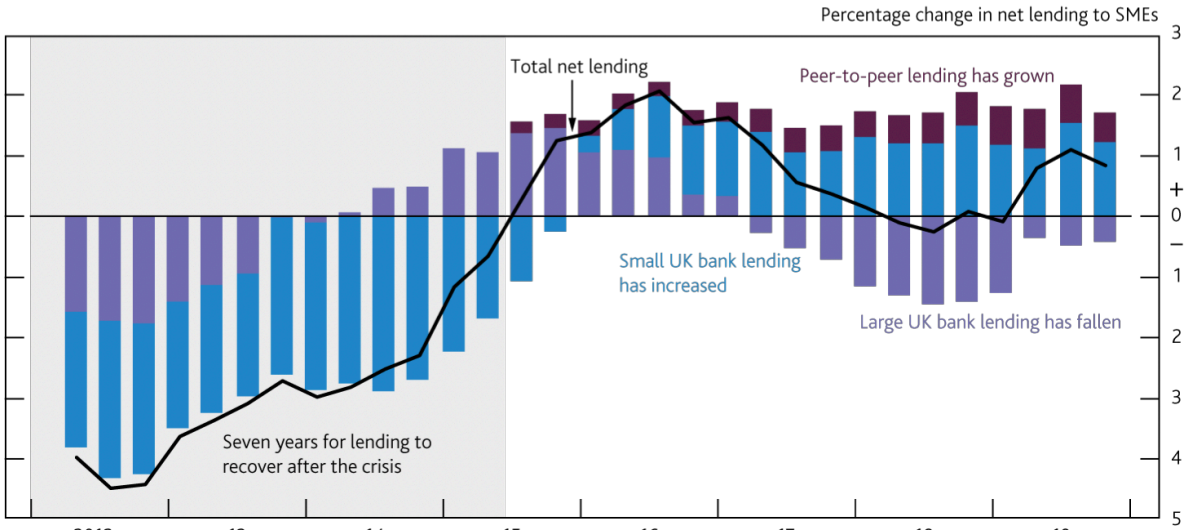
Source: BEIS, Business population (2018)

Al di là delle differenze nella distribuzione territoriale, studi e ricerche hanno dimostrato come altre diversità emergano a livello geografico nell'accesso al credito. Aree quali Londra, Sud-Est, Nord-Ovest, Yorkshire-Humber e le Midlands Orientali offrono minori possibilità di ottenere prestiti. Tuttavia, a Londra, la minore disponibilità di prestiti tradizionali viene sopperita dall'accesso all'*equity finance*, ciò che non vale per le altre regioni. Nonostante la notevole diversità delle varie forme di accesso al credito, sia a livello geografico che strutturale, si può comunque affermare che, a livello aggregato, il credito

bancario costituisca l'85% dello *stock* di debito delle PMI[5]. Tuttavia, la crisi finanziaria ha fatto emergere disfunzionalità che ancora incidono sulla struttura del sistema, testimoniate dal lungo periodo di tempo - sette anni – perché il *lending* a favore delle PMI tornasse ai livelli pre-crisi.

Come mostrato dal grafico sottostante (cfr. Figura 2), dal 2017 la crescita netta del finanziamento alle PMI proviene dalle banche più piccole o da forme alternative di finanziamento quali il P2P. Questo dimostra l'importanza che la diversità dei prestatori, a fronte della diversità dei *business model*, assume nel garantire la *resilience* del sistema delle PMI a possibili nuovi *downturn* o futuri *shock* finanziari.

Figura 2: it took 7 years for lending to SMEs to recover from the financial crisis.



Source: BoE, Peer-to-Peer Finance Association

Al momento molte PMI fanno fatica ad accedere al credito di cui hanno bisogno. I dati a disposizione dimostrano che nel Regno Unito solo il 36% delle PMI fa uso di finanziamenti esterni. Oltre il 50% considera un solo creditore quando cerca di finanziarsi ed il 25% non ha le risorse (tempo e denaro) per cercare ulteriori creditori. Questo fa sí che su dieci imprese ben sei ricorrano a fondi di natura privata per sostenersi. Inoltre, il 70% di esse preferisce crescere più lentamente piuttosto che chiedere prestiti. L'evidente *market failure* si verifica a causa di due asimmetrie informative:

1. *Lender vs Borrower*, ovvero quando l'imprenditore possiede maggiori informazioni dell'istituto di credito. Nel processo di finanziamento delle PMI, il *business model* è spesso eterogeneo, specialmente nel caso di *start-up* o *innovators*. Inoltre, le PMI non hanno una *proven-record* di *credit history*, senza menzionare che il rischio di fallimento è di solito maggiore. Pertanto è più difficile per le PMI accedere ai fondi necessari.

[5] BVA BDR, SME Finance Monitor 2018 Q4.

2. *Incumbent vs Competitor*, ovvero quando l'imprenditore non ha a disposizione molte opzioni quando deve decidere a chi chiedere un finanziamento. Infatti, spesso l'imprenditore tende a lavorare con un presistente *bank account provider*, che è già in possesso delle varie informazioni sul suo *business*/persona. La regolamentazione in ambito di Anti-Money Laundering (AML) e Know Your Customer/Business (KYC/KYB) impone una serie di controlli che allungano le tempistiche di concessione del credito nel caso l'imprenditore decida di rivolgersi ad altri finanziatori. Tempistiche che potrebbero causare un aumento insostenibile dei costi soprattutto nella fase di avvio dell'attività. per un *business* allo stadio iniziale.

La creazione di una *open data platform* e la soluzione tecnologica proposta

Da anni il Tesoro britannico (HMT) ha cercato di stimolare il finanziamento delle PMI lanciando varie iniziative dal lato dell'offerta, tra cui la creazione del Commercial Credit Data Sharing Scheme (2015) e del Bank Referral Scheme (2016), ma senza ottenere i risultati sperati. Più recentemente, lo schema regolamentare offerto da Open Banking[6] sta contribuendo a cambiare il modo in cui l'industria finanziaria britannica utilizza i dati, dal momento che ne è consentito il movimento attraverso pratiche standardizzate che utilizzano sicure Application Programming Interfaces (APIs). Questo permette alle PMI di condividere i dati delle transazioni sui propri conti correnti, il che riduce il vantaggio informativo del *provider* del conto e rende più semplice la competizione tra il sistema bancario tradizionale e le *non-banks*. Il sistema funziona grazie all'accettazione del concetto di *data portability*.

Prima di analizzare il modello proposto dalla BoE per ovviare alle problemtiche finora descritte, va sottolineato come la natura *non-rivalrous* dei dati favorisca i modelli che prediligono l'accesso ad essi piuttosto che il loro possesso. Infatti, il fatto che i dati vengano uitilizzati da una parte non vuol dire che non possano essere utilizzati da altri. I dati, quindi, hanno una natura tale che trascende il singolo *business* e possono essere replicati e combinati con altri dati a costi modesti; il loro valore viene massimizzato quando essi vengono condivisi e combinati. Questi *trend*, che devono essere visti alla luce della crescente legislazione in materia di *data protection* (GDPR), sono possibili grazie all'uso della tecnologia che ha reso la "*data portability*" attuabile ed economicamente vantaggiosa. La rapida trasmissione dei dati favorisce infatti lo sviluppo di un'economia digitale che si baserà sempre di più sul concetto di *portability* contrapposto a quello più classico di *ownership* e *storage*.

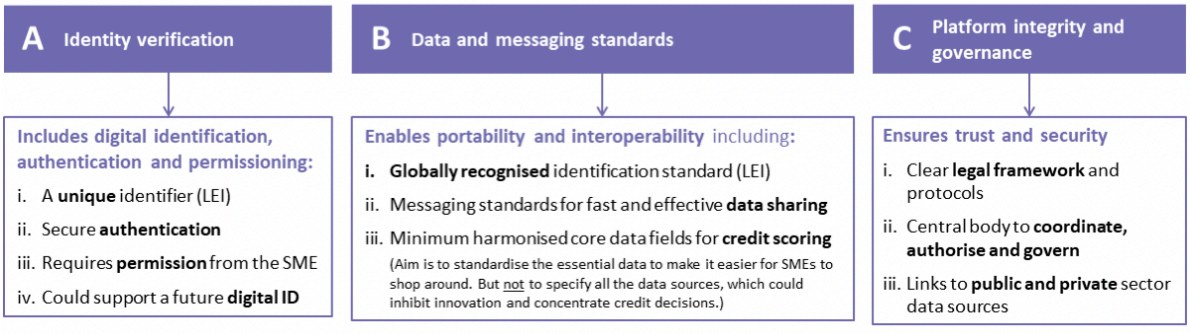
Proprio Open Banking ha, nei fatti, dimostrato la possibilità di condividere dati sensibili in modo sicuro con soggetti terzi utilizzando il sistema delle APIs. Contemporanemante, le *fintech* hanno sviluppato la capacità di sfruttare i dati presenti nel *market place* digitale in tempo reale favorendo la concessione di prestiti *short-term*.

[6] https://www.openbanking.org.uk

La BoE si è dunque chiesta come questa esperienza empirica potesse migliorare il sistema di concessione del credito alle PMI, concludendo che la creazione di una Open Data Platform dovrebbe pertanto basarsi su tre punti fondamentali (cfr. Figura 3):

1. Verifica dell'identità attraverso un Legal Entity Identifier (LEI) per garantire *digital identification*, *authentication* e *permissioning*.
2. Standardizzazione dei dati e dei messaggi mediante APIs per rendere effettive *portability* e *interoperability*.
3. Integrità della piattaforma e *governance* al fine di garantire fiducia, sicurezza e protezione dal *cyber-threat*.

Figura 3: Building blocks of the Open Data Platform.

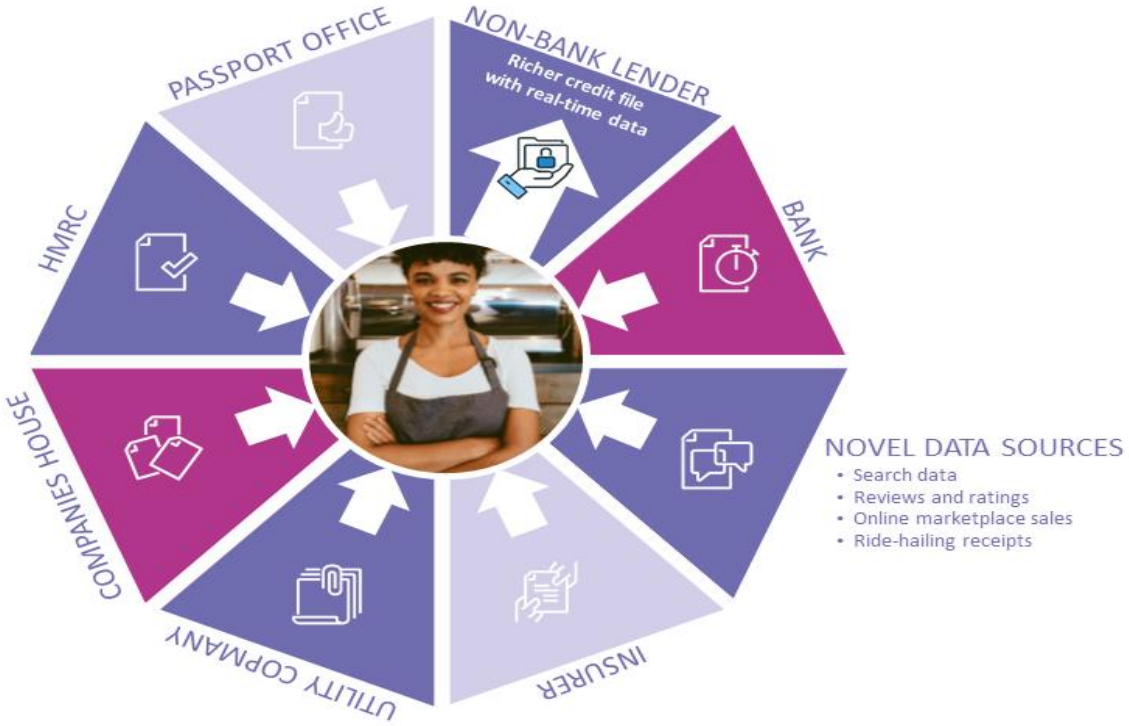


L'Open Platform si configurerebbe, quindi, come una rete decentralizzata di *data providers* che utilizzano una serie standardizzata di APIs per mettere a disposizione i dati all'interno del sistema finanziario in tempo reale, a richiesta delle PMI[7]. Si tratterebbe quindi di un sistema decentralizzato basato sul consenso delle PMI alla condivisione dei dati, senza alcuna struttura di deposito e senza la necessità di costruire un'apposita infrastruttura poiché, come nel sistema di internet, i protocolli e gli *standard* garantirebbero

[7] At the touch of a button, the SME would permission an API call to a handful of data providers with whom it already has a relationship (such as its bank, its utility company and its insurance company) to instantly share specified data fields with a third-party (such as a non-bank business lender). The data transfer would be encrypted end-to-end and would provide access for a specified (minimal) period of time. If the third party needs access again, they can request it easily and the SME can authorise the request effortlessly with their fingerprint, for example, or a glance at their smartphone. Expanding the sources of data that lenders could access, such as data held at insurance and utilities companies, as well as search, ratings and social media data could help to build richer credit files. Linking public sources such as the Passport Office, Driver and Vehicle Licensing Agency, HMRC and Companies House could improve the underwriting process for a loan by reducing the inefficiencies involved in identity verification. Opening access to all this data using common messaging and data standards could eliminate a significant barrier to entry and open up the market to greater competition. Moving data around using a system of APIs like this would also reduce the cost of AML checks. Banks say the burden of compliance is one of their biggest costs, so an efficiency saving like this would give incumbent lenders a clear and immediate incentive to take part and help make it a success (Open Data for SME finance, Bank of England, March 2020).

l'interoperabilità consentendo la creazione di una piattaforma sulla quale si le aziende stesse possano creare l'innovazione necessaria (cfr. Figura 4).

Figura 4: A diagram of the Open Platform applied to the SME finance use-case.



Il sistema cosí creato permetterebbe alle società finanziarie "innovative" di utilizzare nuovi dati per il *credit risk assessment*. Già oggi le *fintech* utilizzano i pagamenti in tempo reale e i dati delle transazioni per rafforzare il proprio *credit-score*. In futuro, i *lenders* potrebbero utilizzare ricerche *online* e *ratings data*, o *real-time shipment* e *satellite imagery data* per costruire un modello diverso di concessione del credito e stabilire la capacità di restituzione del *borrower*. Inoltre, la piattaforma potrebbe condurre alla realizzazione di un vero e proprio passaporto finanziario per gli individui, semplicemente raccogliendo i vari dati dalle varie fonti e dando al consumatore piena contezza del valore dei propri dati; ciò richiederebbe l'adozione delle raccomandazioni del Digital Competition Expert Panel Report[8] pubblicate da HMT il 13 marzo 2019.

La BoE è fortemente determinata a svolgere un ruolo di *leadership* per sostenere il cambiamento necessario, per quanto riconosca che esso possa avvenire solo a fronte di uno sforzo congiunto tra settore pubblico e settore privato. Nel promuovere l'innovazione, la BoE ricorda quale siano i principali obiettivi di *policy* che essa stessa intende perseguire attraverso la creazione del nuovo *framework* regolamentare che cambierà il finanziamento delle PMI attraverso il sistema dell'*open data*:

[8] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf

1. Sostegno all'obiettivo di politica economica del governo per una crescita economica del paese più omogenea, specialmente a fronte dello squilibrio geografico nello sviluppo delle PMI.
2. Effettiva inclusione finanziaria che consenta un più equilibrato e generale accesso al credito da parte di tutte le PMI a prescindere dalla propria posizione geografica.
3. Rafforzamento della stabilità finanziaria e della competitività permettendo a nuove entità di servire il mercato delle PMI.
4. Promozione di una regolamentazione della *privacy* all'altezza delle aspettative e delle esigenze del mercato digitale, con particolare riguardo al consenso sull'utilizzo dei dati, alla trasparenza, alla limitazione temporale e allo scopo.
5. Assicurare la sicurezza cibernetica per garantire la *resilience* del sistema e la fiducia dei consumatori ovvero assicurarsi che non vi sia alcun *central repository*, che lo *storage* di dati sia minimo e che vi sia un efficace sistema di *end-to-end encryption*.
6. Costruire un adeguato sistema di *governance* che garantisca l'adesione di tutti gli attori a un severo sistema di protezione della *privacy*, di *cyber-security* e di risoluzione delle potenziali controversie.

L'esperienza domestica e internazionale

A livello domestico, a seguito della pubblicazione del rapporto Future of Finance l'attività della BoE è stata incessante. Su questo specifico tema dell'Open Data Platform, la BoE ha avviato molti tavoli di discussione con altre banche centrali, *think tanks*, autorità pubbliche ed istituti privati, tra cui non solamente le banche tradizionali ma anche le *non-banks*, *data providers*, *fintech*, *bigtech*, *accounting software providers* ed assicurazioni. Da questa intensa attività sono emerse le seguenti considerazioni:

1. I benefici offerti dalla *data portability* sono stati riconosciuti trasversalmente. Se ben regolamentato, sia le banche tradizionali sia le *fintech* possono trarre beneficio da un sistema "*fully-connected*". Le prime possono infatti risparmiare sui costi, particolarmente sul dispendioso ed ancora manuale processo di *compliace* e AML; le seconde possono trarre grosse opportunità dal semplice accesso a una maggiore quantità di dati.
2. La necessità di adottare tecnologia e *standard* adeguati si collega a una effettiva ed omogenea garanzia che il maggior numero di soggetti possa accedere all'innovazione, di fatto rendendola più fruibile ed immediata.
3. Il valore aggiunto di avere accesso ad *additional data*, specialmente ai c.d. *government-verified data*[9] diminuisce il rischio di frode e di conseguenza il *credit risk*.

[9] Tra questi, dati anagrafici e fiscali.

Come riconosciuto dalla varie autorità nazionali (HMT, BEIS ed FCA *in primis*) se tutte le varie inziative di *open data*, che già avvengono *sector by sector*, utilizzassero gli stessi *standard* di messaggistica, sicurezza e *privacy*, potrebbero essere coordinate meglio e contribuire a costruire un sistema di *data portability* completo. Tuttavia, nonostante il supporto "teorico", le PMI rimangono prudenti con riguardo alla fase di implementazione, che richiederà uno sforzo proprio da parte di quelle stesse imprese PMI che il sistema intende favorire ma che in realtà ancora faticano ad adeguarsi allo stato attuale e agli *standard* in vigore, quali Open Banking.

A livello internazionale, sono vari gli esempi di adozione del concetto di *data portability* e del suo diverso stato di implementazione nelle varie giurisdizioni:

1. **Cina**: le PMI hanno un accesso immediato e diretto al credito grazie all'utilizzo di piattaforme *online*. Il sistema cinese beneficia della sua grandezza e dell'ampio accesso ai dati. Si ispira a quello dei *social media*, mescolando i dati "sociali" con quelli di credito, legando la *payment history* a dati posseduti da agenzie pubbliche e istituzioni finanziarie per calcolare con maggiore precisione la *creditworthiness* del consumatore. Tuttavia, la replica di questo sistema nel Regno Unito presenta complicazioni, sia a causa di *network* presistenti, sia per la mancanza di un *recognised identification scheme* a livello nazionale. Ciò nonostante, il modello cinese dimostra l'importanza giocata da un unico sistema di verifica dell'identità e dalla standardizzazione di dati e messagistica per creare un vero e proprio ecosistema che consenta lo sviluppo della piattaforma.
2. **India**: nel 2010 le autorità hanno creato il sistema di identità digitale Aadhaar, un codice biometrico attribuito a ciascun individuo, che copre il 99% della popolazione adulta (1,2 miliardi di persone). Aadhaar fa parte del più ampio programma "India Stack", pioniere della digitalizzazione in ambito finanziario attraverso una serie di *layered applications*, identificazione biometrica, unificazione dell'infrastruttura del sistema dei pagamenti (UPI) e portabilità dei dati. India Stack mira a creare un vero e proprio *digital single market* forzando la diffusione del *data sharing*. Il modello indiano dimostra l'importanza del ruolo promotore dell'autorità centrale nel guidare lo sviluppo tecnologico. Le critiche rivolte al tipo di garanzie sulla *privacy* offerte da Aadhaar offrono un ulteriore spunto di riflessione sulla necessità di porre in essere un *design* del sistema che ne possa garantire uno sviluppo equilibrato.
3. **Estonia**: il programma governativo e-Estonia ha imposto un'identità digitale per tutti i cittadini e garantisce l'accesso a tutti i servizi digitali offerti, mediante un sistema di *chip* e *public-key encription* che ne tutela la sicurezza. I dati non vengono custoditi in un solo luogo, bensí su un *data-sharing network* chiamato X-Road, di fatto un *distributed data exchange layer* che separa le informazioni detenute in diversi sistemi informatici. Ogni possessore di dati decide quali informazioni rendere disponibili e chi ne può avere accesso attraverso X-Road. L'obbligatorietà del sistema dell'identità

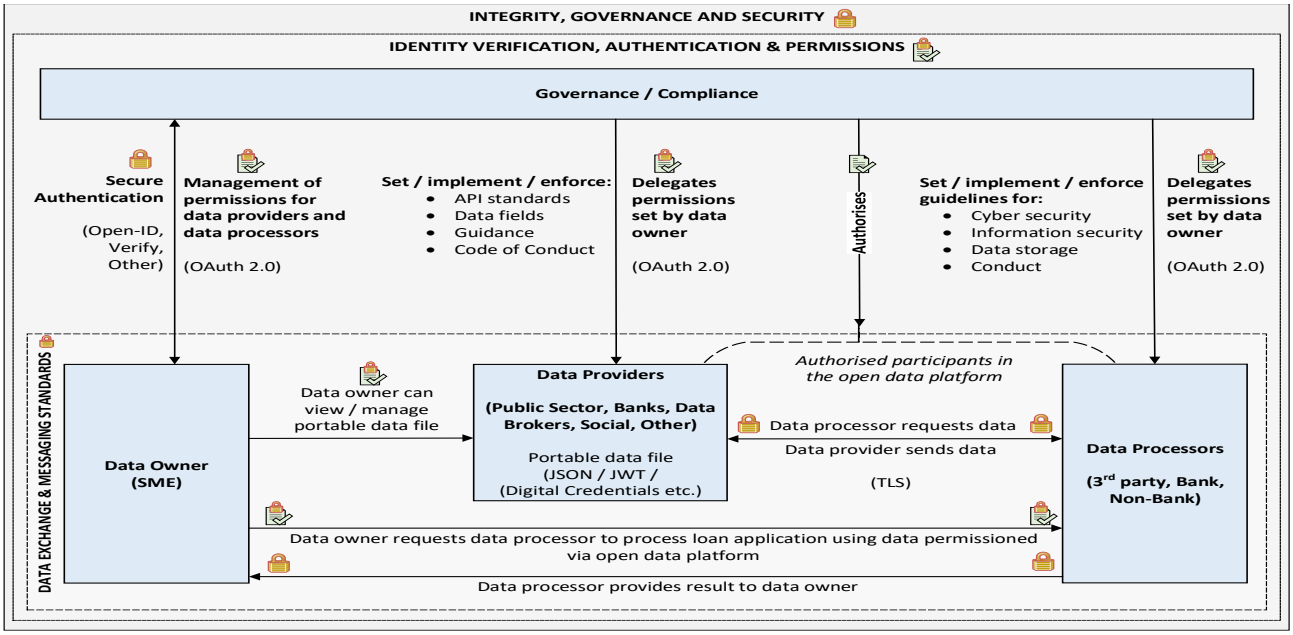
digitale e l'enorme diffusione dei servizi digitali rendono l'Estonia un modello unico per capacità di penetrazione dell'innovazione (99% della popolazione per il 99% dei servizi).

4. **Australia**: l'introduzione del Consumer Data Right (CDR) nell'agosto 2019 facilita la condivisione dei dati con soggetti terzi da parte delle quattro maggiori banche, le istituzioni finanziarie e i consumatori, sul modello di Open Banking. Il modello, che sarà esteso a tutto il settore bancario entro luglio 2020, verrà poi esteso ad altri settori, quali le telecomunicazioni. La diffusione è più ampia che nel Regno Unito, dove le direttive della Competition and Market Authority (CMA) si applicano solo alle 9 maggiori istituzioni. Il modello australiano dimostra, quindi, come sia possibile rendere effettivo il coinvolgimento di istituzioni minori in piattoforme che utilizzano i principi di *open banking*. Inoltre, il CDR prevede pene pecuniarie per gli individui in caso di *data breaching*.

Ulteriori considerazioni tecniche

Il documento della BoE conclude con una serie di considerazioni tecniche che mirano a illustrare scelte e *standard* necessari a realizzare una world-class Open Data Platform, la cui struttura architettonica dovrebbe basarsi su quattro pilastri: *data owner*, *data providers*, *data processors* e *governance* (cfr. Figura 5), che si accompagnerebbero ai principi guida di questo processo: collaborazione tra settore pubblico e privato, fiducia, leverage della tecnologia esistente, apertura e competitività (v. Allegato 1).

Figura 5: Components and flows in the Open Data Platform.



Per informazione.

ALLEGATO 1

TECHNICAL CONSIDERATIONS[10]

Conceptual architecture

Conceptually, the Open Data Platform architecture comprises four components:

- **Data owner** - who has control over setting, maintaining, revoking and reviewing specific permissions on how their data is shared by *data providers* on their behalf and how it is processed by *data processors*.
- **Data providers** - public and private sector data sources. These data providers will be authorised and permissioned to share data when explicitly permitted by the *data owner* to share with an authorised *data processor*.
- **Data processors** - authorised and vetted third parties could interact directly (via their own channels) or indirectly (via a cloud-based accounting platform) with prospective loan applicants. Third parties would be able to request and process data securely, and build a core credit file with additional data from public and private sector *data providers*, based on permissions explicitly set by the *data owner*.
- **Governance** - orchestrates the authorisation and authentication flows as well as possible API endpoint integrations. This may need to be overseen by a public body, which would also be responsible for non-technology aspects such as authorising and vetting third-party participants, implementing standards and guidelines, including around cyber-security, and enforcing a code of conduct.

Principles for the architecture and technology

In designing this Open Data Platform, there are a number of principles that guide our proposed architecture and technology:

- Public-private collaboration – recognise and maximise the relative strengths of the public and private sector. Public authorities can help provide a degree of credibility and set standards for private companies to innovate upon. This should minimise the risk of crowding out innovation by keeping governance and standards to the minimum required to ensure credibility, utility and operational resilience. And it should seek to harness rather than replace the role provided by individual institutions in the system today.
- Ensure trust, while supporting innovation – the standards that are put in place must be best-in-class to ensure operational and cyber-resilience and they must prioritise the interests of end-users to ensure data protection.
- Leverage existing technology – to minimise the burden on industry and make use of existing investments in technology infrastructure and standards, where possible. For

[10] Open Data Platform for SME finance, Capitolo 6 (Bank of England, Marzo 2020).

example, many of the Open Banking API standards could be rolled out more widely, maximising the value of related technology investments by fintechs and banks.

- Open and competitive – use best-in-class and open technologies and standards that enable private companies to compete on level terms, like the early standards deployed with the internet, rather than picking proprietary technologies and standards that create winners and losers.

Design choices

These principles lead to a distributed model, with minimal central governance. This maximises the role of existing nodes in the financial system, while minimising overheads and bureaucracy. It also leads towards a model of minimal data-storage, such that existing data providers maintain responsibility for the data they hold, and data processors do not store multiple copies of data around the system. Such a model enhances cyber-resilience since there is no central data repository and because it minimises the impact of a cyber or data breach at any given node in the financial system.

Similar to Open Banking, the Open Data Platform would involve users sharing their data via APIs with third parties. This section covers some technical requirements to ensure confidence and trust in the platform. In any data exchange, there are three key elements to consider:

1. Identity verification, authentication and permissioning
2. Data exchange and messaging standards, enabling portability and interoperability
3. Integrity, governance and security, ensuring trust

1. Identity verification, authentication and permissioning

The SME needs a way to grant permissions to (public and private sector) data controllers to share their data with third parties. These data controllers need a way to confirm that an SME has granted permission for data to be shared, processed and for what period of time. The data controllers also require assurance and verification that third parties can be trusted with personal data they are permitted to share. Third parties require confirmation of what they are permitted to use and process, for whom and for how long. Each of these groups require a standardised means to:

- Authenticate that the parties sharing and requesting data *are* who they claim to be;
- Confirm permissions for what can be accessed by whom and for how long.

Both public and private sector data controllers and third parties require a secure and standardised way to request and exchange data for platform users. Both groups are required to protect any data exchanged, processed or stored from loss.

OAuth 2.0. OAuth 2.0 is the leading industry standard and widely used to provide a secure method for verifying digital identities. Further, it provides a formal structure for obtaining,

and securely transferring, consumer permissions between entities. OAuth is commonly used for permitting websites to share data with one another.

OAuth 2.0 uses the concept of tokens that can be passed between parties during a transaction for authentication purposes, enabling users to allow third parties to act on their behalf. These tokens could leverage the JSON Web Token (JWT) standard providing an optionally validated and/or encrypted container format that is used to securely transfer information between two parties.

OAuth 2.0 is just a framework and therefore, for financial data use cases, secure implementation of OAuth must be considered by deploying two supporting standards in conjunction.

OpenID Connect. OpenID Connect (OIDC) is a standard built on top of OAuth to provide delegated authentication. OIDC enables a relying party to defer to an identity provider to authenticate users, just as some BigTechs or the Government's Verify system do today. The relying party does not have to be concerned with managing usernames and passwords, instead they trust the identity provider to do that. The identity provider then returns an ID token that the relying party can use to assert a user's identity. It is assumed the identity provider is enabling strong and secure authentication by default.

The OIDC specification defines an element called the claims request parameter, which can be used to request that specific items and their properties, including authorisation, are returned in the ID token. The request parameter also allows users to sign the request, which ensures they can detect if it has been tampered with.

2. Data exchange and messaging standards

Systems and data sources could interface and exchange data via APIs. These APIs could follow the same style and approach taken by Open Banking, leveraging existing APIs for transactions or accounts, for example. Open Banking evolved these APIs iteratively, addressing issues found or introducing necessary features in each new version. The latest version 3.1 of the Open Banking APIs are a much more robust set than those published 18 months ago. Any additional open data initiatives should seek to leverage the gains made there. Core credit data would be comprised of a standardised set of data fields. Specifics of this set of data could be defined by the private sector solely or in collaboration with public sector bodies. Non-core data would not be standardised and instead would be data source specific.

3. Integrity, governance and security

Financial API. The Financial API Specification (FAPI) is a draft standard for configuring financial API security solutions which makes extensive use of OIDC. It defines recommended flows, configuration parameters, and signing and encryption algorithms for implementations of OAuth and OIDC to enhance security and mitigate known risks and

attacks. It also adds additional security controls around all data requests and responses. The FAPI enhances OAuth applications for financial data by providing security even if some attacks on the flows are successful, for example if an attacker manages to phish an access token or intercept requests and responses of a secure message flow. To achieve such protections, the FAPI incorporates several new security mechanisms which aim to increase the security of the protocol. As with any nascent standard, edge cases may reveal areas of improvement when those aims are not met.

All three standards (OAuth 2.0, OIDC and FAPI) are open source and do not therefore favour any proprietary interests. The combination of the three standards should meet the authorisation and authentication needs of the Open Data Platform. But there are additional workflow standards that could further mitigate risks. For example, Open Banking uses a two-stage request mechanism where a payment or account request is first staged before being authorised. This allows a bank to present the information request to the user at the time of consent so they clearly understand what it is they are agreeing to.

JSON Web Token. The purpose of a JSON Web Token (JWT) is to enable the receiving party to trust that the data received was unaltered during transport. It is self-contained, meaning that it can neatly encompass identifying information about a user, what a user can access, an expiration date, a signature for content validation and importantly any other information.

For example, a token can also embed a combination of identifiers such as the Legal Entity Identifier (LEI), Unique Taxpayer Reference (UTR), Companies House Number or VAT number. It could also contain some data elements of a core credit file.

JWT is a designed for lightweight transmission of certain data. It does not encrypt that data, therefore encryption standards should be deployed to secure tokens or data shared with third parties in transit.

Transport Layer Security. Transport Layer Security (TLS) is used to encrypt requests and responses between third parties and banks using certificates. TLS is used in every browser worldwide to provide secure browsing functionality. API endpoints can be secured with TLS. Another alternative could be RSA cryptography which deploys public and private keys. The public key can be shared with everyone, whereas the private key must be kept secret. Both the public and the private keys can encrypt a message, with one key used to encrypt a message and the opposite key used to decrypt it.

Other governance considerations. An Open Data Platform (like Open Banking) will require regulators, government institutes, security firms and data source providers to evaluate and assess criteria for trusted status. Similarly, to ensure the objectives of such a platform are achieved and accessible to all, enforcement of guidelines for user experience and a code of conduct should also be established.

Participants would be expected to implement strong user authentication, using multi-factor authentication at minimum as well as security controls to protect confidentiality and integrity of user's security credentials.

Any governance body overseeing the platform should strongly support adoption of, and compliance with, strong information security management frameworks such as ISO27001 or the National Institute of Standards and Technology cyber-security framework, including requirements for auditing compliance.

The body could convene industry groups, including participants, to support sharing of threat intelligence, developing standards, supporting engagement and communications as well as a developer community. The network platform must be secured and subject to regular security (and cyber-penetration) testing, to identify any vulnerabilities and mitigating actions.