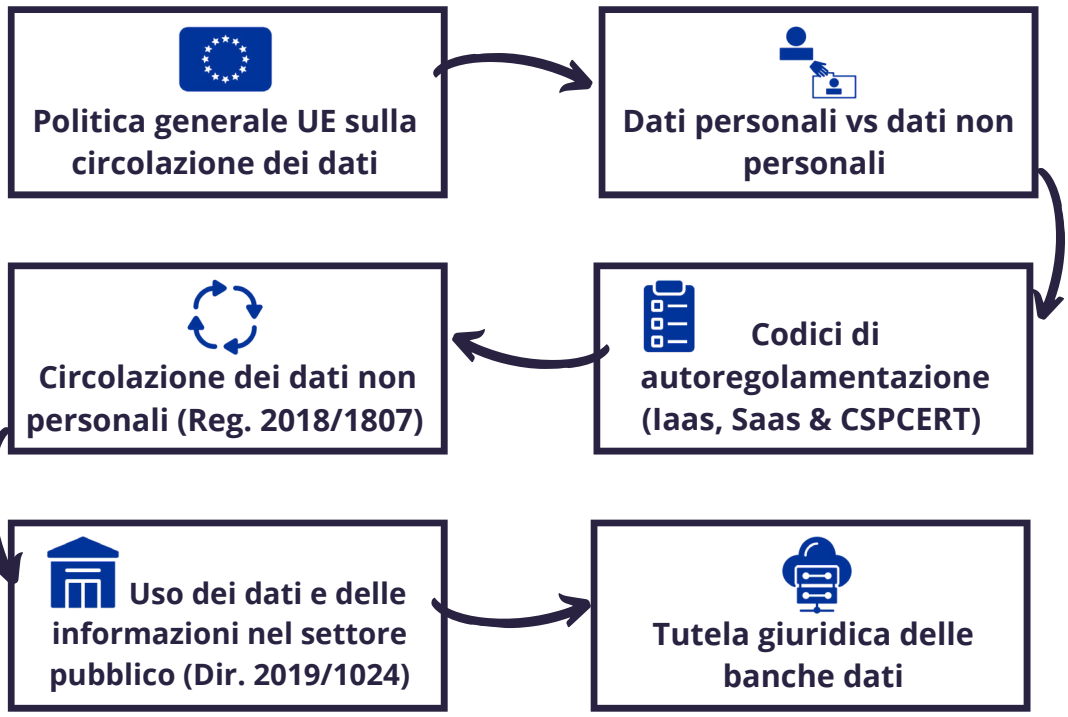
STEFANELLI & STEFANELLI STUDIO LEGALE

DATI NON PERSONALI

libera circolazione e sfruttamento economico

a cura di: Eleonora Lenzi, Ilaria Nanni

SOMMARIO



Dati personali e non personali: il quadro generale

Il rilevante ed incalzante processo di digitalizzazione che da tempo caratterizza l'economia mondiale, ha indotto negli ultimi anni l'Unione europea a valutare e conseguentemente a realizzare interventi legislativi incentrati sull'attuazione della politica europea dei dati.

La diffusione di servizi di Cloud Computing, l'Internet delle cose e la progettazione di sistemi di Intelligenza Artificiale hanno infatti spinto il legislatore europeo ad elaborare un complesso di norme che ogni giorno devono confrontarsi ed adeguarsi all'era digitale, cercando però sempre di rimanere per quanto possibile, al passo con il progresso tecnologico.

Lo sviluppo di strutture innovative ha consentito la creazione di una vera e propria "economia digitale", che necessariamente va ad intersecarsi con il tema dei flussi di dati e del relativo trattamento e circolazione dei dati personali e non personali.

L'innovazione tecnologica, "nutrita" da un'enorme massa di dati personali e non

personali, necessita per il proprio sviluppo della libera circolazione dei dati all'interno del territorio dell'Unione europea, senza che vengano posti ostacoli alla loro archiviazione, importazione/esportazione, e ciò al fine di consentire un passaggio più agevole tra infrastrutture e servizi cloud.

Negli ultimi anni, la Commissione europea, ha incentrato così il proprio intervento legislativo sull'esigenza di garantire la libera circolazione dei dati tra gli Stati membri, e ciò al solo scopo di creare un sistema di produzione e scambio di dati basato su tecnologie informatiche.

Attività di studio, consultazione e approfondimento da parte della Commissione europea hanno reso possibile la realizzazione di due importanti regolamenti, il primo (molto noto) del 2016 sui dati personali, il secondo (meno conosciuto ma non per questo meno importante) sui dati non personali:

- Regolamento (UE) 2016/679 (GDPR) relativo alla **protezione delle persone fisiche con riguardo al trattamento dei dati personali**, nonché alla **libera circolazione di tali dati**, che ha abrogato la precedente direttiva 95/46/CE sulla protezione dei dati;
- Regolamento (UE) 2018/1807 relativo al quadro applicabile alla **libera circolazione dei dati non personali** nell'Unione europea, che si applica dal 28 maggio 2019.

Come evidenziato nella comunicazione della Commissione al Parlamento europeo e al Consiglio del 25/05/2019 "grazie ai due regolamenti, i dati possono circolare liberamente tra gli stati membri, consentendo agli utenti dei servizi di trattamento di dati di utilizzare i dati raccolti nei diversi mercati dell'UE per migliorare la loro produttività e competitività".

In questa sede, preme in particolar modo approfondire le questioni relative ai dati non personali, la loro regolamentazione a livello europeo e i conseguenti riflessi nella cosiddetta "economia dei dati", come nel caso della disciplina dei rapporti tra fornitore di servizi cloud e cliente, della certificazione di sicurezza dei servizi, oppure della raccolta organizzata di dati in banche dati, con un focus sulla libera circolazione, sulle forme contrattuali utilizzabili e quindi sulle possibilità di sfruttamento a livello economico.

Dati personali e dati non personali: le differenze

DATI PERSONALI		DATI NON PERSONALI
Nessun limite o divieto alla circolazione dei dati per motivi attinenti alla protezione delle persone fisiche		Divieto degli obblighi di localizzazione dei dati Eccezione: sicurezza pubblica rispettando il principio di proporzionalità
Portabilità "business-to-consumer" tra interessato e titolare del trattamento		Portabilità "business-to-business" tra utente professionale e fornitore di servizi
Codici di condotta approvati dal Garante Privacy: 1) in materia di informazioni commerciali, 2) per i sistemi informativi 3) per l'utilizzo di dati sulla salute a fini didattici e di pubblicazione scientifica		Gruppo di lavoro SWIPO: sviluppo di due codici di condotta (IaaS e SaaS) + Creazione della certificazione di sicurezza dei servizi cloud (CSPCERT)

Le imprese situate sul territorio dell'Unione europea basano oggi gran parte delle loro attività su "flussi di dati", i quali in forza del rapido progresso tecnologico e della digitalizzazione, risultano indispensabili per la regolamentazione contrattuale e per l'individuazione di nuove opportunità economiche in diversi settori.

La politica comunitaria del Digital Single Market sta infatti favorendo la libera circolazione dei dati sia personali che non personali allo scopo di favorire e sviluppare la cosiddetta "economia dei dati"(per maggiori informazioni si veda il sito UE Costruire una economia dei dati).

Questo processo trova i suoi cardini in due importanti regolamenti:

- **regolamento (UE) 2016/679 relativo ai dati personali**

- **regolamento (UE) 2018/1807 relativo ai dati non personali**

Il primo di questi, noto anche come GDPR ("General Data Protection Regulation") fornisce una definizione intenzionalmente ampia di "dato personale", specificando che si tratta di «qualsiasi informazione riguardante una persona fisica identificata o identificabile».

Il regolamento relativo ai dati non personali invece, ricava la definizione degli stessi tramite un ragionamento a contrariis rispetto alla definizione di dati personali, indicando che per "dati non personali" si debbano intendere «i dati diversi dai dati personali (...)». Si tratta in particolare di dati che in origine non si riferiscono a una persona fisica identificata/identificabile, oppure di dati che inizialmente sorgevano come personali e successivamente sono stati resi anonimi. Per evidenziare tale differenza si può richiamare la COM (2019) 250 final intitolata "Guidance on the Regulation on a framework for the free flow of non personal data in the European Union" nella quale si afferma che «poiché la definizione di dati personali si riferisce alle "persone fisiche", gli insiemi di dati che contengono i nomi e i dati di contatto delle persone giuridiche sono in linea di principio dati non personali». Ciò non toglie che nel trattare il dato della persona giudica, si finisca quasi sempre con il trattare anche i dati delle persone fisiche che operano per la persona giuridica.

Spesso accade, quindi, che dati personali e non personali siano raccolti in un insieme di dati misti (es. i dati sanitari). Preme poi precisare che ove sia possibile una separazione potranno essere applicate le normative di riferimento per ciascun insieme di dati (personali e non personali), laddove invece, l'insieme di dati misti contenga dati che tra loro risultino "indissolubilmente legati", l'art. 2, par. 2 del regolamento (UE) 2018/1807 prevede che si applichi il GDPR all'intero set di dati misti, anche nei casi in cui i dati personali ne rappresentino solo una minima parte.

Ma che rapporto sussiste tra i due Regolamenti?

In seguito, affronteremo tre temi che reputiamo cardine, analizzando brevemente i punti di contatto o le principali differenze tra il regolamento sui dati personali e quello sui dati non personali.

La libera circolazione dei dati

Certamente, il dato comune tra i due regolamenti è la costante promozione del principio

di libera circolazione dei dati all'interno del territorio dell'Unione europea, il quale però vede l'apposizione di limiti differenti:

- il regolamento sui dati non personali si basa sul principio del libero flusso transfrontaliero di dati personali e quindi sul divieto per gli Stati di imporre "obblighi di localizzazione" dei dati «(...) a meno che non siano giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità». Inoltre, le norme del regolamento non si applicheranno qualora le attività di trattamento dei dati siano condotte al di fuori del territorio dell'UE.
- il regolamento sui dati personali dispone invece che la libera circolazione dei dati all'interno del territorio dell'Unione non possa essere limitata né vietata «per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali», e che le norme relative al trasferimento dei dati si applicheranno anche nelle interazioni verso paesi terzi ma impone importanti restrizioni al trasferimento dei dati personali verso Stati fuori dal territorio dell'UE o che non garantiscano un livello adeguato di protezione dei dati.

La portabilità dei dati

Entrambi i regolamenti disciplinano la portabilità dei dati mirando a facilitarne il loro trasferimento, e ciò al fine di evitare pratiche di "vendor lock-in", che si verificano quando gli utenti non possono cambiare il fornitore di servizi perché i dati risultano bloccati nel sistema del fornitore.

Il diritto alla portabilità dei dati assume connotazioni differenti a seconda che si tratti di:

- **dati personali**, nei quali la portabilità si riferisce al rapporto tra l'interessato e il titolare del trattamento, quindi in un rapporto "business-to-consumer";
- **dati non personali**, nei quali invece la portabilità dei dati riguarda le interazioni "business-to-business" intercorrenti tra un utente professionale e un fornitore di servizi.

I codici di autoregolamentazione

L'Unione europea attraverso i regolamenti sui dati personali e non personali incoraggia la redazione e la successiva adozione di codici di condotta e sistemi di certificazione nei diversi settori economici. I codici possono essere elaborati da associazioni di categoria,

organizzazioni rappresentative o da responsabili del trattamento, sebbene nel settore relativo i dati personali, necessitino di un processo di approvazione da parte del Garante Privacy ai sensi degli artt. 40 e 41 del GDPR.

Tra i codici di condotta nell'ambito dei dati non personali è possibile menzionare quelli elaborati dal gruppo di lavoro SWIPO, come i codici IaaS o SaaS (la cui adesione è totalmente volontaria).

Per quanto riguarda invece i dati personali, ad oggi sussistono tre codici approvati dal Garante Privacy: "Per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti", quello "Per il trattamento dei dati personali effettuato a fini di informazione commerciale", e quello di recente approvazione "Per l'utilizzo di dati sulla salute a fini didattici e di pubblicazione scientifica" proposto dalla Regione Veneto.

Dati personali: i contratti per fini commerciali

La politica comunitaria del Digital Single Market favorisce la libera circolazione dei dati allo scopo di sviluppare la cosiddetta "economia dei dati"; alla luce di ciò occorre approfondire "come" circolano i dati o in altre parole se i dati possono essere oggetto di controprestazione contrattuale.

La domanda da porsi è quindi: l'**autorizzazione al trattamento di dati personali rilasciata dall'Interessato può essere il corrispettivo per un bene o un servizio?**

Il tema è oggetto oggi di ampio dibattito.

Con le Direttive 770/2019, 771/2019 e 2161/2019 l'Unione europea risponde in modo affermativo, stabilendo esplicitamente che **il cittadino può autorizzare il trattamento di propri dati come corrispettivo per la fruizione di un contenuto digitale o un servizio digitale**.

Il riconoscimento del trasferimento di dati personali e l'autorizzazione al trattamento per fini commerciali diventano dunque "controprestazione contrattuale", al pari del pagamento in denaro, tanto è vero che l'utente che abbia "pagato" permettendo l'acceso ai propri dati personali, ai sensi della Dir. UE 2019/770, potrà azionare tutti i rimedi previsti dalla disciplina consumeristica in caso di mancata fornitura o di difetto del servizio o del contenuto digitale, quali, ad esempio, il recesso, la riduzione del prezzo, il risarcimento.

Si parla pertanto di "**contratti di dati personali**".

Occorre allora domandarsi quale disciplina civilistica nazionale può ritenersi applicabile a tali contratti.

Ad una prima analisi sembra che nessuno degli istituti noti del diritto civile sia del tutto adeguato a disciplinare il contratto di dati.

Non la vendita (art. 1470 c.c. "La vendita è il contratto che ha per oggetto il trasferimento della proprietà di una cosa o il trasferimento di un altro diritto verso il corrispettivo di un prezzo") e neppure l'appalto di servizi (art. 1655 c.c. "L'appalto è il contratto con il quale una parte assume, con organizzazione dei mezzi necessari e con gestione a proprio rischio, il

compimento di un'opera o di un servizio verso un corrispettivo in danaro"); entrambi gli istituti contrattuali nelle definizioni sia del codice civile che del codice del consumo prevedono il pagamento di un prezzo.

La normativa europea al contrario esclude espressamente la mercificazione dei dati: la Dir. UE 770/2019 sancisce infatti "Oltre a riconoscere appieno che la protezione dei dati personali è un diritto fondamentale e che tali dati non possono dunque essere considerati una merce, la presente direttiva dovrebbe garantire che i consumatori abbiano diritto a rimedi contrattuali, nell'ambito di tali modelli commerciali". Tale previsione osta al fatto di poter considerare il trasferimento dei dati come "prezzo" e quindi di poter applicare l'istituto della vendita o dell'appalto di servizi.

Anche la permuta definita dal codice civile all'art. 1552 come "il contratto che ha per oggetto il reciproco trasferimento della proprietà di cose o di altri diritti, da un contraente ad un altro", non appare del tutto idoneo a disciplinare il contratto di dati; l'utente, infatti, nei contratti di dati non trasferisce la proprietà dei propri dati personali quanto piuttosto ne consente l'accesso ed il trattamento alla controparte contrattuale.

Si potrà quindi pensare ad un contratto "atipico" ovvero ad un contratto che non appartiene ad una fattispecie determinata, ma che è comunque diretto a realizzare interessi meritevoli di tutela secondo l'ordinamento giuridico.

Proprio perché si tratta di un contratto atipico, appare assolutamente rilevante (sia per ragioni di trasparenza che per ragioni di valore giuridico) che il contratto stesso **sia disciplinato in modo esaustivo nelle Condizioni generali di contratto che il prestatore di servizi digitali sottoporrà all'utente, tenendo ben a mente due concetti**

- certamente il contratto di dati rientra nell'ambito della disciplina consumeristica e, se concluso tramite i servizi della società dell'informazione, in quella specifica delle vendite a distanza: andranno quindi applicate le relative discipline del Codice del Consumo
- il consumatore dovrà essere reso edotto del fatto che il servizio o il contenuto digitale NON sono affatto gratuiti, in quanto la "controprestazione" è data appunto dal rilascio dei dati e dall'autorizzazione al loro utilizzo commerciale.

Questi due punti trovano conferma certa non solo nella disciplina delle Direttive del 2019, il cui recepimento è previsto entro l'anno, ma anche dalla recente sentenza del Consiglio di Stato (Facebook vs AGCM n. 2630 del 29/3/2021), in cui i giudici affermano l'ingannevolezza e la scorrettezza commerciale di FB insita nel presentarsi agli utenti come gratis mentre, in realtà, si fa pagare in dati personali che sfrutta poi nella dimensione commerciale.

Dati non personali: disciplina applicabile nella UE

I dati non personali costituiscono, unitamente ai dati personali, uno strumento rilevante per lo sviluppo dell'economia digitale all'interno del Digital Single Market.

Sebbene infatti la definizione di "dati non personali" sia ricavata tramite un ragionamento a contrariis rispetto a quella di "dati personali", si tratta comunque di importanti mezzi attraverso i quali favorire il libero flusso dei dati all'interno di un'economia sempre più caratterizzata dalla digitalizzazione.

Al fine di identificare i dati non personali, essi possono essere qualificati in base alla loro origine:

- **dati anonimi ex-ante**: ossia dati che in origine non si riferiscono ad una persona fisica identificata o identificabile;
- **dati anonimi ex-post**: ovvero dati che inizialmente erano personali e che successivamente sono stati resi non personali attraverso un processo di anonimizzazione.

L'intelligenza artificiale, l'analisi dei megadati, i dati generati nel quadro di processi aziendali ed i dati sull'agricoltura di precisione, costituiscono solo alcuni esempi di fonti di dati non personali.

Negli ultimi anni, grazie allo sviluppo tecnologico, le aziende e le pubbliche amministrazioni non hanno più avuto solo contatti con il mondo dei dati personali, ma bensì hanno iniziato ad interfacciarsi anche con la raccolta e l'utilizzo dei dati non personali, necessitando di conseguenza una regolamentazione della materia.

L'Unione europea ha risposto a questa esigenza attraverso l'elaborazione del Regolamento (UE) 2018/1807 "relativo al quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea".

Tale Regolamento, la cui applicazione decorre già dal 28 maggio 2019, risulta essenziale e presenta due principali obiettivi: da un lato, garantire che i dati non personali possano essere trattati liberamente su tutto il territorio dell'UE, dall'altro lato, vietare le restrizioni alla circolazione dei dati non personali sui luoghi in cui i dati possono essere archiviati o

elaborati.

All'interno del Regolamento relativo ai dati non personali, possono essere altresì facilmente individuati tre capisaldi:

1. Il principio della libera circolazione dei dati all'interno dell'Unione europea

L'art. 4 del Regolamento sancisce il divieto degli obblighi di localizzazione dei dati, a meno che non siano giustificati da motivi di pubblica sicurezza e il tutto nel pieno rispetto del principio di proporzionalità.

L'articolo in esame fissa poi la "deadline" al 30 maggio 2021 per lo svolgimento delle seguenti attività:

- da un lato, gli Stati membri dovranno abrogare qualsiasi obbligo di localizzazione dei dati vigente stabilito dalle leggi nazionali, dai regolamenti o da disposizioni amministrative non conformi al principio generale della libera circolazione dei dati;
- dall'altro lato, si invitano gli Stati membri che ritengono sussistenti misure contenenti obblighi di localizzazione dei dati, a comunicare tali misure alla Commissione europea al fine di giustificare l'eventuale richiesta di mantenimento in vigore, purché ciò avvenga nel rispetto del principio di proporzionalità o per motivi di pubblica sicurezza.

2. Il principio della disponibilità dei dati per le autorità competenti

L'art. 5 del Regolamento prevede il generico principio di "messa a disposizione di dati alle autorità competenti", le quali potranno esercitare il diritto di accesso ai dati indipendentemente dal luogo di archiviazione o elaborazione degli stessi all'interno dell'Unione europea.

Gli stati membri possono inoltre imporre sanzioni laddove sia violato il rispetto di un obbligo di fornire dati conformemente al diritto nazionale e dell'UE.

3. La realizzazione di codici di condotta

La Commissione europea, attraverso l'art. 6 incoraggia e facilita la redazione di codici di autoregolamentazione, e ciò al fine di favorire:

- l'agevolazione del cambio di fornitore di servizi e la portabilità dei dati in formato strutturato;
- gli obblighi di informazione minimi, necessari prima della conclusione di un contratto di trattamento dati;
- gli approcci in materia di sistemi di certificazione, in materia di gestione della qualità, della sicurezza delle informazioni, della continuità operativa e della gestione ambientale;
- tabelle di marcia in materia di comunicazione, volte a sensibilizzare i portatori di interessi relativamente ai codici di condotta.

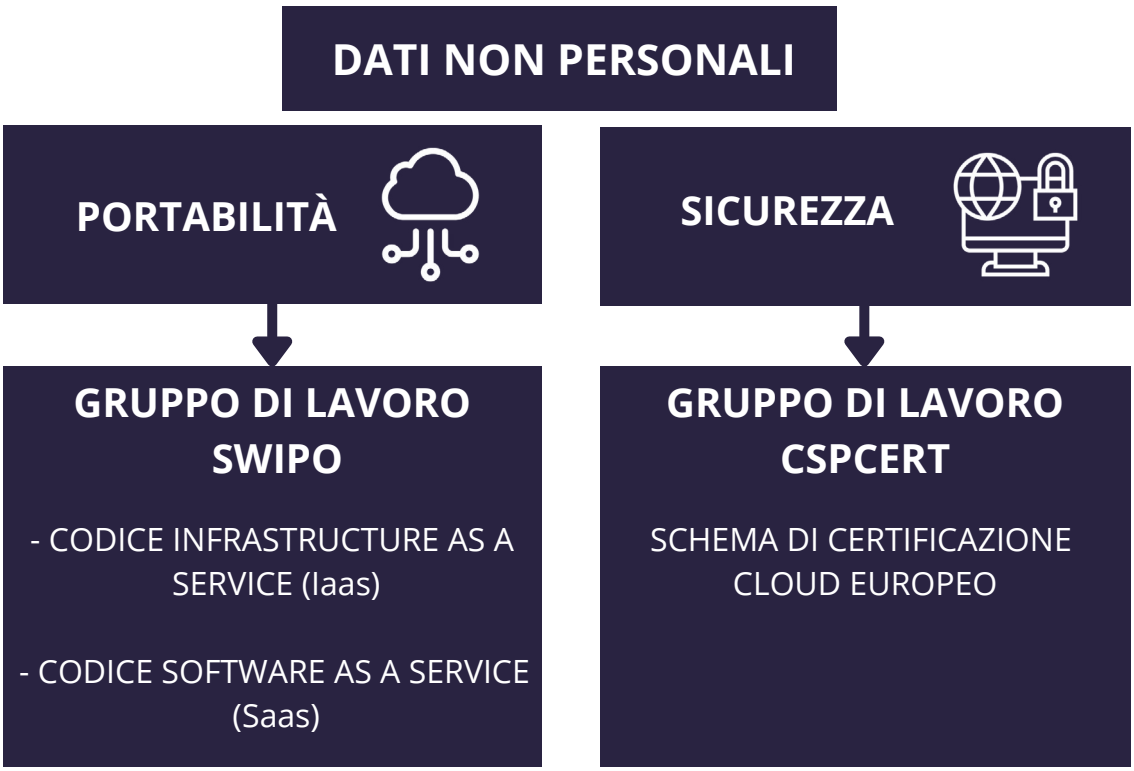
Quali sono le prospettive future in materia di dati non personali?

È lo stesso Regolamento sui dati non personali che all'art. 8 fissa il termine ultimo del 29 novembre 2022 entro il quale la Commissione europea dovrà presentare al Parlamento, al Consiglio e al Comitato economico e sociale europeo una relazione sulla corretta attuazione del Regolamento, e in particolare sulle seguenti questioni:

- l'applicazione del Regolamento agli insiemi di dati c.d. misti, ossia composti da dati personali e non personali;
- l'attuazione da parte degli Stati membri del principio di libero flusso dei dati;
- l'elaborazione e l'effettiva attuazione dei codici di autoregolamentazione da parte degli Stati membri.

Non ci resta dunque che attendere per verificare se gli sviluppi del mercato, l'economia dei dati e le crescenti esigenze di trattazione dei dati a livello contrattuale potranno effettivamente indurre la Commissione europea ad apportare modifiche al Regolamento (UE) 2018/1807.

Dati non personali: valore economico, sicurezza e portabilità. Codici di condotta e certificazioni



I dati costituiscono per l'Unione europea una priorità fondamentale per la crescita economica e lo sviluppo dell'economia digitale. In quest'ottica, i servizi cloud rappresentano l'asse centrale per estrarre il valore economico dai dati, memorizzandoli e condividendoli.

In tal senso, il Regolamento (UE) 2018/1807 in materia di dati non personali, promuove all'art. 6 l'elaborazione di codici di autoregolamentazione (c.d. codici di condotta), con l'intento di "contribuire a un'economia dei dati competitiva basata sui principi della trasparenza e dell'interoperabilità (...)".

A tal fine, nell'ambito della portabilità dei dati non personali, la Commissione europea ha fissato i seguenti obiettivi:

- ridurre il rischio di blocco dei fornitori di servizi Cloud (c.d. vendor lock-in),

- rendere più fluido il mercato europeo dei servizi Cloud,
- consentire anche alle piccole imprese e ai nuovi operatori del mercato di competere in tale ambito,
- individuare obblighi di informazione minimi, aumentando in questo modo la fiducia dei clienti dei servizi Cloud,
- favorire gli approcci in materia di sistemi di certificazione, in materia di gestione della qualità, della sicurezza delle informazioni, della continuità operativa e della gestione ambientale.

In particolare, la Commissione europea ha individuato due gruppi di lavoro, rispettivamente per l'elaborazione dei codici di autoregolamentazione e per lo sviluppo della certificazione di sicurezza dei servizi cloud:

- Gruppo di lavoro SWIPO - Switching from Provider and Porting non-personal data
- Gruppo di lavoro CSPCERT WG - Cloud Service Provider Certification Working Group.

Gruppo di lavoro SWIPO

Il gruppo SWIPO AISBL è un'associazione multi-stakeholder composta da fornitori di servizi cloud (CSP – Cloud service Provider) e clienti (CSC – Cloud service Customer).

Dopo due anni di lavoro, il gruppo SWIPO ha annunciato la pubblicazione di due codici di condotta: uno sulla portabilità dei dati e uno sul Cloud switching, ottenendo, come evidenziato in un articolo del 12 maggio 2021 pubblicato sul sito swipo.eu, un totale di ventuno dichiarazioni di adesione da parte dei fornitori di servizi Cloud.

Nello specifico il tema della portabilità è affrontato nel Codice dei servizi cloud Infrastructure as a service (Iaas) e quelle del cloud switching in quello dei servizi cloud Software as a service (Saas); gli stessi sono stati presentati per la prima volta in occasione della conferenza sull'economia dei dati tenutasi ad Helsinki al termine dell'anno 2019, con lo scopo di fornire una guida volontaria per i Cloud Provider e i Clienti Cloud, e soprattutto per favorire un maggiore flusso e portabilità dei dati in ottemperanza al Regolamento sui dati non personali.

Entrambi i Codici prevedono l'adesione da parte degli operatori del settore in maniera del tutto volontaria, e non si sostituiscono al cosiddetto "Cloud service agreement" (CSA), ossia un accordo formale tra il fornitore e il cliente di servizi cloud, con il quale vengono definite le modalità attraverso cui verrà fornito il servizio Cloud.

Gruppo di lavoro CSPCERT

Il gruppo CSPCERT è stato creato con l'obiettivo di sviluppare uno schema di certificazione Cloud europeo nel contesto della legge sulla sicurezza informatica e di fornire alla Commissione europea e all'ENISA (European Union Agency for Cybersecurity) una serie di raccomandazioni che dovranno essere prese in considerazione nell'implementazione dello schema di certificazione del Cloud.

L'idea alla base della certificazione dei servizi Cloud non è quella di proporre alla Commissione europea un modello completamente nuovo, ma bensì quella di fornire uno schema basato su pratiche e standard già esistenti e utilizzati nel settore.

La proposta definitiva elaborata dal CSPCERT WG è stata finalizzata il 7 giugno 2019, e successivamente presentata alla Commissione europea e all'ENISA i successivi 12 e 13 giugno.

Il testo finale presentato dal gruppo di lavoro, contiene "raccomandazioni per l'implementazione dello schema di certificazione CSP", e nello specifico può essere suddiviso in tre documenti principali:

1. Il primo documento analizza l'elaborazione degli obiettivi di sicurezza che uno schema di certificazione a livello europeo deve includere. Questi obiettivi di sicurezza si basano sull'analisi degli standard, dei sistemi e delle buone pratiche esistenti;

2. Il secondo documento disciplina invece l'analisi comparativa delle metodologie di valutazione della conformità più rilevanti, i loro approcci ed i loro elementi distintivi;

3. Infine, il terzo documento elabora i documenti precedenti, i risultati della consultazione aperta tenutasi durante gennaio - febbraio 2019 e fornisce contenuti aggiuntivi sotto forma di raccomandazioni per la Commissione europea e l'ENISA. Tra le raccomandazioni generali del CSPCERT WG formulate alla Commissione europea, è possibile evidenziare quella di:

- includere lo sviluppo di uno schema di certificazione della sicurezza del cloud a livello di UE nel programma di lavoro a rotazione dell'Unione europea per la certificazione della sicurezza informatica europea ai sensi della legge sulla sicurezza informatica;
- chiedere all'ENISA di preparare uno schema sulla base della proposta presentata dal gruppo di lavoro, come parte dell'esecuzione di tale programma di lavoro a rotazione dell'Unione.

In conclusione, come stabilito nel Regolamento europeo sui dati non personali, la Commissione europea valuterà l'impatto e l'effettiva attuazione dei codici di condotta entro il 29 novembre 2022. Questa attività valutativa si concentrerà in particolare sugli effetti che i codici di condotta avranno sulla fluidità e la competitività del mercato del Cloud per quanto riguarda i codici elaborati dal gruppo di lavoro SWIPO, e sull'esatto coordinamento con la legge in materia di cybersecurity per il gruppo di lavoro CSPCERT.

Open Data: riutilizzo da parte degli operatori economici

La quantità di dati generati in tutto il mondo sta aumentando in questi anni in maniera esponenziale. Al fine di garantire maggiore trasparenza, collaborazione e vicinanza ai cittadini, l'Unione europea ha avviato un processo di cambiamento dello scenario pubblico, incentrato sui c.d. Open Data.

Come evidenziato nel portale dell'Unione europea nella sezione "EU Vocabularies", quando parliamo di Open Data intendiamo la "pratica di pubblicazione di dati (grezzi) in modo che siano accessibili, riutilizzabili, leggibili con dispositivi elettronici e concessi in licenza liberamente. Possono essere generati da un'ampia gamma di soggetti, tra le pubbliche autorità, settore parastatale, imprese e il pubblico".

Si tratta dunque di dati accessibili a tutti, messi a disposizione da Pubbliche Amministrazioni o aziende private che possono essere riutilizzati da persone fisiche o giuridiche per diversi scopi, tra cui l'implementazione dei propri modelli di business o la semplice individuazione di modelli nuovi, o altresì per scopi di ricerca, giornalismo, sviluppo o universitari.

La finalità della pubblicazione dei dati per soli fini di trasparenza amministrativa è stata infatti nel tempo progressivamente sostituita in favore di un riutilizzo dei dati aperti della PA. Ciò è avvenuto soprattutto in riferimento ai c.d. dati dinamici, consistenti in documenti in formato digitale soggetti ad aggiornamenti frequenti o in tempo reale, come ad esempio i dati meteorologici, ambientali, oppure relativi al traffico stradale, il cui valore economico dipende dall'immediata disponibilità e dal costante aggiornamento.

Il passaggio verso lo sfruttamento economico delle informazioni messe a disposizione dalla PA si è concretizzato con l'emanazione della Direttiva 2003/98/CE c.d. Public Service Information Directive (Direttiva PSI), in materia di riutilizzo dei dati della PA dai soggetti che ne facciano richiesta, poi attuata in Italia con il d.lgs. 36/2006 con il quale è stato avviato anche nel territorio italiano un processo di forte promozione al riutilizzo dei dati della Pubblica Amministrazione.

La Direttiva del 2003, poi in parte modificata da una successiva Direttiva del 2013 (Direttiva 2013/37/UE), è stata rifusa nella più recente Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio, volta all'introduzione della nuova disciplina sull'apertura dei dati

e il riutilizzo delle informazioni nel settore pubblico.

L'apertura dei dati viene infatti ampiamente stimolata ed incoraggiata dall'Unione europea al fine di:

- garantire la trasparenza della pubblica amministrazione,
- assicurare maggiore collaborazione e innovazione,
- consentire lo sfruttamento economico dei dati, con conseguente beneficio per l'economia.

La Direttiva affronta diverse tematiche al riguardo, tra cui è possibile menzionare:

Il riutilizzo dei dati (art.1 e art.4)

La Direttiva, detta un complesso di norme minime in materia di riutilizzo e modalità pratiche per agevolare il riutilizzo dei:

- documenti esistenti in possesso degli enti pubblici degli Stati membri,
- documenti esistenti in possesso delle imprese pubbliche,
- dati della ricerca (conformemente alle condizioni di cui all'art.10)
- dati di elevato valore (alle condizioni di cui all'art. 14).

Al fine di poter accedere ai dati e successivamente riutilizzarli, ai soggetti interessati basterà inoltrare una richiesta agli enti pubblici, i quali la esamineranno e metteranno i documenti a disposizione del richiedente ove possibile per via elettronica. Va sottolineato che gli enti pubblici dovranno comunicare al richiedente le motivazioni in caso di decisione negativa circa la richiesta di riutilizzo, e ciò sulla base delle disposizioni del regime di accesso nello Stato membro di riferimento.

Formati disponibili (art. 5)

L'Unione europea incoraggia gli enti pubblici a gestire i dati in un formato che permetta la portabilità al fine di promuoverne la libera circolazione attraverso lo scambio di dati in una dimensione strutturata e comune. Nello specifico, la Direttiva del 2019 vede

l'applicazione di questo principio attraverso la messa a disposizione da parte di enti ed imprese pubbliche di documenti in qualsiasi lingua o formato preesistente, incoraggiando all'apertura dei dati fin dalla progettazione e per impostazione predefinita.

La fornitura di tali informazioni, in un formato preferibilmente elettronico di uso comune, consentirà ai cittadini e alle imprese di individuare nuovi modi di utilizzarle e di creare prodotti e servizi sempre innovativi.

Tariffe (art. 6)

Il riutilizzo dei documenti/dati è completamente gratuito. Tuttavia, i costi marginali sostenuti per la riproduzione, messa a disposizione e divulgazione dei documenti, nonché per l'anonimizzazione di dati personali o per le misure adottate per proteggere le informazioni commerciali a carattere riservato, possono essere recuperati.

Licenze standard (art. 8)

In linea di principio, il riutilizzo dei dati non è soggetto a condizioni, a meno che tali condizioni non siano obiettive, proporzionate, non discriminatorie e giustificate sulla base di un obiettivo di interesse pubblico. La Direttiva europea dispone altresì che anche laddove il riutilizzo sia subordinato a condizioni, esse non dovranno limitare la concorrenza e ridurne le possibilità di riutilizzo.

Quali prospettive per il futuro?

La Direttiva UE 2019/1024 ha fissato il termine del 17 luglio 2021 per attuare le disposizioni legislative, regolamentari e amministrative in materia di dati e riutilizzo dell'informazione nel settore pubblico.

Nello specifico, per quanto concerne il panorama italiano, la Direttiva è stata recentemente inclusa tra gli atti di recepimento mediante la Legge di delegazione europea 2019-2020 (L. 22 aprile 2021, n. 53) con la quale è stato delegato il Governo al recepimento delle direttive e l'attuazione degli altri atti dell'Unione europea.

Il recepimento della Direttiva da parte dei singoli Stati membri costituirà un'importante opportunità per la diffusione degli Open Data presso gli operatori economici di svariati

settori. Infatti, maggiore sarà la qualità degli Open Data messi a disposizione dalla PA, e maggiori saranno le probabilità che i dati verranno utilizzati al fine di creare servizi innovativi e implementare il settore della ricerca.

Open Data: licenze per il riuso

La data driven innovation

L'espressione Data Driven Innovation identifica una politica economica legata all'uso di dati e statistiche per migliorare o favorire la creazione di nuovi prodotti, processi, sistemi organizzativi o mercati; dati relativi non solo alle attività ed alle abitudini degli utenti in rete ma anche a tutta quella massa di dati raccolti quotidianamente da dispositivi wearable, cellulari, macchine intelligenti, macchine industriali, sistemi di videosorveglianza nonché dalle pubbliche amministrazioni.

In realtà la realizzazione di una politica di sviluppo legata all'analisi ed all'impiego dei dati, non può prescindere dalla messa a disposizione dei dati detenuti dalle pubbliche amministrazioni, i c.d. Open Data.

Sullo sviluppo della politica in materia di riutilizzo degli Open Data abbiamo, analizziamo ora brevemente quali possono essere le tipologie di licenze utilizzate per la messa a disposizione dei dati.

Il principio della gratuità dei dati

Il principio cardine che permea l'intera disciplina degli Open Data, confermato anche dalla recente Direttiva 2019/1024 è quello della gratuità dei dati; le informazioni gestite dalle pubbliche amministrazioni per i loro fini istituzionali non possono essere trattate alla stregua di beni delle stesse PP.AA. da cui trarre un utile, per cui la richiesta di un eventuale corrispettivo per il loro riutilizzo è giustificata solo nei limiti della necessità di coprire i costi sostenuti per la riproduzione, la messa a disposizione e la divulgazione dei dati. L'eventuale costo pertanto deve essere legato unicamente alla qualità del servizio reso ovvero alla possibilità di accedere ai dati in un formato aperto.

Open data by default

L'art. 52 del CAD (Codice Amministrazione Digitale) stabilisce che "i dati e i documenti che le amministrazioni titolari pubblicano senza l'espressa adozione di una licenza si intendono rilasciati come dati di tipo aperto".

Sulla base di questo principio quando una amministrazione decide di pubblicare un dato si presume che quel dato sia liberamente utilizzabile senza alcuna limitazione.

Le amministrazioni possono prevedere l'uso di licenze solo se ciò si rende necessario per il rispetto di altre normative, come il GDPR, la tutela dei segreti commerciali ed industriali e comunque motivando la scelta.

Le tipologie di licenze

Le linee guida del 2017 dell'AgID indicano alcune tipologie di licenze standard, che prevedono che i dati resi disponibili in formato open dalle PP.AA. possono essere licenziati con richiesta di attribuzione della paternità dei dati e, eventualmente, con la richiesta di ri-condivisione dei dati sempre in formato aperto.

Le licenze che impongono di indicare la paternità dei dati permettono al licenziatario di copiare, distribuire ed esporre al pubblico i dati nonché di modificarli anche per fini commerciali, con l'unico obbligo di indicare la paternità dei dati, fornendo un link alla licenza ed indicando le eventuali modifiche apportate; si tratta delle c.d. Licenze Creative Commons – Attribuzione (CC-BY). Il licenziatario dovrà indicare l'amministrazione titolare dei diritti, il tipo di documento che è stato riutilizzato, l'autore delle eventuali modifiche (mashup) così da non creare confusione rispetto all'origine del documento.

Le licenze che impongono anche di ri-condividere in formato aperto i dati elaborati ammettono il riutilizzo dei dati anche a fini commerciali a condizione che la distribuzione degli eventuali lavori derivati segua la medesima identica licenza che governa i dati di partenza.

In Italia sono state elaborate due tipologie di licenze nazionali

- IODL versione 2.0 che permette al licenziatario di riutilizzare i dati e creare un lavoro derivato utilizzando vari dataset,
- IODL versione 1.0 che impone l'obbligo per il licenziatario di pubblicare e condividere i lavori derivati con la stessa licenza.

Infine, per consentire la reale fruizione di rilevanti masse di dati è necessario che le PP.AA. mettano a disposizione dati di qualità, che siano chiari, aggiornati, precisi e comprensibili (principi sanciti a livello internazionale dal G8 Open Data Charter).

Banche dati: la tutela giuridica tra diritto d'autore e diritto sui generis

Realizzare un database richiede investimenti in termini di tempo, di organizzazione nonché di risorse finanziarie: è quindi importante fornire all'autore una serie di tutele giuridiche che gli permettano lo sfruttamento economico della propria opera in via esclusiva; a ciò si aggiunge la necessità di dare regole che permettano di condizionare gli accessi ai dati raccolti, soprattutto alla luce dell'ampio numero di informazioni e di dati personali o non personali contenuti in banca dati.

Esaminiamo allora le tutele messe a disposizione dal nostro ordinamento.

Cosa si intende per banca dati

Le banche dati sono definite ai sensi dell'art. 1 della Direttiva 96/9/CE come una "raccolta di opere, dati, o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo".

In altre parole, le banche dati o base di dati (più comunemente conosciute con il termine inglese di database) rappresentano una raccolta di dati strutturati e memorizzati su un supporto elettronico, create da un soggetto definito "autore", che può essere persona fisica e anche giuridica (laddove la legislazione dello Stato membro dell'Unione europea lo consenta - art. 4 direttiva).

Le banche dati saranno poi tutelate solo ove presentino un carattere di originalità.

Il concetto di originalità

Come evidenziato dalla Corte di Giustizia dell'Unione europea nella causa C-604/10, l'originalità della banca dati potrà risultare:

1. dalla scelta dei materiali inseriti nell'opera, avendo particolare riguardo ad eventuali precedenti raccolte aventi i medesimi contenuti (banche dati selettive),

2. dalla scelta delle modalità di disposizione dei materiali all'interno dell'opera (banche dati non selettive).

Nella seconda ipotesi si terrà in considerazione la disposizione originale del materiale attraverso la necessaria osservazione di due concetti:

- coordinamento (c.d. Coordination) inteso come i collegamenti sussistenti fra i vari dati,
- organizzazione (c.d. Arrangement) che prevede un determinato ordine sequenziale di disposizione dei dati, come ad esempio dal punto di vista dell'oggetto oppure a livello cronologico o tematico.

Quale disciplina è prevista dal nostro ordinamento per la tutela giuridica delle banche dati?

La Direttiva 96/9/CE in materia di banche dati è stata recepita poi Italia con il D.lgs. 6 maggio 1999, n. 169: tale decreto di fatto ha introdotto modifiche alla legge 22 aprile 1941, n. 633 sul diritto d'autore per allinearla alla Direttiva sopra citata.

La Direttiva (e in linea la nostra legge sul diritto d'autore) differenzia la tutela a seconda che alla banca dati venga riconosciuto o meno il carattere dell'originalità: più esattamente si distingue tra diritto d'autore (artt. 3-6) e diritto sui generis (art. 7-11):

a) diritto d'autore

Se la banca dati è una creazione intellettuale originale, è possibile proteggerla mediante il diritto d'autore, il quale conferisce il diritto esclusivo di riprodurre, adattare, distribuire la banca dati o variazioni della stessa.

La Corte di Giustizia dell'Unione europea, sempre nella causa C-604/10, ha sottolineato che il criterio dell'originalità richiesto ai fini della tutela, può ritenersi soddisfatto quando l'autore della banca dati:

- esprime la sua capacità creativa con originalità
- effettua scelte libere e creative

Affinché l'autore della banca dati possa beneficiare della tutela prevista dalla legge sul diritto d'autore (e successive modifiche), non è richiesta alcuna procedura particolare: chi crea un'opera letteraria, scientifica o artistica è infatti automaticamente tutelato dal diritto d'autore, che avrà inizio dal momento della creazione dell'opera fino a 70 anni dalla

morte dell'autore.

Il diritto d'autore tutelerà poi esclusivamente la struttura della banca dati e non si estenderà ai suoi contenuti, lasciando impregiudicati eventuali diritti esistenti su di essi.

Per rendere poi chiaro e conoscibile a tutti la sussistenza del diritto, è possibile apporre sull'opera un avviso sul copyright, come, ad esempio, il testo "tutti i diritti riservati", oppure il simbolo © seguito dall'anno di creazione dell'opera, attraverso il quale verranno conseguentemente conferiti i seguenti diritti esclusivi:

- diritti economici: garantiscono il controllo sull'opera e una retribuzione in caso di uso tramite vendita o licenza,
- diritti morali: generalmente tutelano i diritti di rivendicare la paternità dell'opera (diritto di attribuzione) e di respingere eventuali modifiche (diritto di integrità).

b) diritto sui generis

Se la scelta dei materiali o la struttura della banca dati non rappresentano invece una creazione originale, è comunque possibile proteggerne i contenuti attraverso il diritto sui generis.

Si tratta di un diritto totalmente svincolato dal carattere creativo od originale della banca dati, esercitabile solo se la banca dati è frutto di un investimento ingente: in sostanza non si portegge la creatività, ma l'investimento economico.

Così anche la giurisprudenza intervenuta la quale ha stabilito che il diritto sui generis potrà essere invocato dall'autore qualora "il conseguimento, la verifica o la presentazione del loro contenuto abbia richiesto un investimento rilevante sotto il profilo qualitativo o quantitativo" di natura finanziaria, materiale e/o professionale (Corte di Giustizia UE C-604/10).

Sulle finalità della tutela prevista dal diritto sui generis e sulla corretta determinazione dei suoi "confini" ha avuto modo di pronunciarsi recentemente la Corte di Giustizia nella sentenza C-762/19 del 3/6/2021, oggetto di un nostro commento (si veda l'articolo "Motori di ricerca in internet e tutela delle banche di dati: una recente sentenza della Corte di Giustizia Europea").

La durata del diritto del costitutore della banca dati è di 15 anni, decorrenti dal 1° gennaio dell'anno successivo alla data del completamento della raccolta e rinnovabile in caso di modifiche o integrazioni sostanziali apportate alla banca dati.

Infine, risulta importante evidenziare che il diritto d'autore e il diritto sui generis possono in ogni caso applicarsi cumulativamente se le condizioni di protezione di ciascun diritto sono soddisfatte.

Quali prospettive future?

A causa del processo di digitalizzazione e del continuo mutamento degli scenari di raccolta ed archiviazione di informazioni e di dati personali e non personali (si pensi ad esempio alla raccolta dei Big Data), la Direttiva 96/9/CE sulle banche dati non può più ritenersi attuale ed allineata alle esigenze correnti, evidenziando di conseguenza la necessità di un intervento normativo da parte del legislatore comunitario.

In particolare, a seguito alla consultazione pubblica del 2017 condotta dalla Commissione europea relativa alla direttiva sulle banche dati, è emerso che:

1. da un lato, gli obiettivi originari della direttiva 96/9/CE sono ancora in linea con le esigenze dell'UE,

2. dall'altro lato, che la direttiva non ha pienamente raggiunto il suo obiettivo di proteggere un'ampia varietà di banche dati, soprattutto in riferimento al c.d. diritto sui generis.

Pertanto, al fine di facilitare la crescente condivisione dei dati nonché il commercio e la raccolta di dati generati nello sviluppo dell'Internet delle cose, la Commissione europea ha annunciato, nel suo programma di lavoro 2021 e in riferimento all'iniziativa "Un'Europa pronta per l'era digitale", che rivedrà la direttiva sulle banche dati entro il 2030, nel rispetto dei principi del diritto alla riservatezza e alla connettività, la libertà di espressione, la libera circolazione dei dati e la cybersicurezza.

LE AUTRICI

avv. ELEONORA LENZI

dott.ssa ILARIA NANNI

Studio legale Stefanelli&Stefanelli

Sedi
Bologna: Via Azzo Gardino 8/A - 40122
Milano: Via Nino Bixio, 31 - 20129
Roma: Palazzo Marignoli - Piazza di San Silvestro, 8 - 00187
Venezia: Sestiere Castello 2388 - 30122

E-mail: info@studiolegalestefanelli.it

Edizione: ottobre 2021