TopHic | dig deeper

Novembre 2021

Con il PNRR riparte l'Italia?

Parere dell'esperto

PNRR e Data Protection

di ***Guglielmo Troiano***

Manager Grant Thornton FAS

A livello globale gli attacchi informatici sono in continuo aumento, a dimostrazione di quanto le competenze e le risorse di coloro che hanno un interesse a violare i sistemi di sicurezza siano consistenti e pervasive. Infatti, sia le PMI sia le grandi organizzazioni più preparate e con più risorse, siano esse pubbliche o private, subiscono attacchi informatici, spesso di successo, i quali causano ingenti danni finanziari, ma anche e soprattutto all'immagine e alla reputazione.
Un attacco informatico recentemente al centro del dibattito pubblico è quello che lo scorso luglio ha colpito i sistemi informatici di una pubblica amministrazione regionale italiana. Di fatto, con la presentazione del *Digital Service Act* e del *Data Governance Act*, la Commissione Europea ha...

continua all'interno

Overview

PNRR: opportunità e scelta strategica

di ***Giulio Tedeschi***

Partner e Head of Advisory Bernoni Grant Thornton

La fine dell'anno e la programmazione delle attività per il prossimo 2022 vede impegnato l'operatore con le consuete norme della legge finanziaria, ma questa volta anche con l'attivazione del PNRR. È inutile ricordare l'opportunità che il piano porta con sé e così pure la sua valenza strategica nelle scelte.
È altrettanto vero che la riflessione di questi momenti su questi temi riguarda anche il "piano" programmatico dell'attività di ogni impresa e così pure di tutti i professionisti...

continua all'interno

Approfondimento

PNRR e Cybersecurity

di ***Alessandro Leone***

Partner Grant Thornton FAS

Il Piano Nazionale di Ripresa e Resilienza (PNRR) Next Generation Italia, non è soltanto un progetto per la ripresa economica, ma soprattutto un'occasione unica per superare i drastici effetti del periodo pandemico. L'obiettivo principale è quello di rendere l'Italia più verde, più digitale e più resiliente, avendo a disposizione considerevoli risorse finanziarie e puntando sull'affermarsi di valori legati alla qualità della vita individuale e al miglioramento della coesione, dell'inclusione e dell'equità delle comunità.
Appare fondamentale ricordare che il PNRR si collochi nell'ambito di un *framework* di riforme più ampio, teso alla regolamentazione del processo di innovazione tecnologica nell'Unione Europea...

continua all'interno

Supplemento Notizie flash n° 107 del 25 febbraio 1984

Overview

PNRR: opportunità e scelta strategica

di ***Giulio Tedeschi***
Partner e Head of Advisory Bernoni Grant Thornton

La fine dell'anno e la programmazione delle attività per il prossimo 2022 vede impegnato l'operatore con le consuete norme della legge finanziaria, ma questa volta anche con l'attivazione del PNRR.

È inutile ricordare l'opportunità che il piano porta con sé e così pure la sua valenza strategica nelle scelte.

È altrettanto vero che la riflessione di questi momenti su questi temi riguarda anche il "piano" programmatico dell'attività di ogni impresa e così pure di tutti i professionisti.

Il presente numero di TopHic vuole focalizzare l'attenzione su taluni, tra i tanti, temi che si stanno sviluppando lungo questo filone e avviare con i clienti che ci leggono un approfondimento per orientare alcune scelte.

Il PNRR prende la mossa, come noto, dalla necessità di sviluppare a livello paese investimenti per l'ammodernamento dell'economia e tra questi l'area dello sviluppo tecnologico (si fa espresso riferimento alla scarsa familiarità del paese con le tecnologie digitali) accompagnato attraverso investimenti strutturali e con riforme idonee ad attivare i necessari processi di modernizzazione, di ampliamento delle infrastrutture e delle filiere produttive.

Uno dei fondamenti del PNRR è l'evoluzione digitale del Paese, sia attraverso investimenti orientati a tal fine nelle Pubbliche Amministrazioni, sia attraverso sgravi fiscali e incentivi al settore privato collegati ad investimenti in tecnologie e consulenze informatiche.

Una prima considerazione in merito a questa evoluzione digitale è sicuramente legata alla protezione dei dati personali e alla conformità con il Reg. (UE) 2016/679, più noto come GDPR. Si sente talvolta dire che questa normativa non sia "attuale" in quanto cercherebbe di porre un limite allo sviluppo della tecnologia e alla capacità di analisi dei dati maturata grazie a quest'ultima. Si tratta evidentemente di un grosso errore. Infatti, è vero il contrario. Proprio perché la capacità delle automazioni è arrivata ad analizzare quantità enormi di dati applicando correlazioni tra gli stessi e delineando le caratteristiche attitudinali e comportamentali dei singoli individui, si è resa necessaria una normativa che mettesse ordine e che mirasse al rispetto dei diritti fondamentali degli individui. Nella sezione *Il Parere dell'Esperto* vedremo come combinare i vantaggi dall'analisi dei dati offerta dall'evoluzione digitale nel rispetto della normativa.

Del resto, l'evoluzione digitale porta con sé un altro rischio: quello della cybersecurity. È intuitivo, infatti, che se da un lato si aprono opportunità di crescita legate all'adozione dei sistemi informatici, dall'altro la vulnerabilità di questi ad eventuali attacchi criminali costituisce un rischio enorme per la riservatezza delle informazioni e per la continuità delle normali operazioni.

Per tale ragione la *cybersecurity* rientra tra le priorità del nostro Governo e lo dovrebbe essere per gli enti di pubblica amministrazione e per le aziende del settore privato. L'analisi di questo tema è nella sezione *Approfondimento*.

Una menzione deve essere, poi, ricordata sull'esigenza, sempre più sentita, di indirizzare le scelte strategiche – e la conseguente operatività - nel solco di una trasformazione più marcata verso un'economia circolare.

All'interno del piano sono poi previste una serie di riforme in quanto necessarie e richieste dall'Europa. Esse sono note in quanto oggetto di quotidiana discussione così come riportata dai *mass media* - non è compito in questa sede di dettagliarle – e sostanzialmente riguardano la riforma della pubblica amministrazione, della giustizia, della promozione della concorrenza e non ultima quella della semplificazione della legislazione.

Proprio con riguardo a quest'ultima riforma, vorrei soffermarmi su quella di carattere fiscale che sta muovendo proprio in queste ore i primi passi con l'approvazione da parte del Governo del disegno di legge per la delega alla riforma fiscale.

Già molto si è sentito dire soprattutto sull'aspetto della revisione del Catasto e altrettanto del necessario abbattimento del carico fiscale in tema di cuneo fiscale e imposizione IRAP.

Partirei invece dall'evidenziazione del necessario processo di semplificazione delle norme, delle procedure e degli adempimenti tributari.

Aspetto che necessariamente debba passare attraverso una riscritturazione organica dell'impianto normativo, oggi assai disperso confusamente in una pluralità di norme sovente tra loro di difficile coordinamento. Tale è l'approccio metodologico da cui parte il disegno di delega che impegna il Governo a "mettere mano alle norme". Giustamente tale approccio porta alla ovvia e auspicata ipotesi di addivenire finalmente a un "testo unico" della normativa tributaria ove siano organizzate le norme per settori omogenei, coordinandole con l'altrettanta importante finalità di addivenire a un contesto di semplicità della disciplina tributaria. Il disegno di legge codifica questi condivisi principi metodologici e in tal senso l'art. 9 del disegno di legge delega parla di un aggiornamento che persegua lo scopo di semplificare il linguaggio. Si afferma infatti di dover "*… coordinare sotto il profilo formale di sostanziale il testo delle disposizioni legislative vigenti, anche di recepimento e attuazione della normativa dell'Unione Europea, apportando le modifiche opportune per garantire di migliorare la coerenza giuridica, logica e sistematica della normativa… e così per assicurare … l'unicità, la contestualità, la completezza e la chiarezza … della disciplina di ogni settore*".

L'operatore che quotidianamente si confronta nella "giungla" normativa tributaria immediatamente comprende come quest'ultimo principio non rappresenti una semplice affermazione di massima, ma si cali in un'esigenza ragionevole e condivisibile per essere messi nella condizione di applicare e poter rispettare la norma e così per gestire consapevolmente un'area delicata e importante quale è quella fiscale con un approccio orientato a una consapevole "gestione del rischio fiscale".

Un'altra area della riforma fiscale che merita di essere brevemente segnalata attiene al principio dettato all'articolo 3 lettera d) del disegno di legge delega e che riguarda l'obiettivo di armonizzazione dei regimi di tassazione del risparmio "*… tenendo conto dell'obiettivo di contenere gli spazi di elusione …*".

Il riferimento al termine "elusione" rafforza l'importanza che il contribuente sia dotato di una normativa chiara e di immediata applicazione. Le incertezze con cui sovente ci si deve confrontare "esplodono" in particolare nel settore delle rendite e degli investimenti finanziari e comportano il rischio cui poco sopra, con interpretazioni che nella complessità conducono a contestazioni fiscali. In un settore delicato e tutelato dalla stessa Costituzione sull'importanza del "risparmio" non è possibile pensare che l'incertezza di pensiero sulla portata delle norme conduca a rettifiche di imponibili fiscali ove dietro ai comportamenti dei contribuenti vi sia una volontà elusiva.

Il caso dei redditi "finanziari" (tecnicamente quelli derivanti dai redditi di capitale e quelli dai redditi cd diversi per *capital gain*) è giustappunto un caso emblematico per il quale è auspicabile l'intervento normativo con la riforma fiscale.

A parere di chi scrive è infatti necessario eliminare ogni incomunicabilità fra i redditi oggi classificati di capitale (tali sono i proventi, i frutti, gli interessi e i dividenti, ma anche i proventi periodici dell'investimento di capitale e le plusvalenze generate su taluni fondi di investimento) e i redditi oggi classificati come diversi (tali sono le plusvalenze conseguite quale differenza positiva tra prezzo di vendita e costo di acquisto di uno strumento finanziario).

Si è sempre nell'ambito della gestione del risparmio ove l'attuale incomunicabilità normativa oltre a ingenerare incomprensioni, confonde la fiducia agli occhi dei contribuenti con incomprensibili bizzarrie che poi si riflettono anche sulla gestione degli investimenti.

Tanti potrebbero essere gli esempi che quotidianamente gli operatori intercettano su questo delicato aspetto della gestione del risparmio individuale. La riforma fiscale potrebbe pertanto rappresentare il momento di incontro per eliminare queste distinzioni e uniformare i regimi di tassazione non solo in termini di compatibilità per l'investitore comune, ma anche di uniformità normativa (incidenza del prelievo inclusa). Con l'ulteriore beneficio di ridurre il rischio di favorire nella "giungla" normativa l'attuazione di pratiche che giustamente il disegno di legge vuole eliminare. L'esistenza di un unico regime di tassazione, armonico e ragionevole per tutte le tipologie di investimenti finanziari aiuterebbe al pieno rispetto della legge, proteggendo il risparmio e indirizzandolo, peraltro, a sostegno dell'economia del paese, delle PMI, evitando tentazioni di investire in altri paesi. Non è quindi un solo tema di natura fiscale.

Per quanto riguarda il reddito d'impresa delle società, un primo aspetto su cui si sofferma il disegno di legge di riforma tributaria riguarda il riesame dell'IRAP. Il tema appare condivisibile sicuramente per l'obiettivo di una ulteriore semplificazione, ma occorre attendere le modalità che il legislatore delegato vorrà attuare per potersi calare in operatività e commenti.

Passando quindi oltre, nell'area del reddito di impresa il disegno di legge delega all'articolo 4, punto 3b prevede una semplificazione e una razionalizzazione dell'IRES finalizzata alla riduzione degli adempimenti amministrativi a carico delle imprese "*...anche attraverso un rafforzamento del processo di avvicinamento tra valori civilistici e fiscali, con particolare alla disciplina degli ammortamenti...*".

Il tema è sicuramente apprezzabile innanzitutto nell'aspetto del necessario avvicinamento tra reddito civile da bilancio e reddito fiscale (per dare ancora più concretezza alla recentemente normativa codificata all'art. 83 TUIR sulla "derivazione rafforzata" del reddito fiscale dal reddito di bilancio secondo la quale la corretta applicazione dei principi contabili emanati dai competenti *settlor* fa stato e supera anche i criteri di qualificazione, imputazione temporale e classificazione contenuti nel TUIR).

Ma il tema è apprezzabile perché consentirà di rimettere mano al delicato aspetto dell'imputazione degli ammortamenti rivedendo, ai fini fiscali, il regime del decreto emanato nell'ormai lontano 1988, mai aggiornato e che soffre dell'evidente evoluzione tecnologica manifestatasi sui beni di impresa.

L'intervento in questa area dovrebbe poi riguardare anche l'aspetto delle tecniche di determinazione del reddito d'impresa attraverso le note "*variazioni in aumento e in diminuzione*" persegue l'obiettivo di "*...adeguare la disciplina ai mutamenti intervenuti del sistema economico...*" allineandola a quella in vigore nei principali paesi europei, anche per aumentare la competitività del sistema sul piano internazionale.

Tale armonizzazione aiuterà inoltre a ridurre i citati fenomeni elusivi di cui ho fatto all'inizio di questo intervento in continuità con gli obiettivi del legislatore.

Un'ulteriore area di intervento del disegno di legge riguarda l'efficientamento della riscossione. E' un obiettivo che avrà una ricaduta raffica per il contribuente a partire dal superamento dell'attuale sistema dell'aggio di riscossione (dopo il monito pervenuto nel 2021 dalla Corte costituzionale). la delega vuole perseguire un recupero di efficienza favorendo l'uso delle più evolute tecnologie e delle forme di interconnessione del patrimonio informativo con sistemi funzionali alla attività di riscossione (art. 2 del disegno di legge delega).

Le altre aree contenute nel disegno di legge delega e che qui non vengono trattate riguardano tra l'altro interventi sull'imposizione di redditi ai fini Irpef, la rimodulazione di alcune imposte indirette, inclusa l'iva e la revisione delle addizionali comunali e regionali.

Il tutto in un contesto di una "riforma" che non deve incidere sui saldi della finanza pubblica (art. 10 del disegno di legge delega). Il concetto di una riforma, forse, dovrebbe risiedere nella revisione organica e razionale dell'impianto normativo a parità di saldi. La riduzione dell'imposizione in generale non può che passare da provvedimenti che la politica deve elaborare con altri provvedimenti.

Siamo partiti dal PNRR per poi svolgere alcune brevi - e limitate - considerazioni su tre dei tanti aspetti che orienteranno i comportamenti soprattutto strategici degli operatori economici nell'immediato al fine di necessariamente poter cogliere le opportunità collegate all'attuazione del piano.

In linea generale si è parlato di un ammodernamento attraverso una transizione digitale e una transizione un'economia circolare (*green*) qui declinata nei temi propri (i) della *cybersecurity*, (ii) della trasformazione digitale e (iii) della riforma fiscale.

Il tutto non può però prescindere da un "cambio di marcia" che è richiesto a ogni operatore per orientarsi a gestire questo cambiamento. Non può essere sottovalutata l'importanza del contributo della ricerca non più da considerare come un "centro di costo", ma quale valore indispensabile per il rafforzamento e la realizzazione di modelli innovativi idonei a rafforzare le competenze e conseguentemente a favorire la transizione verso un'economia sempre più basato sulle conoscenze.

A realizzare linee di intervento che coprano l'intera filiera del processo di innovazione, di ricerca di base e di sviluppo tecnologico attraverso il trasferimento di conoscenze e competenze proprie di operatori qualificati.

I professionisti di Grant Thornton Italia sono consapevoli di quanto precede e colgono l'opportunità di questa sfida, ben consapevoli che le proprie competenze accresciute con l'impegno alla ricerca che ogni giorno è bagaglio professionale idoneo a offrire una vasta gamma di servizi integrati nell'ampia area aziendale per continuare la collaborazione con i clienti a partire dai temi esposti in questo numero di TopHic.

Con la consapevolezza di essere consulenti dinamici in grado di offrire servizi professionali integrati non quali semplici esecutori materiali di incarichi, ma *trustee provider* globali di consulenza, coinvolti nei processi di sviluppo che clienti, a loro volta, stanno studiando e sviluppando.

Parere dell'esperto

PNRR e Data Protection

di ***Guglielmo Troiano***
Manager Grant Thornton FAS

Il Piano Nazionale di Ripresa e Resilienza (PNRR) *Next Generation* Italia, non è soltanto un progetto per la ripresa economica, ma soprattutto un'occasione unica per superare i drastici effetti del periodo pandemico. L'obiettivo principale è quello di rendere l'Italia più verde, più digitale e più resiliente, avendo a disposizione considerevoli risorse finanziarie e puntando sull'affermarsi di valori legati alla qualità della vita individuale e al miglioramento della coesione, dell'inclusione e dell'equità delle comunità.

Appare fondamentale ricordare che il PNRR si collochi nell'ambito di un *framework* di riforme più ampio, teso alla regolamentazione del processo di innovazione tecnologica nell'Unione Europea. Di fatto, con la presentazione del *Digital Service Act* e del *Data Governance Act*, la Commissione Europea ha mostrato la propria volontà di tracciare nuovi paradigmi per rafforzare il mercato interno dei servizi digitali.

La "*Missione 1: Digitalizzazione, Innovazione, Competitività, Cultura e Turismo*" del PNRR si pone l'obiettivo di dare un forte impulso decisivo al rilancio della competitività e della produttività del nostro Paese.

Una sfida di tale portata richiede un intervento profondo, che agisca su più elementi chiave del sistema economico italiano, in ottica di innovazione, sostenibilità e promozione dell'immagine e del *brand* del Paese.

La spinta che *Next Generation EU* darà alla rivoluzione digitale condurrà, tuttavia, ad un inevitabile ed esponenziale aumento di trattamenti di dati personali, che non potranno prescindere dal rispetto dei principi cardine del GDPR. Pertanto, tutte le realtà private e pubbliche che intendano beneficiare dei vantaggi definiti dal PNRR dovranno necessariamente aver concluso, o quantomeno aver intrapreso, il percorso di conformità alla normativa sulla protezione dei dati personali, che appare oltremodo imprescindibile nella corsa all'innovazione digitale.

Sul punto si è espresso anche il Garante per la Protezione dei Dati Personali, ponendo l'attenzione sulla doppia valenza della tutela prevista dal GDPR nell'ambito del progetto di riforme previste dal PNRR: infondere fiducia nei cittadini in relazione all'attività svolta dai soggetti pubblici nello svolgimento delle proprie funzioni, da una parte, e garantire la sicurezza del processo di innovazione e quindi migliorare la competitività senza che ciò comporti limitazioni ai diritti e alle libertà individuali, dall'altra.

In occasione della presentazione del *report* annuale dell'attività del Collegio, l'Autorità Garante ha ricordato come l'unica strada percorribile per la realizzazione delle Missioni previste dal PNRR sia proprio l'attuazione di un'effettiva sinergia tra *Data Protection* e *Cybersecurity*, poiché solamente la combinazione tra questi due fattori può garantire la realizzazione di un efficace processo di digitalizzazione e innovazione, senza in alcun modo pregiudicare la sicurezza del Paese, oggigiorno tutelata dal Perimetro Nazionale di Sicurezza Cibernetica, ma anche la tutela della dignità dei singoli cittadini.

L' *Authority* evidenzia inoltre la fondamentale importanza del dialogo tra le istituzione e il Garante stesso, nell'ambito della progettazione delle riforme e della loro attuazione. In virtù della propria indipendenza, l'Autorità potrà fornire preziosi e costruttivi spunti e contributi volti al bilanciamento di interessi spesso contrapposti come quello del progresso tecnologico e della tutela dei diritti e libertà individuali.

Ancora, non soltanto il rispetto dei principi consacrati dal GDPR, ma sarà necessario prestare particolare attenzione e dovizia alle garanzie offerte da fornitori e subfornitori, soprattutto ai *players Over The Top* (OTT) di tecnologie quali cloud e intelligenza artificiale.

Sul punto, il PNRR menziona espressamente la c.d. strategia *cloud first*: le Pubbliche Amministrazioni potranno scegliere se migrare verso una nuova infrastruttura *cloud* nazionale all'avanguardia ("Polo Strategico Nazionale" o PSN) o verso una soluzione pubblica sicura, tenendo in debita considerazione la tipologia di dati personali coinvolti nel trattamento, del volume dei dati trattati e del tipo di servizi erogati.

La digitalizzazione della Pubblica Amministrazione (PA) rappresenta uno degli obiettivi prioritari nel Piano Nazionale di Ripresa e Resilienza. Per raggiungere questo obiettivo, sono state previste molteplici misure finalizzate a garantire a cittadini e imprese servizi pubblici di maggiore qualità, efficienza e modernità.

Le infrastrutture digitali, nel privato come nel pubblico, di fatto, ricoprono un ruolo di fondamentale importanza rispetto alla ormai maggior parte delle attività che i cittadini pongono in essere ogni giorno, e formano la colonna portante del sistema di servizi digitali che le Pubbliche Amministrazioni utilizzano ed erogano a cittadini e imprese. Assicurare l'autonomia tecnologica del Paese, in un momento storico dove gran parte degli interessi nazionali viaggia in rete, appare oltremodo mandatorio, e risulta altresì strumentale a garantire il controllo sulla sicurezza dei dati dei cittadini aumentando, nel contempo, la resilienza dei servizi digitali.

Alla luce di quanto sopra, risulta oltremodo di fondamentale importanza la corretta definizione di tutti i fornitori coinvolti nella *supply chain*, anche in considerazione dei trasferimenti di dati personali verso Paesi Extra EU.

La sentenza C-311/18 della CGUE[1], passata ai posteri come "*Schrems II*", ha imposto a tutte le organizzazioni, sia pubbliche che private, profonde riflessioni sulle strategie di *compliance* da adottare, alterando gli equilibri dell'ecosistema digitale a livello globale. La succitata decisione inciderà inevitabilmente anche sull'attuazione del PNRR essendo il *cloud computing* una tecnologia imprescindibile per un effettivo processo di digitalizzazione del Paese e per garantire l'effettiva erogazione di servizi al cittadino a livello omogeneo su tutto il territorio nazionale.

Sul punto, recentemente l'*European Data Protection Supervisor (EDPS)* ha condotto delle analisi[2] atte a verificare la compatibilità con i principi espressi dalla sentenza *Schrems II* dei contratti stipulati da Istituzioni Europee con due dei principali OTT statunitensi di *Cloud Services*, *Amazon Web Service (AWS)* e *Microsoft*. Secondo il parere dell'EDPS, i trasferimenti di dati personali verso gli Stati Uniti si caratterizzano per la particolare criticità. Alla luce di quanto indicato, e tenendo in debita considerazione l'importanza che il *cloud computing* rivestirà in futuro nello sviluppo delle infrastrutture statali, l'EDPS ha ritenuto opportuno delineare un'apposita strategia europea per i trasferimenti di dati personali da parte di soggetti pubblici, poggiante su un approccio *risk-based* e sui principi di *accountability*, grande novità del GDPR, e di cooperazione tra le *Authorities* nazionali e le PA.

In questa sede, particolare importanza assumeranno anche le certificazioni GDPR che permetteranno ai soggetti certificati di dimostrare il raggiungimento di un livello di adeguatezza in grado di accrescere la fiducia di utenti, clienti e fornitori, dando un chiaro segnale del positivo esito del processo di adeguamento, visibile ai terzi.

Per finire, la strategia per la digitalizzazione della Pubblica Amministrazione, propugnata nel PNRR, prevede un importante investimento in tema di interoperabilità delle banche dati. L'obiettivo è quello di migliorare la qualità dei servizi offerti, valorizzando il patrimonio informativo in possesso della PA e il cui utilizzo è stato più volte caratterizzato da gravi inefficienze dovute spesso a una mancanza di coordinamento tra le differenti amministrazioni pubbliche.

Questo scenario, come è semplice intuire, si è sempre tradotto in ulteriori costi e aggravi burocratici per cittadini e imprese.

Per trovare una soluzione al problema rilevato, l'investimento previsto nel PNRR prevede l'istituzione di una Piattaforma Digitale Nazionale Dati (PDND), al cui interno ogni ente pubblico potrà condividere e rendere disponibili, in questi modo, le proprie informazioni attraverso una lista di interfacce digitali (*Application Programming Interface o API*). L'interoperabilità delle banche dati porterà ad una sensibile riduzione dei costi di gestione e a un drastico abbattimento dei tempi di condivisione, spesso lenti a causa della forte burocratizzazione che caratterizza i processi delle Pubbliche Amministrazioni.

I cittadini e le imprese potranno accedere ai servizi pubblici sulla base del principio "*once only*", un concetto di *e-government* per cui cittadini e imprese debbano poter fornire "una sola volta" le loro informazioni ad autorità ed amministrazioni, comunicando quindi in un'unica soluzione le informazioni necessarie alle diverse amministrazioni interessate. A tal riguardo, l'Agenzia per l'Italia Digitale adotterà le Linee Guida definirà i criteri tecnici e gli standard tecnologici per la gestione della Piattaforma Digitale Nazionale Dati, nonché il processo di accreditamento e di fruizione del catalogo API.

Circa gli impatti di tale sistema sui dati personali si è pronunciato il Garante per la Protezione dei Dati Personali. Con parere favorevole dell'8 luglio 2021[3], l'Authority dà atto ad AGID di aver definito un quadro di garanzie e di misure volte ad assicurare l'integrità e la riservatezza dei dati personali, spesso anche particolarmente delicati e sensibili, oggetto di scambio tra le banche dati, rispettando le esigenze di *privacy by design* e *privacy by default*, in coerenza con gli obblighi stabiliti dal GDPR.

Per concludere, il PNRR nella missione Digitalizzazione assegna incentivi e crediti d'imposta alle imprese per prodotti informatici e per programmazione informatica, consulenze e servizi connessi. Questa spinta porterà anche le aziende del settore privato ad intraprendere un rapido percorso verso la digitalizzazione. I *trend* registrati ad oggi, infatti, vedono anche nel settore privato l'adozione del *cloud computing*, l'introduzione degli algoritmi di intelligenza artificiale, la connessione informatica di oggetti e device (c.d. *Internet of Things* o *IoT*), l'evoluzione della robotica nei sistemi di produzione e della robotica dei processi (*Robotic Process Automation o RPA*), quale *driver* per l'esecuzione di attività routinarie o di basso valore aggiunto con la conseguente possibilità di riqualificare il proprio personale verso attività a maggior valore aggiunto.

Anche in questo ambito sarà quindi fondamentale definire degli appropriati processi di *privacy by design e by default*, individuando la necessità di trattare dati personali, specificandone le finalità ed individuando le corrette basi giuridiche che ne legittimano il trattamento, avendo cura di rispettare i principi fondamentali sanciti nel *GDPR*.

Dovranno essere individuati i soggetti che trattano i dati, autorizzandoli attraverso specifiche istruzioni ovvero, se esterni, provvedendo alla valutazione delle necessarie nomine di responsabile del trattamento. Particolare importanza sarà ricoperta dall'identificazione di tutta la catena della *supply chain*, in modo tale da avere il controllo sul processamento dei dati.

Nei servizi *cloud*, e non solo, ha particolare rilevanza l'individuazione dei luoghi ove avvengono i trattamenti per poter individuare le corrette garanzie per gli eventuali trasferimenti al fuori dello Spazio Economico Europeo.

L'evoluzione della digitalizzazione deve essere supportata da una parallela evoluzione delle misure di protezione informatica, le quali, però, potrebbero introdurre qualche problematica legata al potenziale controllo dei lavoratori a distanza. Un'attenta analisi del bilanciamento degli interessi deve guidare verso modalità di gestione opportune, da concordare con i soggetti preposti secondo quanto definito dallo Statuto dei lavoratori.

Sempre in tema di evoluzione della digitalizzazione, particolare attenzione dovrà essere posta agli algoritmi che rischiano di ledere i diritti fondamentali degli interessati, quali ad esempio quelli in grado di prendere decisioni autonome in merito agli interessati o quelli che ne eseguono profilazioni atte ad individuare attitudini o abitudini comportamentali. In questi casi deve essere svolta un'accurata valutazione dell'impatto sui diritti degli interessati, posto il rispetto dei principi del GDPR, valutando le adeguate modalità e le adeguate misure di protezione.

Senza dimenticare, altresì, che l'interessato ha il diritto di non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato: a tal fine sarà oltremodo necessario informarlo del diritto di ottenere un intervento umano e adottare le necessarie disposizioni procedurali per garantirgli la contestazione della decisione.

---

[1] *Corte di Giustizia dell'Unione Europea (CGUE), Causa C-311/18, Data Protection Commissioner v. Facebook Ireland Limited e Maximillian Schrems, 16 luglio 2020, https://eur-lex.europa.eu/legal-content/it/ALL/?uri=CELEX:62018CJ0311.*

[2] *https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opens-two-investigations-following-schrems_en.*

[3] *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9682994.*

Approfondimento

PNRR e Cybersecurity

di ***Alessandro Leone***
Partner Grant Thornton FAS

A livello globale gli attacchi informatici sono in continuo aumento, a dimostrazione di quanto le competenze e le risorse di coloro che hanno un interesse a violare i sistemi di sicurezza siano consistenti e pervasive. Infatti, sia le PMI sia le grandi organizzazioni più preparate e con più risorse, siano esse pubbliche o private, subiscono attacchi informatici, spesso di successo, i quali causano ingenti danni finanziari, ma anche e soprattutto all'immagine e alla reputazione.
Un attacco informatico recentemente al centro del dibattito pubblico è quello che lo scorso luglio ha colpito i sistemi informatici di una pubblica amministrazione regionale italiana. L'attacco ha messo in luce diverse aree di miglioramento nel sistema di difesa. Tale attacco ha causato l'interruzione di un'intera macchina regionale, in quanto la diretta conseguenza dal punto di vista pratico è stata il congelamento dell'intera rete dei servizi regionali, incluso quello relativo alla gestione dei vaccini, con tempi di ripristino non trascurabili. Secondo alcuni studi in Italia il costo complessivo per aziende e cittadini relativo ad attacchi informatici nel 2021 sarà di circa 6.000 miliardi di dollari[4].

Inoltre, come lo stesso Ministro Colao ha precisato, quasi il 95% dei server delle pubbliche amministrazioni sarebbe a rischio di attacchi informatici. Eppure la *cybersecurity* è spesso considerata dalle organizzazioni come un costo di cui è possibile fare a meno, piuttosto che come un investimento. Al contrario, è chiaro che la messa in sicurezza dei sistemi informatici conduca ad un costo inferiore rispetto al valore del rischio di un attacco informatico, con perdita dei dati o interruzione delle normali operazioni.
L'innovazione tecnologica e la transizione digitale degli ultimi anni sono in continua e veloce espansione, contribuendo ad incentrare sempre più il concetto della competitività dei *business* sulla capacità di adottare adeguate soluzioni tecnologiche all'avanguardia e di sviluppare nuove applicazioni in grado di facilitare e velocizzare le operazioni, di aumentare l'efficienza e di ridurre i costi. Conseguentemente, per raggiungere tali obiettivi è necessario pianificare una solida strategia di *cybersecurity*, intesa come la prassi di protezione dei sistemi, delle reti e dei programmi dagli attacchi digitali, i quali sono solitamente finalizzati all'accesso, alla modifica e alla diffusione non autorizzati di dati sensibili o all'interruzione delle operazioni aziendali[5]. La *cybersecurity* opera trasversalmente su diversi livelli di protezione e si basa sull'integrazione di persone, processi e tecnologie per costruire una difesa robusta e garantire la riservatezza, l'integrità e la disponibilità delle informazioni (c.d. *CIA Paradigm*, da *Confidentiality*, *Integrity* e *Availablity*).

La struttura normativa della *cyber* sicurezza italiana è costituita da una pluralità di interventi volti a delineare un'architettura ancora in fase di costruzione. Il 16 dicembre 2020 la Commissione ha pubblicato l'"*EU Cybersecurity Package*", un insieme di regolamenti, direttive e linee guida di *policy* sulla sicurezza informatica, al cui interno in particolare troviamo la Direttiva EU 2016/1140 (*NIS Directive*), e il Regolamento EU 2019/881 sull'ENISA (*EU Cybersecurity Act*). La Direttiva NIS è il primo vero e proprio documento legislativo sulla *cybersecurity* e costituisce un intervento centralizzato finalizzato al raggiungimento di un livello minimo di sicurezza dei *network* e dei sistemi informativi comune in Europa, e in Italia è stata recepita con il Decreto Legislativo n.65/2018. Le principali richieste, in linea con le esigenze di centralizzazione e coordinamento delle informazioni sugli incidenti e sulle vulnerabilità *cyber*, sono l'identificazione di un punto unico di contatto a livello nazionale ed europeo nella cooperazione con le Autorità NIS e con la Commissione Europea, e la creazione di un unico centro di risposta agli incidenti attraverso l'istituzione di un *Computer Security Incident Response Team (CSIRT)*.
L'ENISA, "Agenzia dell'Unione Europea per la Cibersicurezza", ha lo scopo di garantire un elevato ed effettivo livello di sicurezza del *network* e delle informazioni e di incentivare l'affermarsi di una cultura su tale sicurezza per il beneficio dei cittadini, consumatori, aziende e organizzazioni del settore pubblico nel perimetro europeo per assicurare il funzionamento del mercato interno. I principali compiti svolti dall'ENISA sono: (i) la raccolta di informazioni appropriate per l'analisi dei rischi correnti ed emergenti relativi al mondo digitale per le Istituzioni europee e le Autorità degli Stati Membri; (ii) la facilitazione della cooperazione tra la Commissione e gli Stati Membri nello sviluppo di metodologie comuni per prevenire, individuare e risolvere problemi di sicurezza dei *network* e delle informazioni; (iii) il tracciamento dello sviluppo di standard per prodotti e servizi sulla sicurezza dei *networks* e delle informazioni.
In generale, il quadro della *governance* nazionale in materia di *cybersecurity* è rimesso agli organi della sicurezza nazionale, i quali sono chiamati non soltanto a svolgere l'attività informativa attraverso i sistemi digitali, ma anche ad intervenire in ottica di prevenzione, risposta e resilienza.
In Italia il tema della *cybersecurity* deve ancora essere affrontato in modo strutturato, ma è all'attenzione del decisore politico anche nella fase di attuazione del Piano Nazionale di Ripresa e Resilienza, il quale si articola in sedici componenti raggruppate in sei macro missioni tra cui si inserisce la trasformazione digitale. Con riferimento a tale ambito, il PNRR individua tre obiettivi complessivi: la digitalizzazione della PA, l'innovazione della PA e l'innovazione organizzativa del sistema giudiziario. Il raggiungimento di obiettivi di crescita digitale e di modernizzazione della PA costituisce una priorità per la ripresa e il rilancio del paese. Inoltre, la digitalizzazione dei sistemi e dei servizi della PA è ormai un tema non più rimandabile per far sì che la PA sia percepita dai cittadini e dalle imprese come un vero e proprio "alleato" richiamando il termine utilizzato nel PNRR, in grado di ridurre radicalmente le distanze, e dunque le tempistiche burocratiche, tra enti e individui.

Questo è ancora più vero alla luce della transizione "forzata" allo *smart working* resa necessaria dalla pandemia da Covid-19 che ha colpito l'economia italiana più di altri Paesi europei e che ha evidenziato i ritardi accumulati dalla PA.
Il percorso di digitalizzazione della PA si basa in *primis* sullo stanziamento di 620 milioni di euro e si articola in sette aree d'investimento, tra cui si inserisce la *cybersecurity*.
Il primo ambito di intervento riguarda le infrastrutture digitali con l'adozione di un approccio "*cloud first*" in base al quale le amministrazioni devono progressivamente abbandonare le infrastrutture IT proprietarie per convertirsi alla tecnologia *cloud*. Tale misura si è resa necessaria in quanto i centri di raccolta dati delle pubbliche amministrazioni italiane non assicurano un adeguato livello di sicurezza informatica. L'Agenzia per l'Italia Digitale (AGID), preposta al coordinamento della digitalizzazione della PA, ha strutturato la strategia del "*cloud first*" su tre direttrici che le PA possono scegliere di seguire con riferimento alle infrastrutture verso le quali migrare: (i) infrastrutture offerte dai *Cloud Service Providers (CSPs)* privati autorizzati e indicati in appositi registri dalla stessa AGID; (ii) infrastrutture di *Community Cloud* contrattualizzate tramite CONSIP;
(iii) infrastrutture messe a disposizione dal Polo Strategico Nazionale (PSN).
Il secondo ambito di intervento prevede un programma di supporto e incentivo per la migrazione al *cloud* nella fase di analisi tecnica e di definizione delle priorità rivolto in particolare alle amministrazioni locali.

La terza misura di investimento riguarda i dati e l'interoperabilità e cerca di soddisfare l'obiettivo della trasformazione digitale delle PA cambiando il *design* e le modalità di interconnessione tra le banche dati affinché vi sia un accesso trasversale e universale ai dati secondo il principio del "*once only*" il quale stabilisce che le informazioni devono essere richieste ai cittadini una sola volta, con conseguente riduzione dei tempi e dei costi legati alla registrazione delle stesse.
A tale scopo, il PNRR stabilisce la necessità di creare una Piattaforma Nazionale di Dati (PND) *ad hoc* accessibile tramite un servizio apposito e conforme ai requisiti *privacy* del GDPR, evitando al cittadino di fornire le stesse informazioni a più amministrazioni.
Il quarto investimento è diretto al rafforzamento e al miglioramento dell'efficienza dei servizi digitali e della cittadinanza digitale attraverso una più massiccia diffusione di PagoPA[6] e dell'app IO[7], l'introduzione di nuovi servizi digitali anche nel settore mobilità, e un intervento organico per migliorare la *user experience* dei servizi digitali.

L'ampliamento del perimetro digitale rende conseguentemente le organizzazioni ancora più vulnerabili ad attacchi informatici, in quanto i dati raccolti e processati costituiscono il *target* più profittevole agli occhi degli "*intruders*" per il solo fatto di contenere informazioni personali e sensibili. A titolo esemplificativo, secondo alcune stime[8] il valore medio di una cartella clinica venduta sul *Dark Web* si aggira sui 1.000 dollari.

A tal proposito, il legislatore ha ritenuto opportuno dedicare il quinto ambito di intervento esclusivamente alla sicurezza informatica, partendo dall'attuazione della disciplina in materia di "Perimetro di Sicurezza Nazionale Cibernetica". In particolare, gli investimenti riservati alla *cybersecurity* si suddividono in quattro aree di intervento:

1. rafforzamento dei presidi di *front-line* per la gestione degli *alert* e degli eventi a rischio intercettati verso la PA e le imprese di interesse nazionale;
2. costruzione e/o consolidamento delle capacità tecniche di valutazione e *audit* continuo della sicurezza degli apparati elettronici e delle applicazioni utilizzate per l'erogazione di servizi critici da parte di soggetti che esercitano una funzione essenziale;
3. immissione di nuovo personale sia nelle aree di pubblica sicurezza e polizia giudiziaria dedicate alla prevenzione e investigazione del crimine informatico diretto contro singoli cittadini, sia in quelle dei comparti preposti a difendere il paese da minacce cibernetiche;
4. consolidamento degli *asset* e delle unità *cyber* incaricate della protezione della sicurezza nazionale e della risposta alle minacce *cyber*.

La sesta area di investimento si concentra sulla digitalizzazione delle grandi amministrazioni centrali e copre vari ambiti della PA, quali ad esempio la Giustizia, il Lavoro, la Difesa, gli Interni e la Guardia di Finanza.

L'ultima misura di intervento riguarda il rafforzamento delle competenze digitali di base dei cittadini, con il fine di garantire un supporto nel percorso di alfabetizzazione digitale.

Inoltre, ai fini di questo articolo, si riporta l'intento del legislatore a digitalizzare, innovare e mantenere la competitività nel sistema produttivo attraverso gli investimenti per le connessioni ultraveloci in fibra ottica 5G. Queste costituiscono un requisito primario per la realizzazione della *gigabit society* e per consentire alle imprese di usufruire di diverse tecnologie 4.0 (quali sensori, *Internet of Things – IoT* , stampanti tridimensionali[9]). La connessione alla rete e le molteplici interconnessioni tra dispositivi portano da un lato diversi benefici in termini di interazioni con i dati in tempo reale, ma dall'altro aumentano inevitabilmente il perimetro d'attacco. Se da una parte gli esperti lavorano sulla prevenzione e la gestione dei rischi informatici in contesti dinamici, d'altra parte vi è un elemento che rimane al di fuori del loro controllo: il fattore umano, ossia il comportamento degli utenti nell'utilizzo dei dispositivi.

Il primo vero e proprio scudo di protezione è rappresentato dal rispetto delle *best practices* rivolte agli *users*, le quali possono variare da una corretta gestione delle *password* e delle credenziali d'accesso, a un'attenta gestione delle *e-mail* sospette, o dalla connessione a una rete sicura, alla sicurezza fisica dei dispositivi.

Infine, il PNRR nella missione Digitalizzazione assegna incentivi e crediti d'imposta alle imprese per prodotti informatici e per programmazione informatica, consulenze e servizi connessi.

Questa spinta porterà anche le aziende del settore privato ad intraprendere un rapido percorso verso la digitalizzazione. I *trend* registrati ad oggi, infatti, vedono anche nel settore privato l'adozione del *cloud computing*, l'introduzione degli algoritmi di intelligenza artificiale, la connessione informatica di oggetti e *device* (c.d. I*nternet of Things o IoT*), l'evoluzione della robotica nei sistemi di produzione e della robotica dei processi (*Robotic Process Automation o RPA*), quale *driver* per l'esecuzione di attività routinarie o di basso valore aggiunto con la conseguente possibilità di riqualificare il proprio personale verso attività a maggior valore aggiunto.

In questo contesto la *cybersecurity* ricopre un ruolo fondamentale per difendere il patrimonio informatico e per sostenere lo sviluppo futuro, sia nelle Pubbliche Amministrazioni, sia nel settore privato. Ad oggi si riscontra che in molti casi Enti pubblici ed aziende del settore privato devono ancora identificare i ruoli e le responsabilità per la gestione della sicurezza informatica e devono ancora strutturare uno specifico processo di gestione.

In particolare, è necessario definire un processo di analisi dei rischi che consenta di allineare gli investimenti in ambito della sicurezza informatica con gli obiettivi strategici, coinvolgendo opportunamente tutta la catena di comando.

È quindi indispensabile andare a normare tutti i processi cardine della sicurezza: la gestione degli accessi ai sistemi informatici in modo tale che solo le persone autorizzate possano accedere alle informazioni, avendo cura di restringere anche a loro l'ambito alle solo informazioni necessarie; la gestione degli accessi fisici alle sedi e ai locali tecnici; la gestione delle dotazioni personali assegnate; la classificazione delle informazioni e la relativa protezione; la definizione delle corrette procedure di *backup* e di ripristino, nonché le procedure di continuità operativa, eccetera. Devono inoltre essere individuati gli opportuni apparati di sicurezza (a mero titolo esemplificativo: *firewall*, SIEM, antivirus / *end point protection*, ecc.) a protezione della propria infrastruttura ed essere individuati i progetti di miglioramento della sicurezza attraverso una rivalutazione continua. Infine, un buon processo di gestione della sicurezza deve essere dotato di indicatori di rischio e di *performance* con processi di monitoraggio, anche in tempo reale, degli allarmi e dei rischi al fine di poter avviare tempestivamente una risposta all'insorgere delle minacce.

---

[4] *'Cyber Security, approccio sistemico e sostegno alle PMI, Il Sole 24 Ore, 18 agosto 2021 di E. Ferretti.*

[5] *CISCO.*

[6] *Piattaforma di pagamenti tra la PA e cittadini e imprese, PNRR.*

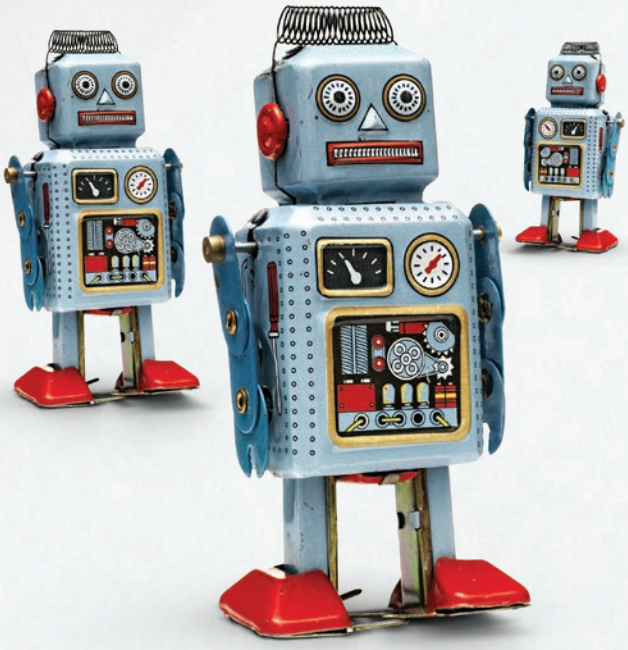
[7] *Front-end/ canale versatile che mira a diventare il punto di accesso unico per i servizi digitali della PA.*

[8] *"Attacchi hacker, dati sanitari in pericolo: la lista segreta dei 35 ospedali colpiti", Corriere della Sera, di M. Gabanelli e S. Ravizza, 28 settembre 2021.*

[9] *Classificazione ripresa dal PNRR.*

STATUS QUO IS ONE OF MANY.

Audit | Tax | Advisory



Status Go™

IS ONE-ON-ONE.

Ready for an approach that's as unique as it is personal?

Welcome to Status Go.

grantthornton.global

Grant Thornton