Il ruolo della Data Protection per una gestione efficace delle misure economiche e sociali per fronteggiare l'emergenza da Covid-19

Giuseppe D'Agostino
Ingegnere delle Telecomunicazioni, Associate Partner Consulting Technology Cybersecurity & Privacy di PwC Italy

Nicolò Giuli
Dottore in Ingegneria gestionale, Manager Consulting Technology Cybersecurity & Privacy di PwC Italy

Le misure per fronteggiare l'emergenza e l'esigenza di digitalizzazione della PA

L'emergenza epidemiologica da Covid-19 ha richiesto una risposta forte e tempestiva da parte dei Governi e delle principali autorità a livello nazionale e sovranazionale.
I pacchetti di misure adottate dall'Unione Europea, quali le iniziative di investimento *Coronavirus CRII – Coronavirus Response Investment Initiative*, CRII+ – *Coronavirus Response Investment Initiative Plus*[57] e l'articolato pacchetto di misure denominato *Next Generation UE*[58] porteranno agli Stati Membri ingenti somme di denaro, legate a fondi strutturali e di solidarietà dell'Unione Europea, che serviranno a contenere l'emergenza, potenziando in primo luogo il sostegno ai sistemi sanitari nazionali.
Analogamente, il governo italiano ha approvato una serie di misure a favore

[57] Per approfondire le misure contenute nei pacchetti approvati da Commissione Europea e Consiglio europeo, si veda il sito internet gestito dalla Commissione Europea dedicato all'emergenza sanitaria da Covid-19, disponibile al link: https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response_en
[58] Il testo completo dell'accordo è disponibile sul sito internet del Consiglio europeo, al link: https://www.consilium.europa.eu/media/45109/210720-euco-final-conclusions-en.pdf

di famiglie, lavoratori e imprese per fronteggiare la crisi, non esclusivamente da un punto di vista sanitario ma anche socio-economico.
I decreti-legge 17 marzo 2020, n. 18 (per semplicità "Decreto Cura Italia"[59]) e 19 maggio 2020, n. 34 (c.d. "Decreto Rilancio"[60]) hanno poi introdotto sul territorio nazionale numerose misure economiche e fiscali, quali agevolazioni e incentivi a beneficio di imprese e lavoratori.
In tale contesto, è evidente come a stretto giro le Pubbliche Amministrazioni italiane, operanti sia a livello nazionale sia a livello regionale e provinciale, si troveranno a gestire e monitorare una mole massiccia di dati e informazioni in relazione alle risorse finanziarie stanziate, nonché ai soggetti persone fisiche beneficiarie delle misure messe in campo.
La crisi in atto e i rigidi "paletti" indicati dell'Unione Europea impongono all'Italia di non commettere errori e di utilizzare tali soldi, concessi sotto forma di sovvenzioni e prestiti, per realizzare le necessarie riforme strutturali, nel rispetto degli obblighi di trasparenza in materia finanziaria.
In tale scenario, è tornato prepotentemente alla ribalta, nei principali palinsesti televisivi e a mezzo stampa, un tema di cui ormai si discute da decenni: la digitalizzazione della Pubblica Amministrazione.
In tempi non sospetti la Pubblica Amministrazione si è posta come priorità strategica quella di semplificare l'accesso da parte dei cittadini e delle imprese ai propri servizi, da perseguire mediante la realizzazione di infrastrutture IT sicure e affidabili, in forte cooperazione con le altre amministrazioni[61].
Gli addetti ai lavori saranno concordi nell'ammettere che i risultati raggiunti in tale ambito non sono sempre stati di pregevole fattura e sono ancora molte le pratiche e le procedure che gli italiani non possono svolgere facilmente per via telematica[62].
In questo momento storico, digitalizzare i servizi della Pubblica Amministrazione diventa un vero e proprio *diktat* e, a tal proposito, fa ben sperare

[59] Pubblicato in Gazzetta Ufficiale n.70 del 17 marzo 2020 e disponibile al link: https://www.gazzettaufficiale.it/eli/id/2020/03/17/20G00034/sg
[60] Pubblicato in Gazzetta Ufficiale n.128 del 19 maggio 2020 e disponibile al link: https://www.gazzettaufficiale.it/eli/id/2020/07/18/20G00095/sg
[61] La trasformazione digitale della pubblica amministrazione è promossa come elemento essenziale dal Piano Triennale 2020-2022 per l'Informatica nella Pubblica Amministrazione elaborato dall'Agenzia per l'Italia Digitale (AgID) al fine di contribuire alla diffusione di nuove tecnologie per mettere al centro dei servizi erogati dalla PA cittadini e imprese. Il suddetto Piano è consultabile sul sito di AgID al link: https://www.agid.gov.it/it/agenzia/piano-triennale
[62] Sul tema, si veda il report pubblicato dall'ISTAT in data 17 aprile 2020 "Pubblica Amministrazione Locale e ICT", disponibile al link: https://www.istat.it/it/archivio/ICT che evidenzia come soltanto nel 54,6% delle Regioni e nel 48,3% dei Comuni sia possibile espletare online l'intero iter – dall'avvio alla conclusione – di almeno un servizio erogato alla cittadinanza.

l'istituzione, ai sensi dell'art. 230 del Decreto "Rilancio", del Fondo per l'innovazione tecnologica e la digitalizzazione[63].
Tale progetto prevede interventi complessi e ambiziosi, volti a intervenire e rivedere le modalità di funzionamento, i criteri di organizzazione e di distribuzione di risorse ed energie nel settore pubblico e a contribuire alla trasformazione tecnologica e digitale dell'amministrazione pubblica, allo scopo di ridurre la distanza con i cittadini e incrementare velocità e sicurezza dei servizi erogati.

La necessità di integrare la *cybersecurity* e la *data protection* nei piani digitali

Tralasciando le argomentazioni politiche, la domanda che si pongono gli addetti ai lavori è pertanto la seguente: riusciranno i sistemi informativi delle pubbliche amministrazioni centrali e locali a reggere l'urto rappresentato dalla mole di richieste e di pratiche che si troveranno a gestire in relazione all'utilizzo e al monitoraggio delle risorse economiche stanziate a livello nazionale ed europeo?
Per perseguire tale obiettivo, e dare una risposta credibile ed efficace all'intero sistema Paese, la soluzione è rappresentata da un connubio perfetto dei seguenti due elementi fondamentali: c*ybersecurity* e protezione dei dati personali. Tale approccio dovrà, in un futuro ormai prossimo, essere adottato in maniera sinergica a livello europeo con interventi sull'intera infrastruttura digitale a supporto dei servizi erogati dalle istituzioni europee e dalle amministrazioni dei singoli Stati Membri; infatti, un'eventuale falla/incidente di sicurezza su uno dei "nodi" comporterebbe impatti negativi sull'intera "rete".
L'adozione di soluzioni tecnologiche di sicurezza e l'integrazione all'interno dei processi e dei servizi erogati dalle singole PA delle prassi e dei princìpi più all'avanguardia in materia di *cybersecurity* e *data protection* consentirà infatti di disporre di un patrimonio informativo e di dati sempre aggiornati ed esatti e di implementare delle logiche di trattamento ed elaborazione di tali informazioni in grado di mitigare adeguatamente i rischi che possono comportare.
Questa è la strada da percorrere per garantire riservatezza e integrità del patrimonio informativo, e, contestualmente, la disponibilità di quei dati (parametro di qualità troppo spesso trascurato) quando la singola PA è

[63] Si veda, a tal proposito, la nota pubblicata sul sito del Ministero dell'Innovazione tecnologica e la Digitalizzazione, disponibile al link: https://innovazione.gov.it/costituito-fondo-innovazione-tecnologica/

chiamata a gestire velocemente le richieste di servizi che pervengono dalla cittadinanza e a riconoscere ed erogare le relative misure e benefici.
La sfida, che alcune pubbliche amministrazioni virtuose hanno già accettato, è quella di definire la propria strategia di *digital transformation* tenendo in considerazione fin dalla progettazione i requisiti in materia di sicurezza delle informazioni e privacy (principio della *Security & Privacy by Design*).
Poter disporre di un controllo reale ed effettivo sui dati, integrando sicurezza e privacy, apre le porte e abilita ad un'ulteriore opportunità che si rivelerà fondamentale al fine della corretta gestione delle misure di politica economica e sociale che il legislatore intenderà concepire: l'interoperabilità e la cooperazione tra le banche dati e i sistemi delle pubbliche amministrazioni. Ciò vale, a maggior ragione, con riferimento a un nuovo paradigma architetturale, affermato all'interno del Piano Triennale 2020-2022 per l'Informatica nella Pubblica Amministrazione definito da AgID, che sta prepotentemente virando verso le piattaforme di *cloud computing*, ritenute come prima opzione in fase di sviluppo di nuovi progetti/servizi (principio del "*Cloud-first*"), determinando ulteriori complessità nella gestione dei rischi in ambito sicurezza e protezione delle informazioni, in termini prevalentemente di *governance* dei dati.

L'interoperabilità e fruibilità delle banche dati come leva abilitante

Non è un mistero che vincoli e limiti a un operato efficiente dell'amministrazione pubblica siano spesso rappresentati da sistemi informativi e banche dati obsoleti, non adeguatamente monitorati e protetti, all'interno di architetture tecnologiche prive di soluzioni di *data warehousing*[64] e *data analytics*[65] in grado di correlare i dati e apportare un valore aggiunto, in fase sia di definizione sia di implementazione delle misure economico-sociali, per un'azione più efficace e mirata a beneficio dell'intero sistema Paese.
In tale contesto, al fine di garantire uno standard di servizio elevato con

[64] Con il termine "data warehouse" si intendono le attività di collezione e aggregazione di dati provenienti da fonti interne ed esterne al sistema informativo di un'azienda finalizzate a all'esecuzione di analisi informative mirate a supportare le decisioni strategiche e operative assunte dal vertice aziendale. In particolare, il termine "data warehouse" può altresì indicare il repository centralizzato in cui far confluire i dati provenienti da database relazioni e non relazionali successivamente oggetto di elaborazione e analisi.
[65] In letteratura informatica, per "data analytics" si intende l'insieme di attività di ispezione, razionalizzazione e modellazione dei dati e delle informazioni in possesso di un'organizzazione per fini descrittivi e predittivi.

riferimento al coordinamento, alla gestione e al monitoraggio delle misure di politica economica e sociale introdotte per fronteggiare l'emergenza Covid-19, contribuirà significativamente l'interoperabilità tra i sistemi delle singole amministrazioni e la fruibilità dei dati in essi contenuti a beneficio delle altre amministrazioni, in funzione naturalmente dello svolgimento dei compiti istituzionali a ciascuna attribuiti. L'interoperabilità a livello di *back-end* rappresenterà, dunque, il fattore di successo per un modello digitale in cui i *front-end*[66], ovvero portali e servizi messi a disposizione della cittadinanza, possano assicurare affidabilità e chiarezza, facilitare la partecipazione civica e soddisfare le esigenze di cittadini e imprese.

Tali princìpi garantiranno, da una parte, il diritto dei cittadini di fruire in maniera semplice dei benefici previsti dalle misure prescritte dallo Stato e dalle autorità locali (*e.g.* Regioni e Province autonome) e, dall'altro, consentiranno alle autorità nazionali il monitoraggio e la valutazione circa gli esiti conseguiti al fine di implementare ovvero correggere le misure e gli interventi introdotti, alla luce dell'evoluzione del quadro macroeconomico, del mercato del lavoro e degli andamenti industriali, produttivi e sociali.

Il tema dell'interoperabilità tra banche dati pubbliche in Italia parte da lontano. Esso vide la luce nel corso degli anni '90 del secolo scorso fino al concepimento di una prima azione governativa strutturata, rappresentato dal Piano di Azione[67], sviluppato nel 2000 dal Ministro della Funzione Pubblica del Governo Amato, Franco Bassanini. Tale Piano definiva una serie di provvedimenti per favorire l'innovazione tecnologica nella Pubblica Amministrazione italiana e perseguire tre obiettivi: efficienza interna della PA, offerta di servizi integrati a cittadini e imprese, accesso telematico a servizi e informazioni garantito a tutti[68]. Le condizioni abilitanti per la realizzazione del Piano includevano le seguenti:

- che tutte le amministrazioni e gli enti siano dotati di un sistema informativo progettato non solo per l'automazione delle funzioni e delle procedure

[66] Nel campo della progettazione *software*, *front-end* e *back-end* rappresentano rispettivamente l'interfaccia di un programma con cui gli utenti interagiscono e la parte che consente l'effettivo funzionamento di queste interazioni. In particolare, gli utenti interagiscono con il front-end fornendo dati e richiedendo particolari servizi; tali richieste e i dati raccolti sono elaborati dal back-end, accessibile solo dagli amministratori del programma.

[67] Il Piano d'azione per l'e-government fu definito dal Ministero della Funzione Pubblica e pubblicato nel giugno del 2000 al fine di definire le azioni necessarie all'ammodernamento dell'Amministrazione italiana mediante adozione e integrazione delle tecnologie ICT. Il Piano è consultabile al link http://www.interlex.it/testi/rappegov.htm

[68] Si veda a tal proposito di A. Cenini, *E-government per lo sviluppo. Il piano del Governo per la digitalizzazione della Pubblica Amministrazione*, disponibile al link http://sspa.it/www.sspa.it/wp-content/uploads/2010/04/cap-4.pdf

interne dell'amministrazione e per l'erogazione di servizi ai propri utenti, ma anche per l'erogazione di servizi direttamente ai sistemi informatici delle altre amministrazioni;
- che tutte le amministrazioni che svolgono un ruolo di back-office, cioè che per ragioni istituzionali possiedono archivi contenenti informazioni necessarie alla erogazione di servizi propri, ma anche di servizi di amministrazioni terze, rendano accessibili senza oneri i propri servizi sulla rete a tutte le amministrazioni che svolgono un ruolo di front-office, per consentire loro la erogazione del servizio senza richiedere al cittadino informazioni già in possesso della Amministrazione;
- che le amministrazioni di front-office realizzino una integrazione dei servizi delle amministrazioni di back-office per fornire servizi integrati secondo le esigenze del cittadino e non secondo l'organizzazione delle amministrazioni eroganti.

Il Piano, dunque, affermava la necessità di innovare l'amministrazione pubblica e fornire servizi utili ed evoluti alla cittadinanza mediante la riprogettazione di processi e procedure in un nuovo paradigma basato sull'integrazione dei *back-end* e sulla cooperazione applicativa.
Il suddetto Piano non ebbe grande successo in termini realizzativi, a causa non solo dell'obsolescenza tecnologica degli standard tecnici e architetturali utilizzati dalla PA ma anche dalla mancata condivisione complessiva del nuovo paradigma culturale suggerito[69].
Qualche anno più tardi, il Codice dell'Amministrazione Digitale (comunemente noto per brevità con l'acronimo "CAD")[70] promosse nuovamente un modello architetturale basato sull'integrazione e sull'interoperabilità dei servizi erogati dalle pubbliche amministrazioni mediante l'interrogazione e la consultazione reciproca delle banche dati di propria competenza, nonché con l'adozione di protocolli e meccanismi di scambio di dati e informazioni.
Il principio di fondo è che qualunque dato detenuto da una pubblica amministrazione possa essere reso accessibile e fruibile alle altre amministrazioni,

[69] Per approfondire le problematiche nella realizzazione del Piano di Azione del Ministro Bassanini, si suggerisce la lettura di A. Fuggetta, *Quale strategia ICT per la PA: dalla storia la lezione per non ripetere vecchi errori,* pubblicato su agendadigitale.eu e disponibile al link https://www.agendadigitale.eu/infrastrutture/quale-strategia-ict-per-la-pa-dalla-storia-la-lezione-per-non-ripetere-vecchi-errori/

[70] Il Codice dell'Amministrazione Digitale (CAD), istituito con decreto legislativo 7 marzo 2005 n. 82 e successivamente modificato e integrato, rappresenta il testo unico di riferimento per le norme concernenti l'informatizzazione della PA nei rapporti con cittadini e imprese. È disponibile sul sito dell'AgID al seguente link: https://docs.italia.it/italia/piano-triennale-ict/codice-amministrazione-digitale-docs/it/v2017-12-13/index.html

in linea con le esigenze di semplificazione delle procedure e di efficienza dell'azione amministrativa.
Ciò premesso, la valorizzazione del patrimonio di dati pubblici, che consenta alla cittadinanza di interfacciarsi agevolmente con le pubbliche amministrazioni, da intendersi come unica entità, rimane un obiettivo astratto se l'amministrazione pubblica non è in grado di garantire riservatezza, integrità e disponibilità dei dati, nonché la resilienza dei propri sistemi informativi.
Ciò deve avvenire necessariamente nel rispetto delle prescrizioni in materia di protezione e tutela dei dati personali dei soggetti interessati, rappresentati, nel caso di specie, dai richiedenti e dagli effettivi beneficiari delle misure di sicurezza.
Le notizie di cronaca, negli ultimi anni, hanno assestato duri colpi e minato la fiducia dei cittadini nei confronti delle istituzioni statali e dell'amministrazione pubblica, non sempre in grado di verificare correttamente i requisiti per l'accesso a determinate misure socio-economiche, con la conseguente proliferazione di spiacevoli fenomeni quali, a titolo esemplificativo, quello dei "falsi invalidi" e delle molteplici truffe ai danni dello Stato con riferimento alla percezione di misure di sostegno al reddito da parte di soggetti non in possesso dei requisiti di legge.
Ciò avviene (anche) perché le singole amministrazioni non incrociano le proprie banche dati e non mettono a disposizione di altri soggetti aventi finalità istituzionali il proprio patrimonio informativo, che potrebbe arricchire e perfezionare l'azione amministrativa altrui.
In coerenza con gli obiettivi connessi all'attuazione del CAD, per un efficace ed efficiente scambio dati tra pubbliche amministrazioni è indispensabile che la raccolta, l'elaborazione e la conservazione dei dati avvenga nel rispetto di alcune misure di sicurezza in materia di protezione dei dati personali.

Regole tecniche e modalità sicure di scambio dati tra PA

Alla luce di quanto sopra esposto, c'è da aspettarsi nei prossimi mesi un massiccio ricorso allo strumento della Convenzione per regolamentare la fruibilità dei dati per via telematica da parte delle amministrazioni pubbliche.
Le Pubbliche Amministrazioni che intendano mettere a disposizione gli accessi alle proprie banche dati alle altre amministrazioni mediante cooperazione applicativa o tramite accessi via web, dovranno adottare le regole tecniche e le misure di sicurezza identificate dal Garante per la protezione dei dati personali con il Provvedimento del 2 luglio 2015 "Misure di sicurezza e

modalità di scambio dei dati personali tra amministrazioni pubbliche"[71].
Naturalmente, prima di consentire l'accesso alle proprie banche dati, il soggetto erogatore (ovvero l'amministrazione che mette a disposizione del soggetto fruitore il proprio patrimonio informativo) deve preliminarmente verificare la sussistenza di una base giuridica legittimante la consultazione e l'accesso ai dati da parte del fruitore, ovvero la presenza di una finalità istituzionale coerente con la natura e la qualità dei dati richiesti.
Le misure di sicurezza prescritte dal Garante per la protezione dei dati personali rappresentano un adeguato standard di sicurezza a tutela dei dati personali che consentirà il trattamento di dati esatti e costantemente aggiornati, con i quali le singole amministrazioni pubbliche potranno gestire efficacemente le misure economico-sociali nel rispetto dei propri compiti e finalità istituzionali.
Tali misure richiedono innanzitutto la presenza di misure di protezione perimetrali, nonché l'utilizzo di reti private virtuali sicure (Secure VPN)[72] basati su protocolli di comunicazione che prevedono la cifratura dei dati in transito mitigando, di conseguenza, i rischi di intercettazione. Un potenziale attaccante, infatti, non sarebbe in grado di decifrare, né modificare il contenuto; ciò si applica anche al rischio di intercettazione delle credenziali in fase di autenticazione da parte degli utenti del soggetto fruitore, protette mediante meccanismi crittografici robusti.
Nell'implementazione delle Convenzioni, inoltre, devono trovare spazio attività periodiche di *vulnerability assessment*[73] e *penetration testing*[74] così da rilevare e proteggere i sistemi e le banche dati pubbliche da vulnerabilità note, nonché da anomalie quali mancanza di *patch* di sicurezza ed errori di configurazione.
Oltre alle suddette misure, l'Autorità di Controllo ha identificato tre principali

[71] Tale Provvedimento è disponibile sul sito internet dell'Autorità di Controllo al link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/4129029
[72] La rete virtuale privata (in inglese *Virtual Private Network)* è una rete di telecomunicazioni instaurata tra due soggetti che utilizzano un protocollo di trasmissione pubblico, come i protocolli internet, come tecnologia di trasporto. Essa è dunque da intendersi come estensione geografica di una rete locale privata (LAN) in cui gli utenti possono accedere, da remoto, a un server su una rete privata per il tramite della rete internet.
[73] Attività di analisi di sicurezza, condotte mediante tool automatici di scansione dei sistemi, finalizzate all'identificazione del grado di esposizione dei sistemi informatici a eventuali attacchi e alla rilevazione di potenziali vulnerabilità quali porte aperte su router e IP, accessi avvenuti senza autenticazione o non autorizzati, software obsoleti, ovvero per cui non sono state installate patch di sicurezza rese disponibili dai produttori di software.
[74] Attività di simulazione di un attacco, condotta mediante tecniche automatizzate e manuali, volta a individuare i punti più vulnerabili di un sistema e tentare di violarli, al fine di testare l'efficacia delle difese le cui vulnerabilità potrebbe essere sfruttate da un attaccante esterno.

ambiti con impatti a livello tecnologico, da indirizzare e gestire con efficacia per garantire il valore aggiunto derivante dalla fruibilità e/o interoperabilità delle banche dati pubbliche.

Modalità di accesso

Per consentire la fruibilità dei dati, l'amministrazione erogatrice può ricorrere a una delle seguenti modalità tecniche:

- accesso in modalità di cooperazione applicativa, ovvero tramite servizi esposti in cooperazione applicativa, offerti dalle singole amministrazioni attraverso un unico elemento del proprio sistema informativo, denominato Porta di Dominio ("Pdd") che colloquia con l'esterno;
- accesso via web, ovvero tramite un sito telematico o altre applicazioni *software* del soggetto erogatore, cui il soggetto fruitore può accedere debitamente autorizzato e previa autenticazione.

Nel caso della cooperazione applicativa, è necessaria l'adozione di standard di sicurezza, quali autenticazione OAUTH2.0[75] e connessioni private e protette basate su protocolli di crittografia SSL/TLS[76] sul layer costituito dall'integrazione tra le Porte di Dominio o fra API Gateway[77], *entry-point* al sistema, la cui finalità è quella di esporre i servizi in maniera sicura e controllata.
Modalità di accesso alternative, quali la posta elettronica certificata e soluzioni di trasferimento di file in modalità FTP[78] sicuro possono essere utilizzate esclusivamente laddove l'infrastruttura tecnologica e la struttura organizzativa delle amministrazioni coinvolte non consenta l'adozione delle due

[75] OAuth è l'abbreviazione di "Open Authorization" ovvero un protocollo standard aperto che consente una autorizzazione API sicura. Tramite autorizzazione API, pertanto, tale protocollo garantisce un alto livello di sicurezza e concede a un'applicazione client l'accesso limitato a risorse protette attraverso lo scambio di token.
[76] Certificato *Secure Sockets Layer (SSL) e Trasnport Layer Security (TLS),* rilasciati da un'Autorità di Certificazione o da rivenditori autorizzati, sono protocolli standard che stabiliscono una connessione cifrata sicura tra un *web browser* e un *server* o una rete. Rappresentano la tecnologia di sicurezza standard che garantisce l'autenticazione del dominio del sito cui l'utente si collega e la reale identità dell'azienda collegata a quel dominio. Per completezza, si segnala che sono ormai note alcune vulnerabilità anche sul protocollo SSL, che è risultato suscettibile ad alcune tipologie di attacco man-in-the-middle quali il c.d. "Poodle Attack".
[77] Con il termine "Application Programming Interface" (API) si indica un set di protocolli con i quali sono realizzati i *software* applicativi e che consentono la comunicazione tra servizi e la trasmissione di dati tra diverse applicazioni o pagine web.
[78] Il protocollo File Transfer Protocol (FTP) è un protocollo di livello applicazioni per la trasmissione di dati da un host all'altro in un'architettura di tipo client-server. La sua versione "sicura" FTPS aggiunge al protocollo FTP la cifratura dei dati in transito.

menzionate in precedenza. In particolare, con riferimento al protocollo di trasferimento in modalità FTP, può essere preso in considerazione garantendo altresì la cifratura del canale di trasmissione dei dati (*e.g.* mediante reti private virtuali) o adottando meccanismi di cifratura sulle singole sessioni di trasferimento dati.

Selezione dei dati

Il soggetto erogatore è tenuto a identificare e selezionare i dati personali che potranno essere consultati dal fruitore, nel rispetto dei principi di minimizzazione, pertinenza e non eccedenza prescritti dal Regolamento (UE) 2016/679. Pertanto, per ciascuna amministrazione richiedente l'accesso alle banche dati nella disponibilità dell'amministrazione erogatrice, dovranno essere definiti dei profili di autorizzazione e dei "coni" di visibilità finalizzati a consentire l'accesso e la consultazione dei soli dati strettamente necessari per le finalità istituzionali perseguite dal soggetto fruitore.
La *ratio* di attribuzione a ciascuna risorsa del fruitore del rispettivo profilo di autorizzazione è rappresentata dal principio del "*need to know*" secondo cui è necessario limitare l'accesso ai dati e alle informazioni di cui l'utente ha effettivamente e strettamente bisogno per espletare le proprie mansioni. Tale obiettivo potrà essere realizzato mediante la definizione e l'implementazione di sistemi di *Identity & Access Management*[79] in grado di garantire, attraverso la creazione e la gestione di differenti profili di autenticazione e autorizzazione, l'identità dell'utente e attivare le sole funzionalità per le quali l'operatore dell'amministrazione fruitrice è abilitato a operare.
Nel caso in cui le esigenze del fruitore non dovessero richiedere l'accesso e la consultazione di interi set di dati, l'erogatore può valutare di consentire modalità di accesso che offrano un livello minimo, quali valori di tipo booleano (vero/falso) come esito delle interrogazioni effettuate dal fruitore. Ciò vale, in particolare, per i servizi di interrogazione di banche dati pubbliche finalizzati ad accertare l'esattezza e o l'effettiva esistenza di un dato.

Procedure di autenticazione e autorizzazione degli utenti

Nel definire le modalità tecniche di interoperabilità tra le banche dati pubbliche, l'erogatore e il fruitore devono definire e implementare procedure

[79] Con "Identity & Access Management" si intendono sistemi integrati di tecnologie e procedure finalizzate alla gestione degli accessi degli utenti alle risorse IT di un'organizzazione, inclusi sistemi, applicazioni e dati, al fine di proteggere il patrimonio informativo da accessi non autorizzati.

per il rilascio delle utenze e la gestione delle autorizzazioni degli utenti interessati dalla Convenzione. Tali procedure devono consentire sempre l'identificazione univoca della persona fisica che ha effettuato l'accesso ai servizi del soggetto erogatore.
Come detto in precedenza, tale obiettivo può essere perseguito mediante sistemi di *Identity & Access Management* in grado di gestire:

- la fase di accreditamento dell'utente, ovvero di censimento di ciascun soggetto dell'amministrazione fruitrice che potrà operare sui sistemi oggetto di Convenzione. A ciascuno di tali soggetti sarà assegnata un'utenza nominativa;
- la fase di identificazione dell'utente che ha effettuato l'autenticazione. Il sistema di *Identity Management* deve verificare che l'utente che sta effettuando l'accesso sia stato previamente accreditato; successivamente, il sistema ne identifica il corretto ruolo e lo abilita all'accesso sui sistemi/servizi dell'amministrazione erogatrice, consentendo l'utilizzo delle sole funzionalità autorizzate, correlate al profilo dell'utente.

Alla luce delle prescrizioni contenute nel Decreto Semplificazioni (Decreto n. 76 del 16 luglio 2020), si raccomanda l'autenticazione da parte degli utenti dell'amministrazione fruitrice esclusivamente mediante credenziali del Sistema Pubblico di Identità Digitale ("SPID")[80] di livello 2 o superiore. Rispetto al primo livello, che consente l'accesso ai servizi online attraverso le credenziali rappresentate da nome utente e password scelti dall'utente, il secondo livello garantisce un livello di sicurezza maggiore, richiedendo, oltre alla coppia di credenziali username e password, anche un terzo elemento, ottenuto dall'utente mediante la generazione di un codice temporaneo di accesso (*One Time Password*, c.d. "OTP") per il mezzo di un dispositivo in suo uso e possesso esclusivo.
In alternativa allo SPID, l'autenticazione può avvenire mediante Carta Nazionale dei Servizi (CNS) o Carta di Identità Elettronica (CIE).
In tale contesto, risulta evidente come tutte le operazioni di trattamento di dati personali effettuate da personale autorizzato dell'amministrazione fruitrice siano debitamente tracciate.
Il livello di sicurezza richiesto da autorità quali AgID e Garante per la protezione dei dati personali evidenzia come i dati siano un valore intrinseco

[80] Lo SPID (Sistema Pubblico di Identità Digitale) è il sistema unico di accesso con identità digitale ai servizi online della pubblica amministrazione italiana e soggetti privati aderenti. L'identità SPID è rilasciata da uno degli *identity provider* accreditati e autorizzati dall'Agenzia per l'Italia Digitale (AgID).

alle organizzazioni pubbliche; pertanto, la loro protezione da minacce che potrebbero pregiudicarne autenticità, riservatezza e/o disponibilità rappresenta un elemento imprescindibile di qualsivoglia agenda digitale o percorso di *digital transformation* che il sistema Paese intenderà intraprendere.
Vorrà dunque la Pubblica Amministrazione italiana imparare a concepire realmente *cybersecurity* e *data protection* come processi di continuo miglioramento a supporto dei servizi erogati alla cittadinanza; le misure di sicurezza adottate siano, dunque, continuamente rimesse in discussione ed eventualmente integrate/aggiornate al fine di garantirne l'adeguatezza con riferimento ai rischi per i diritti e le libertà dei soggetti interessati dai trattamenti di dati personali.
Soltanto così sarà possibile instaurare un rapporto di fiducia con i cittadini e con le istituzioni europee. Perché se le pubbliche amministrazioni falliranno nel proteggere i nostri dati personali, esse non saranno in grado di mettere a fattor comune il proprio patrimonio informativo. E senza interoperabilità tra le banche dati pubbliche, l'azione dell'amministrazione pubblica sarà priva di quel vigore e di quell'efficacia che le iniziative di risposta all'emergenza Covid-19 ci impongono per una ripresa economico-sociale reale.
Insomma, è in gioco la tenuta dell'intero Paese.
E si deve ripartire da qui. Dai nostri dati personali.