Camera dei Deputati – Senato della Repubblica

Commissione parlamentare di vigilanza sull'anagrafe tributaria

Audizione del Direttore dell'Agenzia delle entrate

Avv. Ernesto Maria Ruffini

Indagine conoscitiva
Sicurezza delle banche dati dell'anagrafe tributaria e tutela della riservatezza dei dati dei contribuenti

Roma, 24 luglio 2024

Sommario

Premessa

Signor Presidente, Onorevoli Commissari,

desidero, innanzitutto, ringraziare questa Commissione per l'opportunità concessa all'Agenzia delle entrate di fornire il proprio contributo nell'ambito dell'**indagine conoscitiva** sulla *«**Sicurezza delle banche dati dell'anagrafe tributaria e tutela della riservatezza dei dati dei contribuenti**»*.

Negli ultimi anni, l'Agenzia delle entrate ha posto in essere, per il perseguimento dei propri fini istituzionali, un processo di trasformazione digitale che interessa tutta l'azione amministrativa, volto a garantire una maggiore semplificazione dei rapporti con i contribuenti, sia nell'erogazione dei servizi, sia nella fase dei controlli fiscali, nel rispetto della *privacy* dei cittadini.

L'Agenzia aggiorna annualmente la propria **strategia digitale** allo scopo di valorizzare al massimo il patrimonio informativo a sua disposizione, garantendo allo stesso tempo la legittimità degli accessi e, più in generale, la sicurezza e la protezione dei dati.

Per la progettazione e la realizzazione delle soluzioni tecnologiche – incluse quelle relative alla *cybersecurity* e alla protezione dei dati – l'Agenzia si avvale del ***partner* tecnologico Sogei**, sulla base di un contratto esecutivo definito nell'ambito di un atto regolativo stipulato tra il Ministero dell'economia e delle finanze – Dipartimento delle finanze e la stessa Sogei, finalizzato allo sviluppo, all'evoluzione e alla conduzione operativa del Sistema Informativo della Fiscalità (SIF).

1. Il patrimonio informativo dell'Agenzia delle entrate

L'Agenzia delle entrate è titolare di un **ampio patrimonio informativo,** costituito da numerose banche dati, anche di grandi dimensioni, eterogenee per struttura e contenuto, soggette a costante aggiornamento e con un'importante profondità temporale.

Tale patrimonio informativo viene costantemente incrementato sia dai dati che l'Amministrazione acquisisce direttamente nell'ambito dei processi amministrativi (fiscali e immobiliari) di propria competenza, sia dai **flussi informativi provenienti da enti esterni**, per effetto di specifiche disposizioni normative.

Si tratta, in particolare, di informazioni che pervengono all'Agenzia per il tramite di comunicazioni trasmesse attraverso i **canali digitali**, sia direttamente dai contribuenti o da loro intermediari abilitati (dichiarazioni dei redditi, atti soggetti a registrazione, pagamenti con modelli F24 e F23, dichiarazioni di inizio attività, fatturazione elettronica, corrispettivi, ecc.), sia da enti esterni (operatori finanziari, società erogatrici di servizi, assicurazioni, CCIAA, INPS, INAIL, Comuni, ecc.).

Il patrimonio informativo così costituito alimenta e aggiorna costantemente i *database* di

piattaforme di analisi e applicativi informatici, progettati e gestiti a livello centrale e utilizzati dalle strutture territoriali dell'Agenzia, da enti esterni abilitati all'accesso, nonché, naturalmente, da parte degli stessi cittadini, imprese e loro intermediari, attraverso i servizi *online* messi a disposizione.

L'Agenzia ha inoltre definito una complessiva strategia di sviluppo di tecniche di analisi sui cosiddetti "***big data***", anche mediante l'utilizzo di tecniche di intelligenza artificiale, finalizzata a superare le tradizionali tecniche di analisi a favore di approcci innovativi e in linea con lo stato dell'arte della rapida evoluzione tecnologica in quest'ambito.

2. L'accesso da parte dei dipendenti ai sistemi informatici e alle banche dati dell'Agenzia delle entrate e le misure di prevenzione e contrasto degli accessi abusivi

2.1 Il sistema di gestione dei dati personali

L'Agenzia delle entrate, insieme all'Agenzia delle entrate-Riscossione, si è dotata di un **Sistema di gestione per la protezione dei dati personali** realizzato secondo gli *standard* internazionali ISO/IEC 27000, dando così attuazione al principio di responsabilizzazione (*accountability*), che impone al titolare del trattamento dei dati personali di mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che ogni trattamento è effettuato **conformemente al Regolamento Generale sulla Protezione dei Dati**[1].

Si tratta di uno strumento di carattere organizzativo e gestionale utilizzato per rispettare, in modo **visibile e dimostrabile**, i criteri ed i requisiti previsti dalla normativa europea e nazionale in materia di protezione dei dati personali.

In particolare, il Sistema di gestione per la protezione dei dati personali ha lo scopo di:

- definire il contesto del trattamento dei dati personali;
- individuare e classificare le risorse e gli strumenti impiegati nel trattamento;
- identificare e gestire i rischi connessi al trattamento;
- incrementare la competenza e la consapevolezza del personale riguardo la sicurezza ed i rischi connessi al trattamento dei dati personali;
- applicare i principi e le regole imposte delle normative nazionali ed europee;
- incrementare la fiducia dei portatori di interesse;

[1] Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, di seguito RGPD.

- rafforzare l'immagine e migliorare l'affidabilità dell'organizzazione.

Attraverso il Sistema di gestione per la protezione dei dati personali viene garantito un presidio di sicurezza sul trattamento dei dati personali nelle sue tre componenti: **organizzativa**[2], **fisica**[3] e **tecnologica**[4].

2.2 Le misure per gli accessi alle banche dati da parte dei dipendenti dell'Agenzia

Le regole di accesso e di utilizzo degli applicativi e delle banche dati gestite dall'Agenzia delle entrate sono ispirate al rispetto dei **principi di necessità**, **pertinenza**, **non eccedenza** e **minimizzazione del trattamento dei dati personali** previsti dal **RGPD** (Regolamento Generale sulla Protezione dei Dati) e dal codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196, come modificato dal decreto legislativo 10 agosto 2018, n. 101).

Ogni utente, pertanto, è abilitato dal diretto responsabile ad accedere solo agli applicativi informatici e alle banche dati, tra cui l'Anagrafe Tributaria, di cui ha bisogno per eseguire i compiti e le mansioni che gli vengono affidati.

Tutte le applicazioni, prima di consentire qualsiasi trattamento dei dati, interagiscono con il sistema di controllo accessi affinché tutti gli operatori che vogliono accedere siano preventivamente

---

[2] Il presidio alla sicurezza dei dati si attua attraverso l'individuazione dei ruoli e delle responsabilità, l'emanazione di istruzioni e l'utilizzo di apposite procedure. Al riguardo, il Sistema di Gestione per la protezione dei dati personali è composto dal Manuale e da specifica documentazione, nonché da procedure operative che comprendono anche la tenuta del Registro delle attività di Trattamento, del Registro delle istanze degli interessati, del Registro delle violazioni dei dati personali, la metodologia per effettuare l'Analisi del rischio e la Valutazione d'impatto. L'adempimento degli obblighi previsti dalla normativa *privacy* viene effettuato dai Responsabili delle strutture dell'Agenzia, per competenza rispetto ai processi organizzativi presidiati, rimanendo in capo all'Agenzia delle entrate la qualità di titolare dei trattamenti dei dati personali. Ciascun dipendente viene autorizzato al trattamento dei dati personali in relazione ai processi che ricadono nelle competenze dell'ufficio al quale è assegnato con un formale ordine di servizio, per un periodo di tempo non superiore a quello necessario in riferimento alle finalità del trattamento stesso. Un incarico formale al trattamento dei dati è invece necessario nei casi in cui un dipendente sia chiamato ad eseguire un trattamento di dati personali riferito a processi che esulano dalle competenze dell'ufficio nel quale è incardinato (ad esempio, nel caso di partecipazione ad un gruppo di lavoro con competenze trasversali). Ampio spazio viene attribuito alla formazione e all'aggiornamento dei dipendenti, con l'erogazione periodica di corsi in materia di sicurezza e di protezione dei dati a tutto il personale dell'Agenzia.

[3] Motivi di *privacy* e di sicurezza impongono misure organizzative di controllo degli accessi, quali la dotazione di cartellini di riconoscimento dei dipendenti e misure logistiche di chiusura di stanze, armadi e di archivi.

[4] Ogni dipendente è abilitato dal diretto responsabile ad accedere solo agli applicativi informatici e alle banche dati, tra cui l'Anagrafe tributaria, di cui ha bisogno per eseguire i compiti e le mansioni che gli vengono affidati. Tutte le applicazioni, prima di consentire qualsiasi trattamento dei dati, interagiscono con il sistema di controllo degli accessi affinché tutti gli operatori che vogliono accedere siano preventivamente identificati e autenticati e ne sia verificata sui sistemi l'autorizzazione all'accesso. Inoltre, tutte le abilitazioni del personale sono riviste e aggiornate con periodicità trimestrale. Sugli accessi alla banca dati e sulle operazioni svolte dagli utenti viene effettuata un'attività di tracciamento per le finalità di sicurezza. Sulla base dei *log* di accesso vengono raccolte evidenze per individuare eventuali attività illecite svolte sui sistemi informativi, utili per finalità di controllo interno nei confronti del personale dipendente o per rispondere a possibili richieste di informazioni provenienti dall'Autorità giudiziaria.

identificati e autenticati e ne sia verificata sui sistemi l'autorizzazione all'accesso.

L'**autenticazione dell'operatore** avviene sempre utilizzando almeno un fattore di autenticazione, la *password* di accesso, sottoposta a una specifica *password policy* con opportune caratteristiche di sicurezza quali la lunghezza minima, la scadenza e il blocco in caso di ripetuti errori di inserimento.

La **gestione delle abilitazioni** è supportata da uno specifico applicativo informatico (SIGA 3.0) con l'obiettivo di promuovere e garantire la coerenza tra le linee di lavoro richieste e quelle effettivamente necessarie alle funzioni svolte da ogni dipendente-utente del sistema, sia al momento della concessione dell'abilitazione all'accesso alle informazioni contenute nella banca dati, sia durante il successivo svolgimento dell'attività lavorativa. La regolamentazione prevede, in linea generale, la verifica delle abilitazioni con frequenza trimestrale, ma essa deve essere effettuata ogni qual volta si renda necessario, ad esempio:

- a seguito di cambio di mansione di uno o più operatori;
- quando un operatore è assegnato all'Ufficio o trasferito ad altro Ufficio.

Il **Codice di comportamento dei dipendenti dell'Agenzia**, inoltre, detta specifiche e dettagliate disposizioni per l'utilizzo dei sistemi informatici (articolo 18) e per l'accesso alle banche dati (articolo 19); ne consegue che i comportamenti tenuti dai dipendenti in contrasto con le citate disposizioni costituiscono, anzitutto, illecito disciplinare, con l'applicazione di sanzioni di elevato tenore, in alcuni casi finanche espulsive e, ricorrendone i presupposti, illecito penale per violazione dell'articolo 615-*ter* c.p.

Sotto il profilo del **controllo successivo** e del **contrasto agli accessi abusivi** svolto dall'Agenzia rilevano i seguenti strumenti.

- Il **tracciamento di tutti gli accessi e degli utilizzi dei sistemi informatici**, con lo scopo di raccogliere e analizzare le informazioni di *log*[5] delle operazioni effettuate. Il sistema di tracciamento, i cui dati sono gestiti e conservati da Sogei, costituisce anche una fondamentale misura di dissuasione nei confronti degli operatori, attesa la possibilità di ricostruire le attività di accesso, collegandole a una precisa identificazione dell'utente e della postazione da cui accede. Sulla base dei *log* di accesso vengono raccolte evidenze per individuare eventuali attività illecite svolte sui sistemi informativi, utili per finalità di *audit* interno nei confronti del personale dipendente o per rispondere a possibili richieste di informazioni provenienti

[5] Il *log* è una registrazione sequenziale e cronologica delle operazioni effettuate da un sistema informatico.

dall'Autorità giudiziaria.

- Sono stati sviluppati percorsi di **analisi informatizzata dei dati relativi agli accessi alle banche dati finalizzata ad evidenziare comportamenti potenzialmente anomali** degli operatori. Gli esiti di tali analisi costituiscono fonti d'innesco per successivi approfondimenti istruttori o per lo svolgimento di indagini amministrative ed eventualmente per segnalazioni agli organi disciplinari e all'Autorità giudiziaria.
- L'applicativo informatico ***Mistral***, in uso dal febbraio 2018 e sviluppato anche in attuazione di misure tecniche ed organizzative richieste dal Garante per la Protezione dei Dati Personali, consente di individuare e inviare automaticamente ad ogni responsabile di struttura **segnalazioni di accessi potenzialmente anomali** effettuati dagli operatori dell'ufficio ai dati dell'Anagrafe Tributaria e ad alcuni applicativi informatici di maggiore utilizzo. Ogni responsabile di struttura, a seguito della segnalazione ricevuta, ha l'obbligo di verificare la legittimità degli accessi. Sono considerati anomali gli accessi effettuati durante i giorni feriali, in caso di mancata presenza in sede del dipendente, quelli effettuati durante l'orario notturno (20.00-7.30) e durante i giorni festivi.

Nell'ambito del costante processo di evoluzione e di ammodernamento degli strumenti di cui trattasi, è attualmente in fase di analisi e sviluppo con il *partner* tecnologico una ulteriore implementazione delle modalità di accesso a Serpico mediante l'introduzione di controlli bloccanti basati sull'obbligo per l'operatore di indicare il codice identificativo della lavorazione (ID lavorazione) presente nell'applicativo di *workflow* in uso ed a lui assegnata per la quale richiede l'accesso alla banca dati.

3. L'interoperabilità delle banche dati

La digitalizzazione e la modernizzazione della Pubblica Amministrazione si fondano anche sulla costruzione di un'**infrastruttura digitale** basata sull'efficiente utilizzo delle informazioni immesse nel **sistema informativo pubblico** e, quindi, in possesso della P.A. nel suo complesso, richiedendo ai cittadini i dati necessari alla fruizione di un servizio "**una volta sola**" (c.d. principio "*once-only*").

In coerenza a tale principio, i dati **contenuti dell'Anagrafe tributaria**, nella quale confluiscono le informazioni di carattere fiscale dei contribuenti, **sono resi disponibili** dall'Agenzia **a una vasta platea di pubbliche amministrazioni ed enti** che svolgono attività di interesse pubblico e che li utilizzano per semplificare gli adempimenti a carico dei cittadini e per incrementare l'efficienza ed

efficacia delle proprie attività istituzionali.

A tale fine, l'Agenzia ha definito da tempo un **catalogo dei servizi *standard* di cooperazione informatica**, che consente di rendere noti i servizi offerti in materia di scambio di informazioni, con le relative modalità di erogazione, dandone visibilità alle categorie di enti che accedono alle banche dati; alla luce delle finalità e delle normative di riferimento. Per alcune categorie di enti è stato definito un *panel* di servizi *standard*, in continua evoluzione, che consente di uniformare il trattamento e di velocizzare l'*iter* di convenzionamento, necessario per l'accesso a tali informazioni.

Nel rispetto di quanto previsto dalla normativa sulla protezione dei dati personali, **i servizi sono messi gratuitamente a disposizione** degli enti per l'esercizio delle proprie funzioni istituzionali, in virtù di una norma di legge o di regolamento che autorizza l'ente all'accesso, attraverso un processo di autorizzazione per le finalità richieste e riconosciute pertinenti dall'Agenzia.

In linea generale, esistono tre differenti modalità di accesso controllato ai dati:

- **consultazione *online***, con la quale utenti abilitati possono effettuare interrogazioni relative a informazioni presenti nell'Anagrafe tributaria;
- **fornitura massiva**, mediante la quale le informazioni presenti in Anagrafe tributaria vengono rese disponibili attraverso scambi di flussi su protocollo di comunicazione sicuro;
- **interoperabilità**, con l'interazione diretta *machine-to-machine*, in una specifica cornice amministrativa e di sicurezza, tra i sistemi dell'Agenzia e quelli di utenti esterni.

4. Gli accessi da parte di altri enti e i sistemi di monitoraggio

4.1 Accesso in federazione da parte della Guardia di finanza

La Guardia di finanza accede ad alcune applicazioni dell'Agenzia delle entrate tramite un'infrastruttura di federazione. Accede, inoltre, al sistema informatico dei servizi catastali (SISTER), tramite i servizi telematici dedicati.

L'accesso federato è consentito esclusivamente per richieste che avvengono dalla rete della Guardia di finanza sulla base di accordi che, tra l'altro, comprendono specifiche *policy* di sicurezza. Tramite il tracciamento adottato dalla singola applicazione utilizzata, è possibile risalire all'effettivo operatore che ha avuto accesso all'applicazione, alle operazioni effettuate e ai dati consultati.

Per quanto riguarda la modalità di autenticazione, identificazione e gestione degli utenti, la Guardia di finanza adotta una procedura che prevede la verifica sistematica e la revisione periodica delle abilitazioni secondo i requisiti di sicurezza propri e nel rispetto dei requisiti previsti dalla normativa vigente.

Gli utenti autorizzati ad accedere agli applicativi dell'Agenzia sono gli appartenenti alla Guardia di finanza ai quali è stato attribuito dall'amministratore utenze del Corpo uno specifico profilo di abilitazione, previa individuazione da parte dei comandanti dei Reparti interessati. Al fine di garantire l'effettiva rispondenza delle abilitazioni attribuite agli utenti con le funzioni effettivamente svolte dagli stessi, è prevista la verifica sistematica e la revisione periodica delle abilitazioni.
L'Agenzia delle entrate, tramite Sogei, procede al tracciamento degli accessi agli applicativi e delle operazioni compiute da ciascun utente della Guardia di finanza. In particolare, gli accessi e le operazioni compiute sugli applicativi sono associati a un codice identificativo che permette esclusivamente al predetto Corpo (e non all'Agenzia) di identificare univocamente l'utente che ha effettuato l'accesso o l'operazione. Anche la Guardia di finanza procede al tracciamento degli accessi agli applicativi effettuati dagli utenti del Corpo ed effettua controlli periodici, anche a campione, per il tramite di ciascun Comandante di Reparto, per verificare il rispetto delle disposizioni regolamentari, comunicandone, in caso di criticità, l'esito all'Agenzia delle entrate. L'Agenzia delle entrate comunica tempestivamente alla Guardia di finanza le eventuali anomalie rilevate nell'utilizzo degli applicativi in esame da parte degli utenti del Corpo.

4.2 Accessi degli altri enti della fiscalità

Oltre alla Guardia di finanza, anche altri enti della fiscalità (Dipartimento delle finanze, Agenzia delle dogane e dei monopoli, Agenzia del demanio) accedono ad alcune applicazioni interne dell'Agenzia rivolte ai propri dipendenti tra cui, principalmente, *Serpico*.
I meccanismi di autenticazione degli utenti sono propri di ciascun ente, così come le politiche di gestione del ciclo di vita dell'utenza.
I profili autorizzativi assegnabili agli operatori di questi enti sono stati previamente definiti con l'Agenzia e non sono modificabili in autonomia dagli enti stessi.
Questi ultimi sono, invece, autonomi nell'abilitare i loro operatori tramite i propri gestori, utilizzando *workflow* di autorizzazione definiti in ciascuna struttura.

4.3 Accessi da parte di enti esterni al sistema informativo della fiscalità

I sistemi che consentono l'interrogazione dei dati dell'Anagrafe tributaria rivolti a utenti autorizzati di **enti esterni** al Sistema Informativo della Fiscalità sono di due tipologie:

- accesso ai dati anagrafici e fiscali (***Siatel v2.0 – PuntoFisco, ARCO***)[6];
- consultazione dei dati dell'Archivio dei rapporti finanziari (***CAR***)[7].

In entrambi i casi è previsto un sistema di controllo accessi che impone all'utente di autenticarsi e possedere specifiche autorizzazioni per poter accedere alle informazioni. I profili di abilitazione sono attribuiti all'utente dal rispettivo amministratore dell'ente, con l'eccezione dell'Archivio dei rapporti finanziari, per il quale l'intero ciclo di vita dell'utenza e delle abilitazioni è gestito dall'Agenzia[8].

In relazione al sistema ***CAR***, è presente un **doppio livello di autorizzazione** interno all'applicazione che impedisce l'accesso diretto al dato: l'utente di livello 1 inserisce le richieste di accesso ai dati e un altro utente, di livello 2, deve autorizzare l'accesso.

Tutte le misure di sicurezza descritte sono state approvate dal Garante per la protezione dei dati personali.

4.4 Accordi per l'accesso ad applicazioni dell'Agenzia da parte di amministrazioni di particolare rilevanza istituzionale

Specifiche modalità di accesso alle applicazioni in uso ai dipendenti dell'Agenzia sono previste per gli utenti appartenenti:

- al Ministero dell'interno – Direzione Investigativa Antimafia;
- al Raggruppamento Operativo Speciale dei Carabinieri (ROS);
- alla Presidenza del Consiglio dei ministri.

---

[6] Gli enti che accedono a PuntoFisco sono, a titolo esemplificativo e non esaustivo: Ministeri, Regioni, Province, Comuni e Unioni di Comuni, Città Metropolitane, Comunità montane, ANAS, ATER, ASL, ARPA, Azienda diritti studi universitari, Consorzi di bonifica, Consiglio Regionale, CAF, INPS, INAIL, Università, Consorzio Parco, Enti autonomi case popolari, Ispettorato Lavoro, Camere di commercio, DIA, *Authority* di Vigilanza e Controllo, Università. Per i predetti enti varia il profilo di accesso: alcuni hanno un profilo più esteso (ad es. dati reddituali, consultazioni massive, registro), altri hanno un profilo minimo (solo dati anagrafici).

[7] Gli enti che accedono a CAR sono: Dipartimento per la Pubblica Sicurezza - Ministero dell'Interno, DIA, Ministero della Giustizia (Procure e UNEP), Consob, Unità d'informazione finanziaria per l'Italia, Agenzia delle entrate-Riscossione.

[8] Allo scopo di fornire una indicazione quantitativa di tali accessi, si evidenzia che:

- gli **utenti** che accedono al sistema ***Siatel v2.0 - PuntoFisco*** sono circa 67.900, gli utenti ***ARCO*** sono circa 3.090, gli utenti che accedono a ***CAR*** sono circa 1.930;
- gli **enti** che accedono a ***Siatel v2.0 - PuntoFisco*** sono 9.972 di cui 7.869 comuni; oltre i Comuni, gli enti con maggior numero di utenti (oltre ai Comuni) sono INPS e Ministero della Giustizia.

5. L'attività di analisi del rischio "fiscale" e la valutazione d'impatto relativa al trattamento dei dati personali

5.1 Premessa

In generale, è utile sottolineare l'esistenza di quella che, in termini economici, si definisce "**asimmetria informativa**" tra l'Amministrazione finanziaria e i contribuenti. Le informazioni relative all'esistenza del presupposto per la debenza del tributo e la misura del prelievo sono, infatti, per lo più in possesso del contribuente. Il Fisco deve, pertanto, acquisire, direttamente o indirettamente, le informazioni necessarie al perseguimento dei fini istituzionali. Detta asimmetria informativa può essere ridotta mediante l'utilizzo delle banche dati a disposizione dell'Amministrazione finanziaria, nell'ambito delle quali è condotta l'attività di **analisi dei fenomeni evasivi**. Al riguardo, il Legislatore ne ha fornito una specifica definizione[9]. Si tratta, in particolare, di un'attività che, tramite l'**utilizzo integrato delle banche dati** di cui dispone l'Amministrazione finanziaria, è volta a individuare i contribuenti che presentano un profilo di rischio fiscale, inteso quale rischio di operare, colposamente o dolosamente, in violazione di norme di natura tributaria, ovvero in contrasto con i principi o con le finalità dell'ordinamento tributario[10].

---

[9] Ai sensi dell'articolo 2 (*Razionalizzazione e riordino delle disposizioni normative in materia di attività di analisi del rischio*) del decreto legislativo 12 febbraio 2024, n. 13, con la locuzione "analisi del rischio" (ai fini fiscali - da non confondersi con quella relativa alla tutela della *privacy*) si intende «*il processo, composto da una o più fasi, che, al fine di massimizzare l'efficacia delle attività di prevenzione e contrasto all'evasione fiscale, alla frode fiscale e all'abuso del diritto in materia tributaria, nonché di quelle volte a stimolare l'adempimento spontaneo, tramite modelli e tecniche di analisi deterministica ovvero probabilistica, nel rispetto della normativa in materia di trattamento di dati personali, utilizza, anche attraverso la loro interconnessione, le informazioni presenti nelle basi dati dell'Amministrazione finanziaria, ovvero pubblicamente disponibili, per associare, coerentemente a uno o più criteri selettivi, ovvero a uno o più indicatori di rischio desunti o derivati, la probabilità di accadimento a un determinato rischio fiscale, effettuando, ove possibile, anche una previsione sulle conseguenze che possono generarsi dal suo determinarsi*».

[10] In tema di contrasto all'evasione fiscale mediante l'utilizzo delle banche dati, è utile evidenziare che, al fine di contrastare la cosiddetta "evasione da riscossione", ossia il "*gap*" tra le maggiori imposte accertate e gli importi effettivamente incassati tramite l'attività di riscossione coattiva, con la legge di bilancio 2024 (legge 30 dicembre 2023, n. 213) è stata introdotta una misura volta a favorire l'accesso alle informazioni necessarie al potenziamento dell'azione di riscossione. In particolare, l'articolo 1, comma 100, ha previsto – in coerenza con le previsioni dell'articolo 18 della legge 9 agosto 2023, n. 111 (Delega al Governo per la riforma fiscale) – la possibilità per l'agente della riscossione di avvalersi, prima di avviare l'azione di recupero coattivo, di modalità telematiche di cooperazione applicativa e degli strumenti informatici, per l'acquisizione di tutte le informazioni necessarie al predetto fine, da chiunque detenute. In tal modo l'attività di riscossione potrà essere più semplice e veloce e, quindi, più efficiente, a vantaggio anche dello stesso debitore, grazie ad azioni esecutive, condotte dall'agente della riscossione, più mirate. Le soluzioni tecniche di cooperazione applicativa e di utilizzo degli strumenti informatici saranno definite con uno o più decreti del Ministero dell'economia e delle finanze, nel rispetto dello Statuto dei diritti del contribuente, sentito anche il Garante per la protezione dei dati personali, ai fini dell'adozione di idonee misure di garanzia a tutela dei diritti e delle libertà degli interessati. Tale garanzia sarà assicurata attraverso la previsione di apposite misure di sicurezza, anche di carattere organizzativo, in conformità alle disposizioni unionali e interne in materia di protezione dei dati personali.

L'attività di analisi del rischio viene ovviamente svolta rispettando in modo rigoroso i dettami della normativa unionale e di quella interna in materia di tutela dei dati personali[11].

Nel prosieguo, per ragioni di chiarezza espositiva, verranno separatamente illustrati gli adempimenti svolti per conformarsi alla normativa *privacy* e quelli derivanti da specifiche prescrizioni formulate dall'Autorità garante della *privacy*.

5.2 I documenti di valutazione dell'impatto sulla protezione dei dati personali

Il Regolamento *privacy* (RGPD) ha previsto nuove tutele a favore degli interessati e nuovi obblighi a carico di titolari[12] e responsabili del trattamento[13] di dati personali.

Tra le principali novità introdotte, vi sono quelle relative all'analisi del rischio ed alla valutazione d'impatto (o "***Data Protection Impact Assessment***", di seguito "**DPIA**") sulla protezione dei dati.

L'analisi del rischio sulla protezione dei dati è una procedura finalizzata a descrivere un trattamento di dati personali, valutarne la necessità e la proporzionalità, nonché la conformità legale, ed a gestirne gli eventuali rischi per i diritti e le libertà delle persone fisiche da esso derivanti, effettuando una valutazione del livello del rischio e determinando le misure – tecniche, informatiche e organizzative – idonee a mitigarlo.

L'analisi del rischio e la valutazione di impatto sulla protezione dei dati rappresentano, dunque, uno strumento essenziale per la **tutela dei dati personali** e sono diretta espressione del **principio della responsabilizzazione** (cd. *accountability*), in forza del quale ciascun titolare deve, in prima battuta, auto-valutare il livello di rischio dei propri trattamenti e adottare le necessarie misure di tutela.

In particolare, l'articolo 35, comma 1, del RGPD – nelle ipotesi in cui da un trattamento possa derivare un rischio elevato per i diritti e le libertà delle persone interessate – obbliga il titolare a

---

[11] Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (c.d. Regolamento privacy) e decreto legislativo 30 giugno 2003, n. 196 (c.d. Codice privacy). Inoltre, nella realizzazione delle attività si tiene conto anche delle indicazioni fornite dalle «*linee guida relative al regolamento generale sulla protezione dei dati messe a punto dal gruppo di lavoro "Articolo 29"*» e approvate dal Comitato europeo per la protezione dei dati.

[12] Ai sensi dell'articolo 4, par. 1, punto 7), del Regolamento *privacy*, per titolare del trattamento si intende «*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri*». Pertanto, in relazione alle attività di analisi del rischio fiscale, il titolare del trattamento è l'Agenzia delle entrate.

[13] Ai sensi dell'articolo 4, par. 1, punto 8), del Regolamento *privacy*, per responsabile del trattamento si intende «*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*». Per quanto concerne le attività di analisi del rischio svolte dall'Agenzia delle entrate, il responsabile del trattamento e la società SOGEI S.p.a.

svolgere una valutazione d'impatto (DPIA) prima di darvi inizio, consultando l'autorità di controllo (cioè il Garante per la protezione dei dati personali) nel caso in cui le misure tecniche e organizzative individuate per mitigare l'impatto del trattamento non siano ritenute sufficienti e, dunque, quando il rischio residuale (cioè il rischio che permane dopo l'applicazione delle misure di sicurezza) per i diritti e le libertà degli interessati resti elevato.

La valutazione d'impatto (DPIA) comporta l'applicazione di **specifiche misure di sicurezza e/o controlli ulteriori** rispetto a quelli già esistenti in relazione al trattamento, al fine di attenuare il livello di rischio ed assicurare la protezione dei diritti e delle libertà degli interessati.

Essa può essere effettuata per ogni attività di trattamento (sia nuova che già in essere) ma il Regolamento individua alcuni casi in cui è obbligatoria, e cioè in presenza di:

- una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basato su un trattamento automatizzato, compresa la profilazione, sulla quale si fondano decisioni che incidono significativamente sui diritti e libertà degli interessati;
- un trattamento su larga scala di particolari categorie di dati personali;
- una sorveglianza sistematica su larga scala di una zona accessibile al pubblico;
- un trattamento che integra almeno due dei nove criteri identificati dal Gruppo di lavoro articolo 29.

Il documento di DPIA non è necessario quando i trattamenti:

- hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è stata già condotta una valutazione di impatto;
- sono stati già sottoposti a verifica da parte dell'Autorità di controllo prima del maggio 2018 e le loro condizioni (es. oggetto, finalità, ecc.) non hanno subito modifiche;
- fanno riferimento a norme e regolamenti UE o di un singolo stato membro per la cui definizione è stata già condotta una DPIA.

Nonostante, come detto, la predisposizione del documento di DPIA non sia sempre obbligatoria, l'Agenzia delle entrate, per ogni tipologia di analisi del rischio svolta, **ha sempre redatto il documento in argomento**, così da massimizzare la tutela dei diritti degli interessati. Come si dirà meglio nel prosieguo, in taluni casi i documenti di DPIA sono stati inviati all'Autorità Garante per l'approvazione preventiva. Tale passaggio, tuttavia, non è derivato dalla valutazione del rischio residuo, bensì da previsione legislative *ad hoc* che disciplinano l'utilizzo di alcune banche dati.

5.3 Il trattamento di alcune particolari categorie di dati

Nel contesto del Regolamento *privacy* è possibile individuare **tre categorie di dati**:

- i **dati personali comuni**, che si riferiscono a caratteristiche generiche delle persone fisiche;
- i **dati particolari** – *ex* articolo 9 del Regolamento – che concernono aspetti quali lo stato di salute, gli orientamenti sessuali, le opinioni politiche *et similia*;
- i **dati giudiziari** – *ex* articolo 10 del Regolamento – cioè quelli relativi alle condanne penali e ai reati, ovvero alle connesse misure di sicurezza (personali o patrimoniali).

Tale distinzione non è meramente descrittiva, poiché le diverse categorie di dati soggiacciono a regole di trattamento differenziate.

In particolare, accanto ad un nucleo di regole uniformi (ad esempio, esistenza di una base giuridica che autorizzi l'utilizzo; necessità e proporzionalità dei trattamenti; correttezza, coerenza e completezza dei dati, ecc.), per i dati particolari e giudiziari sono previsti adempimenti specifici.

Ciò premesso, è necessario evidenziare che l'Agenzia delle entrate non gestisce *database* popolati con dati particolari e giudiziari. Tuttavia, alcune informazioni fiscalmente rilevanti possono essere indirettamente espressive di un dato particolare. Un esempio classico è quello relativo allo stato di salute, che potrebbe essere desunto attraverso l'ammontare delle spese mediche portate annualmente in detrazione.

Per massimizzare le tutele degli interessati, nello svolgimento delle attività di analisi del rischio, i dati suscettibili di essere utilizzati per inferire informazioni particolari non sono oggetto di trattamento individuale. Esemplificativamente, le detrazioni fiscali relative alle spese mediche non vengono separatamente visualizzate nei *dataset* di analisi ma solo – se l'informazione è rilevante – in forma aggregata con le altre spese fiscalmente detraibili sostenute dal contribuente.

5.4 L'intervento umano nell'attività di analisi del rischio

In tutti i processi di analisi del rischio svolti dall'Agenzia delle entrate **l'intervento umano è sempre garantito sia a monte, sia a valle del procedimento**.

I percorsi di analisi utilizzati sono, infatti, interamente sviluppati dal personale dell'Agenzia che, quindi, ha il pieno dominio sugli stessi. Inoltre, le elaborazioni prevedono sempre delle fasi di *test* intermedie volte a verificare che le operazioni eseguite corrispondano e quelle programmate. In ultimo – ma non certo per importanza – gli *output* delle attività di analisi del rischio non sono utilizzati per creare dei provvedimenti impositivi, bensì vengono trasmessi alle strutture di controllo

che, dopo un'ulteriore valutazione, decidono verso quali soggetti avviare un'attività istruttoria, che viene svolta nel pieno rispetto del principio del contraddittorio (recentemente potenziato dall'articolo 6-*bis* dello Statuto dei diritti del contribuente).

A ciò si può aggiungere che gli algoritmi utilizzati dall'Agenzia delle entrate sono sempre spiegabili, non discriminatori e – nei limiti previsti dalle disposizioni di riferimento – trasparenti.

Con il termine "**spiegabilità**" si rinvia alla possibilità di comprendere quali siano le variabili che hanno portato ad un determinato risultato. Tale caratteristica, oltre ad essere una *best practice* nel settore del trattamento dei dati, in ambito fiscale diviene una vera e propria necessità.

Infatti, come anticipato, le risultanze delle attività di analisi del rischio sono destinate ad alimentare le attività istruttorie delle strutture di controllo. Tenuto conto che l'ordinamento tributario si caratterizza per la previsione di stringenti obblighi motivazionali, una segnalazione basata su un algoritmo di cui non è chiaro il procedimento logico non sarebbe di alcuna utilità per i funzionari istruttori, poiché richiederebbe un riesame complessivo della posizione.

La **non discriminazione** consiste nello scongiurare il pericolo che le decisioni algoritmiche vengano prese in base a dati non pertinenti rispetto al contesto specifico. Esemplificativamente, si può pensare ad un algoritmo che, in base alle informazioni utilizzate in sede di addestramento, individui come fiscalmente rischiosi i contribuenti appartenenti ad una certa etnia.

In ambito fiscale, tale rischio è residuale poiché, come anticipato *supra*, le informazioni utilizzate non rientrano tra quelle "particolari".

Tuttavia, come ulteriore misura di sicurezza, l'Agenzia non utilizza in sede di addestramento algoritmico informazioni diverse da quelle fiscalmente rilevanti.

Ad esempio, non viene mai precisato lo Stato di nascita dei contribuenti (informazione che potrebbe approssimare la cittadinanza), in modo da scongiurare del tutto il rischio che tale variabile venga utilizzata in sede di sviluppo metodologico.

Per quanto riguarda, infine, la **trasparenza** "esterna", la stessa – nel contesto del RGPD – viene obbligatoriamente richiesta in relazione ai processi decisionali completamente automatizzati, che, come già detto, non sono utilizzati nell'ambito delle attività di analisi del rischio fiscale. In particolare, gli articoli 13, par. 2, lett. f) e 14, par. 2, lett. g) del RGPD, impongono al titolare del trattamento di rendere noto l'esistenza di un trattamento decisionale automatizzato, precisando che occorre specificare le «*informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato*».

Quando la pubblicazione della logica degli algoritmi è stata ritenuta necessaria dal Garante della *privacy*, l'Agenzia ha prontamente provveduto tramite il proprio sito istituzionale. Su tale specifico punto, si rinvia alle considerazioni relative alle attività di analisi del rischio basate sui dati dell'Archivio dei rapporti finanziari.

5.5 Le misure di segregazione organizzativa, con particolare riferimento alle piattaforme di analisi avanzata dei dati

Nell'ambito delle attività di analisi del rischio, vengono utilizzate diverse soluzioni *software* che si differenziano per il grado di flessibilità delle elaborazioni effettuabili.

In dettaglio, gli analisti hanno a loro disposizione:

- degli **applicativi c.d. "verticali"**, che permettono di analizzare dei fenomeni preimpostati in sede di progettazione; ad esempio, esistono applicativi dedicati alla fatturazione elettronica, oppure all'individuazione dei soggetti che hanno omesso la dichiarazione pur avendo percepito componenti di reddito imponibili; in questo caso, in ossequio ai principi di *privacy by design* e *by default*, i dati utilizzabili sono solo quelli riferiti allo specifico fenomeno che si intende investigare;
- delle **piattaforme di analisi avanzata dei dati**, che consentono di sviluppare dei progetti ispettivi usando "liberamente" i dati presenti in Anagrafe tributaria, ferme restando le limitazioni previste dall'Autorità Garante; in questo caso, sono state definite delle rigide *policy* di utilizzo e le progettualità devono: essere analiticamente descritte in un documento progettuale che evidenzia sia gli aspetti tecnico-tributari che quelli di gestione dei dati; essere preventivamente autorizzate dalle strutture centrali dell'Agenzia; essere testate da un'articolazione organizzativa diversa da quella che ha sviluppato l'iniziativa.

Inoltre, vengono utilizzate – esclusivamente a livello centrale e da una sola articolazione organizzativa – dei *software* che permettono l'implementazione di algoritmi predittivi. Il personale addetto a tali ultime attività è in possesso di una particolare qualificazione professionale in ambito ingegneristico, econometrico, statistico, fisico, così da assicurare sempre un elevato livello qualitativo delle elaborazioni.

5.6 Le prescrizioni specifiche del Garante della *privacy*: l'Archivio dei rapporti finanziari e i dati fattura integrati

5.6.1 L'Archivio dei rapporti finanziari

In via preliminare, si evidenzia che l'**Archivio dei rapporti finanziari** costituisce un'apposita sezione dell'Anagrafe tributaria ed è una base dati che contiene le informazioni relative:

- ai conti correnti e agli altri rapporti finanziari di cui un contribuente è titolare o può disporre sulla base di deleghe o procure ad operare (c.d. "**sezione anagrafica**");
- alle movimentazioni contabili in forma aggregata, al saldo iniziale, a quello finale e, per alcune tipologie di conto, al valore medio di giacenza, che interessano in un anno solare ciascun rapporto continuativo, nonché alle operazioni c.d. "*extra*-conto", vale a dire effettuate al di fuori di un rapporto continuativo con l'intermediario finanziario (c.d. "**sezione contabile**").

Detto archivio è stato istituito ad opera dell'articolo 7, sesto comma, del decreto del Presidente della Repubblica 29 settembre 1973, n. 605 (sezione anagrafica) e dell'articolo 11, comma 2, del decreto-legge 6 dicembre 2011, n. 201 (sezione contabile).

Il comma 4 del citato articolo 11 ha, inoltre, previsto la possibilità per l'Agenzia delle entrate di utilizzare le informazioni in esso presenti per le analisi del rischio di evasione.

Successivamente, il comma 682 dell'articolo 1 della legge 27 dicembre 2019, n. 160, ha disposto che l'Agenzia delle entrate, per le summenzionate analisi del rischio, possa avvalersi, anche previa pseudonimizzazione dei dati personali, delle tecnologie, delle elaborazioni e delle interconnessioni con le altre banche dati di cui dispone, allo scopo di individuare i criteri di rischio utili a far emergere le posizioni da sottoporre a controllo o nei cui confronti avviare attività di stimolo dell'adempimento spontaneo.

Inoltre, il comma 684 del citato articolo 1 ha statuito, nel rispetto del principio di responsabilizzazione di cui all'articolo 35 del regolamento (UE) 2016/679, che l'Agenzia delle entrate redigesse una valutazione unitaria di impatto sulla protezione dei dati (*Data Protection Impact Assessment* - DPIA) da sottoporre al parere preventivo del Garante per la protezione dei dati personali.

Con il provvedimento n. 276 del 30 luglio 2022 il Garante per la protezione dei dati personali ha espresso parere favorevole rispetto alla summenzionata valutazione di impatto *privacy,* uno stralcio della quale è consultabile sul sito dell'Agenzia delle entrate.

Il predetto parere contiene alcune prescrizioni che dovevano essere adempiute prima dell'avvio delle attività di analisi del rischio e, in particolare, l'effettuazione di alcune pubblicazioni sul sito istituzionale dell'Agenzia delle entrate.

Per salvaguardare le esigenze di riservatezza delle attività istituzionali dell'Agenzia delle entrate ed evitare l'adozione di condotte suscettibili di eludere i controlli, in aderenza alle linee guida del Comitato europeo di protezione dei dati, non sono stati forniti gli elementi di dettaglio concernenti i singoli percorsi di indagine né le informazioni sull'architettura informatica utilizzata.

Fatti tale premesse, si passa ad esaminare le **singole misure addizionali di garanzia previste per l'utilizzo dei dati dell'Archivio dei rapporti finanziari**.

5.6.2 Pseudonimizzazione

Nell'ambito delle attività di analisi del rischio basate sui dati dell'Archivio dei rapporti finanziari viene utilizzata, come misura di sicurezza aggiuntiva, la **pseudonimizzazione**, che – ai sensi dell'articolo 4, n. 5), del Regolamento *privacy* – rappresenta *«il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile*».

In particolare, tale misura di sicurezza viene attuata:

- sostituendo, con una chiave rotativa, i dati onomastici dei contribuenti con codici alfanumerici;
- perturbando, in maniera casuale, le variabili numeriche, così da ridurre la possibilità di una re-identificazione indiretta dei contribuenti.

La pseudonimizzazione è effettuata da un'apposita struttura organizzativa di Sogei, che è la sola a conoscere il metodo di associazione che consente di risalire a ritroso agli originari codici fiscali dei contribuenti.

Per garantire, anche nel tempo, che le informazioni presenti nei diversi *dataset* non siano attribuite ad una persona fisica identificata o identificabile, Sogei utilizza degli identificativi pseudonimi dotati di una validità temporale limitata.

L'Agenzia delle entrate, infine, non ha accesso ai metodi di associazione utilizzati in fase di pseudonimizzazione.

Solo a valle delle attività di analisi del rischio, dopo aver quindi individuato i contribuenti fiscalmente rischiosi, gli elenchi dei soggetti da controllare vengono riportati "in chiaro", di modo che possano essere valutate le attività istruttorie da intraprendere.

5.6.3 Segregazione organizzativa

Per limitare significativamente il numero di soggetti che possono utilizzare i dati dell'Archivio dei rapporti finanziari è previsto che solo un'unità organizzativa possa svolgere il trattamento.
Peraltro, solo pochi addetti in servizio presso detta unità sono effettivamente autorizzati ad usare i dati.

5.6.4 Dati dei contribuenti minori di età

Per quanto concerne il trattamento dei dati riferiti ai soggetti minori di età, esso si rende necessario poiché gli stessi – pur se attraverso l'attività svolta dai loro tutori legali e, per gli atti di straordinaria amministrazione, previa autorizzazione del giudice tutelare – possono essere titolari di redditi, nonché proprietari di beni fiscalmente rilevanti. In ogni caso, al fine di salvaguardare la loro posizione giuridica, l'attività istruttoria non viene mai svolta nei loro confronti e i dati identificativi di detta particolare categoria di contribuenti non è mai presente nelle liste di controllo, poiché in loro vece sono indicati i rispettivi tutori/rappresentanti legali.

5.6.5 I dati fattura integrati

In via preliminare, si rileva che la fattura elettronica è un documento informatico, in formato strutturato, trasmesso per via telematica al Sistema di Interscambio[14] e da questo recapitato al soggetto ricevente.
La fattura elettronica contiene obbligatoriamente le informazioni stabilite dall'articolo 21 del decreto del Presidente della Repubblica 26 ottobre 1972, n. 633, ovvero, nel caso di fattura semplificata, quelle stabilite dall'articolo 21-*bis* e, in particolare, quelle riferite alla base imponibile, all'aliquota, all'imposta, nonché alla natura, quantità e qualità dei beni e servizi oggetto di scambio.
Per "**dati fattura integrati**", invece, si intendono i dati, estrapolati dai *file* fattura, riferiti alla natura, qualità e quantità delle operazioni.

[14] Di cui al decreto del Ministro dell'economia e delle finanze 7 marzo 2008.

Ai fini delle attività di analisi del rischio, in esito al provvedimento del Garante della *privacy* n. 454 del 22 dicembre 2021, tali ultimi dati vengono trattati limitatamente alle fatture emesse per operazioni eseguite nei confronti di altri operatori economici e mai con riferimento alle fatture emesse da soggetti che operano nel settore legale.

Il trattamento, inoltre, viene effettuato da un'unica articolazione organizzativa, così da limitare la massimo l'accesso alle informazioni.

6. Implementazione del modello *privacy* in Agenzia

In coerenza con l'esigenza di digitalizzazione, l'Agenzia ha adottato, nell'ambito **SIF** (Sistema Integrato della Fiscalità) e con il supporto di Sogei, un'apposita piattaforma per gestire, con un approccio integrato, gli aspetti di *governance*, rischio e controllo dei processi di protezione dati richiesti ai fini di una corretta responsabilizzazione dell'ente. Tale piattaforma si articola in moduli funzionali, all'interno dei quali sono attivati specifici processi e *workflow* operativi a supporto delle strutture che presidiano, per competenza organizzativa, il funzionamento del Sistema di gestione per la protezione dei dati personali.

Attraverso la piattaforma dedicata affluiscono le procedure operative in tema di *privacy*, quali la tenuta e l'aggiornamento del Registro delle attività di trattamento, che avviene sistematicamente e continuativamente laddove si rilevino nuovi trattamenti da effettuare o modifiche dei trattamenti già registrati, nonché del Registro delle istanze degli interessati per il tracciamento di tutte le richieste pervenute, della relativa documentazione e del relativo esito in tema di diritto di accesso, diritto di rettifica, diritto alla cancellazione, diritto di limitazione di trattamento, diritto alla portabilità dei dati, diritto di opposizione e diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato.

Anche l'analisi del rischio dei trattamenti e la valutazione di impatto sulla protezione dei dati personali (DPIA) vengono effettuate tramite l'apposita piattaforma.

7. *Cybersecurity*

La complessità della gestione del patrimonio dell'Agenzia a livello di infrastruttura informatica, nonché la rilevanza dei dati trattati, impone la necessità di intraprendere tutte le azioni e gli investimenti necessari a progettare e attuare misure volte alla salvaguardia del sistema nel suo complesso.

La sicurezza informatica, attraverso l'individuazione delle aree di rischio e delle possibili minacce,

fornisce una risposta alla necessità di realizzare un sistema integrato di protezione dei dati attraverso l'applicazione di *standard* internazionali di sicurezza e l'adeguamento alle misure previste da AgID, traguardando i livelli di sicurezza più elevati.

La vastità e complessità delle risorse dell'Agenzia richiede l'adozione di sistemi centralizzati di gestione e controllo degli accessi ai sistemi informatici, di sistemi per il monitoraggio e rilevazione di attacchi informatici seguendo le norme di sicurezza riconosciute a livello internazionale. Per garantire un corretto utilizzo delle risorse dal punto di vista della sicurezza è stato realizzato un sistema di accesso unico e centralizzato alle applicazioni.

In tale ambito si analizzano e si individuano **politiche**, **regole, processi** e **strumenti** innovativi atti a garantire e rafforzare la sicurezza informatica nella sua accezione più ampia, dalla sicurezza dei sistemi alla tutela del patrimonio informativo, anche a sostegno della semplificazione dei processi, fondata sempre più spesso sull'adozione di nuovi strumenti informatici.

Una parte rilevante delle attività svolte dall'Agenzia ha riguardato la realizzazione di strumenti e procedure operative che, riferendosi agli *standard* internazionali in tema di sicurezza, hanno centralizzato il governo del sistema di controllo degli accessi e affidato ai responsabili delle varie strutture organizzative la gestione e il monitoraggio delle abilitazioni dei dipendenti.

La sicurezza informatica interviene nelle seguenti aree.

- ***Governance* della sicurezza.** L'Agenzia ha realizzato un articolato sistema di servizi di protezione, *policy*, processi e procedure di monitoraggio e di miglioramento continuo, allo scopo di minimizzare i rischi e rispondere alle minacce interne ed esterne; in particolare, l'Agenzia ha introdotto un nuovo **Sistema di Gestione della Sicurezza Informatica (SGSI),** costituito da un insieme di politiche e procedure operative, linee guida e istruzioni che stabiliscono i principi da seguire per prevenire i rischi informatici e proteggere le informazioni trattate; a titolo esemplificativo, il SGSI ha armonizzato i principi per la classificazione dei documenti, l'uso dei controlli crittografici, la continuità operativa, la gestione degli *asset* informatici, la gestione degli accessi logici, lo sviluppo e manutenzione dei sistemi informatici, la *cloud security*, la gestione degli eventi di sicurezza, il corretto utilizzo delle risorse informatiche.
- **Evoluzione e ampliamento del sistema di tracciamento degli accessi.** L'Agenzia ha ampliato il tracciamento degli accessi al sistema informativo dell'Anagrafe tributaria, incrementando il numero dei sistemi sottoposti al tracciamento strutturato e migliorando le funzioni di analisi e allarme, nonché di reportistica, per un controllo efficace sulle modalità di

interrogazione in AT effettuate dagli utenti interni ed esterni.

- ***Identity Access Management* (IAM)**. L'Agenzia ha realizzato un'infrastruttura specifica dedicata al controllo degli accessi mediante la centralizzazione in un unico portale degli accessi ai servizi applicativi ("Scrivania dei servizi"), alla gestione degli utenti e delle relative autorizzazioni, anche attraverso la realizzazione di nuove funzionalità, a garanzia di una sempre più efficace protezione delle risorse e dei dati aziendali. È stato anche introdotto il meccanismo di *Single Sign On* tra le applicazioni e la postazione di lavoro, centralizzando la verifica delle credenziali in un unico punto, con il molteplice obiettivo di semplificare il processo di autenticazione per l'operatore, di rendere uniformi le *password policy* e di semplificare l'evoluzione verso nuove modalità di autenticazione sempre più robuste.
- ***Endpoint security***. Nell'ambito del progetto del *digital workplace* è stato incrementato il livello di sicurezza delle postazioni portatili mediante l'adozione di strumenti evoluti di rilevamento delle minacce, la centralizzazione della configurazione e l'introduzione di un processo strutturato e centralizzato di monitoraggio delle vulnerabilità. Nell'ambito del progetto di adozione di servizi applicativi in *cloud* sono stati adottati specifici strumenti di crittografia a riposo dei documenti e di classificazione documentale in aderenza alle politiche definite nel Sistema di Gestione della Sicurezza Informatica. È anche attivo un processo automatico di monitoraggio delle variazioni di classificazione ed è in fase di valutazione l'attivazione del processo di rilevazione di anomalie, quali, ad esempio, l'invio all'esterno di documenti classificati come interni e l'adozione delle conseguenti azioni di contrasto e mitigazione.
- **Standardizzazione delle procedure di firma e cifratura.** Relativamente allo scambio di dati e documenti, sia all'interno dell'Amministrazione finanziaria sia con gli enti esterni ad essa, sono in costante aggiornamento i meccanismi che assicurano la riservatezza delle informazioni. In particolare, nel 2023 è stato completato il processo di standardizzazione degli algoritmi utilizzati per la cifratura dei dati, unitamente a quelli di *hashing*, allineando la *baseline* di sicurezza allo stato dell'arte degli algoritmi internazionalmente accettati come sicuri. Parimenti, per aumentare il livello di sicurezza, è stata incrementata la lunghezza delle chiavi utilizzate nei certificati di firma e cifratura, portandola anche oltre il livello ordinariamente riconosciuto come sicuro, allo scopo di poter garantire un idoneo *standard* di sicurezza anche rispetto all'evoluzione tecnologica futura.
- **Formazione e *security awareness*.** Per innalzare il livello di sicurezza e aumentare l'efficacia in termini di protezione dei dati, sono state progressivamente sviluppati le competenze

essenziali degli utenti, le tecniche e i metodi fondamentali per prevenire gli incidenti e reagire al meglio alle minacce; in particolare, oltre il 90 per cento del personale è stato formato e aggiornato, attraverso la partecipazione ad almeno un'edizione dei corsi di *security awareness,* proposti con frequenza annuale. Inoltre, gli addetti alla sicurezza informatica centrali e regionali sono formati in materia di *threat intelligence*, gli operatori con privilegi amministrativi in materia di gestione delle risorse informatiche e i programmatori interni all'Agenzia in materia di sviluppo sicuro. Infine, sono organizzate specifiche sessioni – che coinvolgono sia le strutture centrali e periferiche, sia Sogei – nelle quali viene simulata l'applicazione dei processi e delle procedure per la gestione degli incidenti (Simulazioni *Tabletop*).

- **Adeguamento allo *standard* AgID.** Le misure di sicurezza AgID prevedono tre livelli (alto, *standard* e minimo, quest'ultimo obbligatorio per le amministrazioni pubbliche). L'Agenzia ha puntato ad ottenere l'adeguamento al livello *standard* ma sta costantemente lavorando per raggiungere il livello alto per la gran parte delle misure previste da AgID. Allo stato attuale, in relazione all'applicabilità delle misure di sicurezza AgID al contesto dell'Agenzia, sono state realizzate **24** misure di livello *standard* e **9** di livello alto.
- **Evoluzione delle applicazioni ad uso nell'ambito della sicurezza informatica** (*Vitruvio*, *Monade*, *Mistral*).
- **Coordinamento delle attività di sicurezza informatica tra Agenzia e Sogei** tramite uno specifico tavolo congiunto, chiamato "Tavolo permanente per la sicurezza – TPS".
- **Ottimizzazione delle procedure di interazione con organismi di sicurezza.** L'Agenzia ha ottimizzato il colloquio con il CERT Sogei e tra il CERT-Mef e il Nucleo Accreditato IT (NaIT - Agenzia), attivando uno specifico prodotto dedicato all'interscambio di informazioni di sicurezza denominato "*The Hive*" (sistema di gestione degli incidenti di sicurezza, che consente alle organizzazioni di rispondere in modo efficace a minacce informatiche). In questo modo il processo di interscambio di informazioni, tra cui quelle relative agli incidenti, è stato strutturato ed è pertanto più efficientemente monitorato.
- **Estensione della cifratura dei dispositivi portatili, adozione di soluzioni di autenticazione forte e separazione tra ambienti elaborativi.** Su tutti i portatili assegnati ai dipendenti sono attivi meccanismi di cifratura dei dati a riposo, mentre l'accesso alle risorse *cloud* e all'infrastruttura di lavoro agile avviene tramite autenticazione multi-fattore. L'Agenzia sta, inoltre, completando l'assegnazione a tutti i dipendenti di una macchina virtuale *standard* e sicura, che consente la completa separazione tra l'ambiente applicativo e quello di lavoro,

aggiungendo un ulteriore livello di sicurezza.

Alle misure elencate, si aggiungono tutte le attività di sicurezza che Sogei, in virtù degli accordi contrattuali, svolge sui sistemi e sui servizi erogati per conto dell'Agenzia ai cittadini. L'Agenzia effettua con regolarità, in collaborazione con il *partner* tecnologico, l'attività di vigilanza in materia di sicurezza informatica, con l'obiettivo di monitorare, migliorare ed incrementare i presidi di sicurezza informatica dell'Anagrafe tributaria.

Grazie per l'attenzione