Centres for European Policy Network
FREIBURG | BERLIN | PARIS | ROMA

cepStudio

Per una *leadership* europea in materia digitale

Diciassette raccomandazioni

Bert Van Roosebeke, Martina Anzini, Philipp Eckhardt & Anne-Carine Pierrat

Il presente documento rappresenta la sintesi di uno studio realizzato per la società SAP. Le opinioni espresse in tale studio sono da attribuire unicamente agli autori e non riflettono necessariamente il punto di vista della società SAP.

La versione integrale dello studio è disponibile in lingua inglese qui

Friburgo in Brisgovia, dati aggiornati al mese di febbraio 2020

Autori:

Bert Van Roosebeke,Directeur de recherches

Martina Anzini

Philipp Eckhardt

Anne-Carine Pierrat

Centrum für Europäische Politik FREIBURG | BERLIN

Kaiser-Joseph-Strasse 266 | D-79098 Freiburg

Schiffbauerdamm 40 4315 | D-10117 Berlin

Tel. + 49 761 38 69 30

cep@cep.eu

Traduzione e distribuzione:

Centro Politiche Europee ROMA

Via G. Vico, 1 | I-00196 Roma

Tel. + 39 0684388433

cepitalia@cep.eu

Il **Centro Politiche Europee** ROMA e i suoi partner
Centrum für Europäische Politik FREIBURG | BERLIN e **Centre de Politique Européenne** PARIS
compongono il **Centres for European Policy Network** FREIBURG | BERLIN | PARIS | ROMA

*Gli istituti della rete **cep** sono specializzati nell'analisi e nella valutazione degli atti promossi dalle istituzioni dell'Unione europea nell'ambito delle politiche di loro competenza e nel quadro d'insieme del processo di integrazione. Il lavoro scientifico, riflesso in particolare nelle proprie pubblicazioni, viene portato avanti indipendentemente da qualsiasi interesse di parte e in favore di un'Europa che rispetti lo stato di diritto e i principi dell'economia sociale di mercato.*

SOMMARIO

Lo studio individua tre priorità principali e diciassette raccomandazioni dettagliate per un'agenda politica europea volta ad affermare la leadership europea nell'economia digitale. Definire delle priorità è urgente. L'Europa è in ritardo rispetto agli Stati Uniti e alla Cina per quanto riguarda l'intelligenza artificiale e il *cloud computing*, due delle tecnologie che maggiormente influenzeranno la crescita economica negli anni a venire.

Mentre gli effetti di rete e le economie di scala hanno portato a un predominio americano e cinese nei mercati *Business to Consumer* ('B2C'), l'UE dovrebbe ora intraprendere le azioni necessarie per evitare che lo stesso avvenga nei mercati *Business to Business* ('B2B').

Le misure protezionistiche non sono utili per riconquistare la sovranità tecnologica europea. Di conseguenza, le tre priorità hanno tutte un approccio orientato al mercato, e cioè volto a stimolare l'innovazione e a salvaguardare la concorrenza tra i fornitori nell'economia digitale.

Come **prima priorità**, l'UE dovrebbe promuovere attivamente un vero mercato interno dei dati, in quanto l'UE non sta sfruttando il potenziale economico relativo alla condivisione e al (ri)utilizzo dei dati presenti sul proprio territorio. Le azioni in questo campo dovrebbero riguardare dati personali, pubblici e non personale.

Per quanto riguarda i dati personali, si chiede una maggiore armonizzazione, nonché l'uso di *sandboxes* e *regulatory hubs* per creare certezza giuridica nell'applicazione del GDPR.

La disponibilità di dati pubblici dovrebbe essere aumentata attraverso la standardizzazione dei formati dei dati, attraverso l'inclusione della disponibilità dei dati come criterio di selezione negli appalti pubblici e attraverso regole più stringenti per l'accesso ai dati pubblici di elevato valore.

Le ragioni per cui le imprese esitano a condividere dati non personali sono molto diverse e non tutte possono essere risolte con un'apposita politica pubblica. L'iniziativa dell'UE per un *data space* europeo può tuttavia contribuire a ridurre i costi di transazione associati alla condivisione dei dati tra imprese.

L'obbligo imposto a volte dagli Stati Membri di conservare i dati personali, pubblici o di tipo non personale sul territorio nazionale ostacola la realizzazione di economie di scala ed è a ben vedere incompatibile con l'idea stessa di un mercato interno dei dati. Obblighi di questo genere dovrebbero rimanere l'eccezione e invitiamo la Commissione a procedere coerentemente contro le prescrizioni di localizzazione che non sono giustificate ai sensi del Regolamento generale sulla protezione dei dati e del Regolamento per la libera circolazione dei dati non personali nell'Unione europea.

Come **seconda priorità**, l'UE dovrebbe garantire un'effettiva concorrenza sui mercati digitali nella sfera B2B. I mercati B2B sono nettamente diversi dai mercati B2C e non riscontriamo la reale necessità di un'azione normativa per salvaguardare la concorrenza. Nel campo delle attività *cloud*, l'integrazione verticale e l'accesso limitato alle infrastrutture sui diversi livelli del mercato (IaaS, PaaS e Saas) potrebbero limitare la concorrenza in futuro. Il diritto della concorrenza è in grado di gestire tali problemi e non è necessaria una regolamentazione specifica del settore. Negli stessi mercati, l'accesso limitato ai dati essenziali può limitare la concorrenza. In questi casi, potrebbero essere necessari interventi normativi volti a garantire la portabilità dei dati sui mercati del *cloud*. In ogni caso, tali interventi dovrebbero interessare solo gli operatori che detengono una posizione dominante sul mercato.

La **terza priorità** riguarda una politica industriale digitale europea e individua nella competitività generale dell'economia digitale europea la condizione preliminare per la sovranità digitale.

La politica industriale digitale dovrebbe proteggere l'apertura dell'economia, consentire economie di scala, comprendere una regolamentazione delle infrastrutture favorevole agli investimenti e promuovere le competenze digitali.

Proponiamo un quadro europeo per un *cloud computing* sicuro e affidabile come elemento principale di tale politica industriale digitale. Il quadro di riferimento risponde ai timori relativi alla sicurezza dei dati, alla governance degli stessi e alla disponibilità dei servizi nel *cloud*. Tali preoccupazioni derivano in ultima analisi dall'uso diffuso di *hyperscalers* non europei da parte delle aziende dell'UE e riflettono il carattere di bene pubblico della disponibilità di servizi *cloud* per le nostre economie e società.

Il quadro prospettato è proporzionato, efficiente e non discriminatorio. Esso definisce schemi di certificazione volontaria per i fornitori di servizi *cloud* sulla base del Regolamento europeo sulla cibersicurezza. Di seguito, proponiamo una struttura di *governance* che garantisce servizi *cloud* sicuri agli operatori di alcuni settori essenziali come i servizi finanziari, l'energia o i trasporti in tutta l'UE. La nostra proposta mira soprattutto ad evitare distorsioni della concorrenza tra gli operatori attivi su tali mercati.

17 Raccomandazioni per una *leadership* Europea nell'economia digitale

NOVE RACCOMANDAZIONI PER UN MERCATO UNICO DEI DATI NELL'UE

- **Raccomandazione n. 1**: la Commissione dovrebbe continuare a monitorare da vicino l'evoluzione del mercato del *data trusteeship* per individuare tempestivamente l'emergere di qualsiasi ostacolo che impedisca loro di operare al di là dei confine nazionali.

- **Raccomandazione n. 2**: la Commissione Europea dovrebbe utilizzare l'imminente revisione del Regolamento generale sulla protezione dei dati per garantire la certezza del diritto attraverso un più alto livello di armonizzazione.

- **Raccomandazione n. 3**: vanno sostenute le iniziative che mirano ad aumentare la chiarezza giuridica del Regolamento generale sulla protezione dei dati stabilendo un dialogo tra le autorità e le imprese. Queste ultime possono aiutare le autorità di garanzia della protezione dei dati a individuare e conoscere i nuovi sviluppi tecnologici, garantendo al tempo stesso il rispetto del diritto alla protezione dei dati. Allo stesso tempo, queste iniziative, siano esse chiamate "*sandbox*" o *regulatory hubs*, devono essere neutrali rispetto alle dinamiche di mercato (e cioè accessibili a tutti gli operatori del mercato).

- **Raccomandazione n. 4**: la Commissione dovrebbe sviluppare, insieme ai vari soggetti interessati, piattaforme aperte di standardizzazione e formati uniformi per i dati degli enti pubblici, così che tali dati siano disponibili. La standardizzazione dovrebbe essere effettuata su base settoriale.

- **Raccomandazione n. 5**: la Commissione dovrebbe mirare ad estendere il campo di applicazione della Direttiva relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico così da includervi le società private che forniscono servizi di interesse pubblico, garantendo così la disponibilità di dati privati relativi alla fornitura del servizio di interesse pubblico. La Commissione dovrebbe, inoltre, incoraggiare gli Stati membri e le loro autorità a subordinare l'aggiudicazione degli appalti pubblici alla accessibilità dei dati generati in questo contesto.

- **Raccomandazione n. 6**: la Commissione dovrebbe esaminare se l'istituzione di un obbligo generale di accesso ai dati del settore pubblico e ai dati di interesse pubblico possa essere necessaria, in primo luogo per i set di dati di maggior valore. Dovrebbe esaminare, in particolare, le pratiche di condivisione dei dati delle aziende pubbliche e private in particolari settori - ad esempio i trasporti, il geospaziale - per valutare se la spontanea condivisione dei dati, basata su accordi volontari, sia sufficiente o se siano necessari ulteriori interventi - sia attraverso misure di *soft law* che attraverso il diritto comunitario vincolante.

- **Raccomandazione n. 7**: l'iniziativa della Commissione Europea sullo spazio europeo dei dati può contribuire a ridurre i costi di transazione associati alla condivisione dei dati B2B in Europa. L'iniziativa merita di essere sostenuta fintanto che rimane neutrale dal punto di vista del mercato.

- **Raccomandazione n. 8**: non dovrebbe essere introdotto un nuovo diritto di proprietà sui dati. Il controllo di fatto di dati attraverso il diritto contrattuale e le restrizioni tecniche è sufficiente per lo sviluppo del mercato dei dati.

- **Raccomandazione n. 9**: poiché i requisiti di conservazione dei dati sul territorio nazionale ostacolano lo sviluppo di un mercato unico dei dati nell'UE, la Commissione UE dovrebbe procedere in modo coerente contro di essi laddove non giustificati ai sensi del Regolamento generale sulla protezione dei dati e del Regolamento per la libera circolazione dei dati non personali nell'Unione europea. Per consentire l'identificazione dei requisiti di conservazione locale dei dati ai sensi del Regolamento generale sulla protezione dei dati, dovrebbe essere esaminata la possibilità di istituire un registro che li enumeri.

CINQUE RACCOMANDAZIONI PER CONSERVARE UNA CONCORRENZA EFFICACE SUI MERCATI DEL *CLOUD* E DIGITALI

- **Raccomandazione n. 10:** il mercato dei servizi *cloud* su larga scala (e cioè quello degli *hyperscalers*) è attualmente caratterizzato da un'intensa concorrenza tra un numero relativamente ridotto di competitori che devono far fronte a costi fissi elevati. Resta da vedere se l'attuale livello di concorrenza prevarrà anche in futuro. In ogni caso, un intervento pubblico motivato da preoccupazioni in materia di concorrenza – come la regolamentazione dei costi di passaggio da un fornitore di servizi *cloud* a un altro, dei requisiti di interoperabilità o dei prezzi per l'utente finale – è giustificabile solo se a un fornitore di servizi *cloud* è ascrivibile un significativo e non contendibile potere di mercato. In presenza di un tale potere di mercato, il diritto della concorrenza sembra in grado di offrire una risposta adeguata. Si sconsiglia l'uso di una regolamentazione settoriale specifica per i fornitori di servizi *cloud* dominanti.

- **Raccomandazione n. 11**: occorre verificare caso per caso se un fornitore di *Platform as a Service* ('PaaS') detenga o meno un significativo potere di mercato. In ogni caso, la constatazione di una posizione dominante non contestabile da parte di un fornitore di piattaforma dovrebbe essere una condizione preliminare per un intervento *antitrust*. Se dimostrata, tale posizione dominante può essere affrontata in modo appropriato utilizzando il diritto generale della concorrenza. Non è evidente la necessità di una regolamentazione specifica del settore.

- **Raccomandazione n. 12**: le pratiche di abbinamento o aggregazione (rispettivamente denominate *tying* e *bundling*) messe in atto dai fornitori di *cloud* che si integrano verticalmente nel mercato PaaS non sono problematiche, a meno che tali fornitori non detengano un potere di mercato non contendibile sui mercati del *cloud*. In tal caso, il diritto della concorrenza è in grado di far fronte a questo comportamento abusivo.
  In assenza di *tying* e *bundling*, il rifiuto da parte di un fornitore di *cloud* integrato verticalmente di concedere ai concorrenti PaaS l'accesso alla sua infrastruttura *cloud* può essere affrontato utilizzando la dottrina delle *essential facilities*. Questa dottrina offre un compromesso convincente tra la protezione dei diritti di proprietà intellettuale e la concorrenza sui mercati secondari. La necessità di intervento è limitata ai casi in cui sono soddisfatti i seguenti criteri: (1) il fornitore di servizi *cloud* detiene una posizione dominante non contendibile sul mercato dei servizi *cloud*, (2) l'uso del *cloud* è inevitabile, (3) i fornitori PaaS concorrenti offrono una prodotto innovativo rispetto a quello dell'*incumbent* (e quindi diverso) e (4) il fornitore di servizi *cloud* non può offrire ragioni obiettive che giustifichino il rifiuto di accesso.
  Sebbene la regolazione settoriale dell'accesso alle infrastrutture essenziali possa anch'essa mitigare i problemi associati alla presenza di fornitori di *cloud* dominanti e integrati verticalmente sul mercato PaaS, non sono chiaramente evidenti i vantaggi di tale regolamentazione rispetto al diritto della concorrenza.

- **Raccomandazione n. 13:** l'accesso privilegiato ai dati può ostacolare la concorrenza. L'integrazione verticale degli operatori attivi nel mercato *Infrastructure as a Service* ('IaaS') fino ai mercati PaaS e *Software as a Service* ('SaaS') e la conseguente concentrazione del mercato possono aggravare i problemi di concorrenza sul mercato SaaS, legati all'accesso privilegiato ai dati. Inoltre, l'accesso privilegiato ai dati può causare problemi di concorrenza in numerosi mercati a valle.
  Grazie alla dottrina delle *essential facilities*, il diritto della concorrenza offre una solida base per affrontare i problemi relativi all'integrazione verticale. Allo stesso tempo, però, nel momento in cui i dati si rivelano la *essential facility*, garantirvi l'accesso può rivelarsi molto difficile e poco pratico. In tal caso, possono essere necessari rimedi alternativi o interventi normativi che impediscano che i dati siano o diventino una *essential facility*. Tali interventi dovrebbero mirare ad aumentare la trasferibilità dei dati, sia abbassando le barriere al cambio di fornitore, sia impedendo situazioni di *lock-in*, sia riconoscendo diritti di portabilità dei dati.
  Tuttavia, nel fare ciò, i diritti di proprietà intellettuale dovrebbero essere tenuti in debita considerazione. In ogni caso, la individuazione di una posizione dominante sul mercato in assenza di concorrenza potenziale su un ben definito mercato dei dati a monte deve essere una condizione preliminare per qualsiasi intervento. Nei casi in cui i mercati sono definiti in modo molto ristretto (ad esempio a livello dei singoli marchi), l'individuazione di una posizione dominante sul mercato può essere piuttosto semplice e la regolamentazione potrebbe essere una buona opzione. In tutti gli altri casi, il diritto della concorrenza può garantire una più accurata definizione del mercato rilevante e un'analisi più raffinata della dominanza sul mercato.

- **Raccomandazione n. 14:** gli strumenti più appropriati per garantire la certezza del diritto nell'applicazione del diritto della concorrenza al *pooling* di dati sono i seguenti:
    - le linee guida della Commissione perché, individuando le circostanze significative per l'applicazione dell'articolo 101 del TFUE agli accordi di *pooling* di dati, le imprese possono farvi affidamento nel valutare la liceità dei propri comportamenti;
    - le lettere di orientamento, perché il livello di cambiamento apportato dai *Big Data* nell'analisi del diritto della concorrenza è talmente elevato da rendere probabile che sorgano questioni genuinamente nuove. Ciò consentirebbe alla Commissione di accogliere le richieste di lettere di orientamento avanzate dagli operatori.

TRE RACCOMANDAZIONI PER UNA POLITICA INDUSTRIALE EUROPEA NEL DIGITALE

- **- Raccomandazione n. 15**: Stabilire un'economia digitale europea competitiva è una *condicio sine qua non* per la sovranità digitale. La maggior parte del lavoro e degli investimenti per raggiungere questo obiettivo deve provenire da investitori privati. Ciononostante, l'UE, i legislatori nazionali e i responsabili politici dovrebbero stabilire un quadro normativo appropriato affinché ciò avvenga. Tale quadro dovrebbe (1) salvaguardare l'apertura dell'economia e (2) la concorrenza, (3) consentire economie di scala, (4) comprendere una regolazione delle infrastrutture favorevole agli investimenti e (5) promuovere le competenze digitali.

- **- Raccomandazione n. 16**: l'UE, attraverso la Commissione, dovrebbe negoziare un accordo con gli USA che chiarisca le norme relative all'accesso transfrontaliero alle prove elettroniche nel contesto di un procedimento penale. Tale accordo non solo dovrebbe proteggere i cittadini e le imprese dell'UE garantendo le necessarie salvaguardie, ma dovrebbe anche mirare ad aumentare la certezza del diritto nelle richieste di accesso ai dati da parte delle autorità giudiziarie statunitensi ai fornitori di servizi dell'UE, prevenendo così dei conflitti tra ordinamenti giuridici.

- - **Raccomandazione n. 17:** proponiamo un quadro europeo per un *cloud computing* sicuro e affidabile che affronti le preoccupazioni relative alla sicurezza dei dati, alla *governance* degli stessi e alla disponibilità dei servizi nel *cloud*. Il crescente utilizzo di tali servizi comporta molti vantaggi economici, ma allo stesso tempo ci pone di fronte a rischi politici e operativi che possono mettere a repentaglio la continuità dei servizi essenziali. Il carattere di bene pubblico della disponibilità dei servizi *cloud* giustifica l'intervento pubblico.
- Proponiamo la creazione di un quadro europeo per il *cloud computing* sicuro e affidabile in quanto proporzionato, efficiente e non discriminatorio.
  Esso si dovrebbe articolare in tre fasi.
  - Nella **fase 1**, l'UE dovrebbe definire requisiti comuni per il *cloud computing* sicuro e affidabile che affrontino le preoccupazioni degli utenti relative alla sicurezza dei dati, alla *governance* degli stessi e alla disponibilità dei servizi. Come richiesto dalla Commissione europea, l'Agenzia europea per la sicurezza delle reti e dell'informazione ('ENISA') dovrebbe redigere schemi di certificazione di base per la sicurezza del *cloud computing*. Inoltre, l'ENISA dovrebbe redigere schemi complementari di certificazione della sicurezza del *cloud*

computing per le pubbliche amministrazioni e i settori che forniscono servizi essenziali (secondo la direttiva Network and Information Security directive o 'NIS').

- Nella **fase 2**, le modalità già esistenti per il rilascio di certificati nella regolamentazione sulla sicurezza informatica (*Cybersecurity Act*) possono essere applicate alla certificazione dei fornitori di servizi *cloud* senza alcuna modifica. Non è necessario rendere obbligatoria la certificazione.
- Nella **fase 3**, l'utilizzo dei servizi *cloud* da parte degli operatori attivi in determinati settori può essere subordinato all'utilizzo di un fornitore certificato che offra un certo livello di sicurezza *cloud*. Tali requisiti normativi devono essere basati sul rischio, proporzionati e non possono distorcere la concorrenza, né tra fornitori di servizi *cloud* né tra gli enti regolamentati.
- Al fine di raggiungere un'applicazione uniforme di questi requisiti normativi, raccomandiamo nella fase **3a)** di identificare in modo coerente gli operatori di servizi essenziali a cui si applicheranno i requisiti normativi. Per questo motivo, proponiamo un ruolo più formale per il "gruppo di cooperazione" della direttiva NIS. In particolare, riteniamo che quest'ultimo dovrebbe identificare gli operatori del settore dell'energia, dei trasporti e dei mercati finanziari (ma non per le banche).
- Dopo aver confermato in una fase **3b)** che i requisiti di sicurezza *in-the-cloud* per gli operatori di servizi essenziali seguiranno lo schema di certificazione di sicurezza *in-the-cloud* dell'UE, diverrà necessario in una Fase **3c)** il garantire un'applicazione uniforme dello schema di certificazione.

Nel settore finanziario, l'attuale struttura di vigilanza, ben sviluppata, può essere sufficiente per raggiungere questo obiettivo. Per il settore dell'energia e dei trasporti, suggeriamo l'istituzione di nuovi organi decisionali di vigilanza e di autorità di sicurezza informatica, responsabili della uniformità di applicazione. Data la natura nazionale dei mercati della sanità, dell'acqua e delle infrastrutture digitali, suggeriamo che in tali settori le autorità nazionali siano responsabili dell'applicazione dei sistemi di certificazione *cloud*.

Sebbene sia improbabile un'applicazione uniforme nel settore pubblico dello schema di certificazione UE per la sicurezza *in-the-cloud*, l'uso dello schema di certificazione da parte del settore pubblico ne aumenterebbe la rilevanza nonché il peso dei fornitori che vi aderiscono.