CAMERA AVVOCATI TRIBUTARISTI LIGURIA

L'INTELLIGENZA ARTIFICIALE NELL'ACCERTAMENTO

Il tortuoso sentiero fra le sirene dell'AI ACT, le cautele del DDL 1146 e le trincee alsaziane.

Abstract.

Il D. Lgs. 13/2024, in attuazione dell'art. 17 della Legge 111/2023, prevede espressamente l'impiego di sistemi di intelligenza artificiale al servizio dell'attività di analisi del rischio fiscale dei contribuenti, anche nella prospettiva dell'accertamento.

La definizione legislativa italiana manifesta una criticità rilevante nella misura in cui pretende di applicare lo strumento dell'intelligenza artificiale non solo ai dati contenuti nell'Anagrafe Tributaria e nelle altra banche dati pubbliche (ad eccezione di quelle di polizia), ma anche ai dati *pubblicamente disponibili*, che in quanto tali, non forniscono alcuna garanzia di certezza, genuinità e rilevanza concreta, ai fini dell'accertamento della capacità contributiva.

Tutto ciò avviene in un contesto normativo europeo che, anziché fornire garanzie nell'impiego dello strumento, sembra sottovalutarne i rischi, proprio mentre, a livello nazionale, si cerca di disciplinare in modo più cauto e garantista l'impiego dell'intelligenza artificiale nell'ambito della pubblica amministrazione.

Sullo sfondo di questo quadro, incombe poi la necessità di ridisegnare le fondamenta stesse degli strumenti più invasivi del procedimento istruttorio tributario (accessi, ispezioni e verifiche) all'indomani della sentenza Italgomme Pneumatici Srl e altri contro Italia, la quale, nel richiedere una più precisa delimitazione dei poteri dell'Amministrazione, ed imponendo una effettiva motivazione, lascia comunque aperta la porta al concetto di "*analisi del rischio*" quale strumento lecito che, in un contesto di trasparenza, potrebbe essere impiegato proprio per giustificare in concreto la necessità di adottare le misure più invasive quali accessi, ispezioni e verifiche.

INDICE

PREMESSA

La Legge 9 agosto 2023 n. 111 (c.d. "delega fiscale") ha investito il Governo del compito di disciplinare l'utilizzo dell'intelligenza artificiale (AI) nell'ambito dei procedimenti tributari di accertamento.

In particolare, l'art. 17 della legge delega prevede di potenziare l'impiego di sistemi di IA, sia per favorire la compliance fiscale ("*prevenire gli errori dei contribuenti*" e stimolare l'adempimento spontaneo), sia per concentrare i controlli sui soggetti a più alto rischio fiscale, così da massimizzare l'efficacia dell'azione anti-evasione.

In attuazione di tali principi, il D.Lgs. 29 gennaio 2024 n. 13 ha introdotto rilevanti innovazioni in materia di accertamento tributario, in particolare con l'art. 2 "*Razionalizzazione e riordino delle disposizioni normative in materia di attività di analisi del rischio".*

La disposizione in esame dichiara una triplice funzione:

- definire una serie di concetti "*con riferimento a tutte le disposizioni di legge che richiamano l'analisi del rischio in materia tributaria"*
- consentire l'utilizzo di pressoché tutte le banche dati, anche mediante interconnessione fra loro, a fini di analisi del rischio, del controllo, dell'erogazione di servizi ecc., coinvolgendo attivamente anche la Guardia di Finanza
- introdurre nella normativa vigente in materia di accertamento (art. 31 e 32 DPR 600/73; art. art. 51 DPR 633/72) le disposizioni sull' "*analisi del rischio*" come definita dalla stessa disposizione.

Ai fini che qui ci occupano, il tema centrale è proprio quello del concetto di "***analisi del rischio***" e delle modalità con cui viene attuata.

L'ANALISI DEL RISCHIO

Nella definizione legislativa "**analisi del rischio**" è - parafrasando il testo - un "***processo"*** che ***"tramite modelli e tecniche di analisi deterministica ovvero probabilistica", "utilizza, anche attraverso la loro interconnessione, le informazioni presenti nelle basi dati dell'Amministrazione finanziaria, ovvero pubblicamente disponibili"***.

Tale processo mira ad 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"* ed ha la finalità 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".*

L'intelligenza artificiale entra direttamente in questo contesto, in quanto l'"***analisi probabilistica"***, a cui fa riferimento la definizione di "analisi del rischio" è - sempre per definizione normativa - l' "***insieme dei modelli e delle tecniche di analisi che, sfruttando soluzioni di intelligenza artificiale ovvero di statistica inferenziale,*** *consentono di isolare rischi fiscali, anche non noti a priori, che, una volta individuati, possono essere utilizzati per l'elaborazione di autonomi criteri selettivi, ovvero permettono di attribuire una determinata probabilità di accadimento a un rischio fiscale noto".*

Chiarito che all'Agenzia delle Entrate viene richiesto (o "imposto") di attuare questo "processo" di utilizzo concreto di tutte la banche dati di cui ha la disponibilità, **l'articolo 2 fissa anche gli scopi di tale impiego**, stabilendo che:

A. **I risultati dell'analisi del rischio**, oltre che per le finalità di **prevenzione e contrasto** all'evasione fiscale, alla frode fiscale e all'abuso del diritto in materia tributaria, nonché di stimolo dell'adempimento spontaneo, **possono essere utilizzati anche per lo svolgimento di controlli preventivi.**

B. Le informazioni presenti in tutte le basi dati di cui l'Agenzia delle entrate dispone, ivi comprese quelle presenti nell'apposita sezione dell'**Anagrafe tributaria**, nonché quelle memorizzate nel sistema di interscambio (**fatture elettroniche**), con la sola esclusione delle banche dati utilizzate per finalità di polizia o di prevenzione, indagine e perseguimento di reati, **possono essere utilizzate dall'Agenzia delle Entrate** (e in forza del comma 7 anche dalla G.d.F), anche tramite **interconnessione tra loro e con quelle di archivi e registri pubblici**:

- per le attività di **analisi del rischio fiscale**
- per le attività di **controllo**
- per le attività di stimolo dell'**adempimento spontaneo**
- per quelle di **erogazione di servizi** ai contribuenti.

Tali attività, prosegue la narrativa dell'art. 2, potranno essere svolte anche mediante condivisione di strutture informatiche fra AdE e GdF, mediante "*unità integrate di analisi del rischio*" e dovranno comunque inserirsi nel quadro delle disposizioni del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196, nonché dell'articolo 23, paragrafo 1 del GDPR, considerati i principi di necessità e di proporzionalità.

Allo scopo si prevede che uno specifico regolamento del MEF e sentito il Garante per la protezione dei dati personali dovrà disciplinare:

a) le specifiche limitazioni e le modalità di esercizio dei diritti del titolare dei dati trattati in modo da assicurare che tale esercizio non possa arrecare un pregiudizio effettivo e concreto all'obiettivo di interesse pubblico;
b) le disposizioni specifiche relative al contenuto minimo essenziale di cui all' articolo 23, paragrafo 2, del GDPR ;
c) misure adeguate a tutela dei diritti e delle libertà degli interessati.

IL PROBLEMA DELLE FONTI APERTE

La lettura della disposizione attuativa ci fornisce una prima notizia non esattamente edificante.

Allo stato, lo strumento dell'intelligenza artificiale può essere utilizzato non **solo** per interconnettere dati presenti nelle banche dati dell'Agenzia delle Entrate e nelle banche dati pubbliche, ma può essere impiegata ad ampio spettro acquisendo **anche informazioni *pubblicamente disponibili.***

La domanda che si pone è: *"pubblicamente disponibili*" dove?
E la risposta - ahimè - è abbastanza scontata…

E' evidente infatti che il legislatore, con l'impiego di questa formulazione, volutamente generica, intenda riferirsi alle informazioni reperibili online (ad es. siti web, social media) e non solo alle banche dati istituzionali.

Questa apertura rappresenta un cambio di passo rispetto al passato recente, ove simili tentativi avevano incontrato riserve da parte delle autorità garanti.

Ed in effetti, lo stesso Garante per la protezione dei dati personali, nel **Parere del 11 gennaio 2024**, reso sullo schema di decreto legislativo in esame, **aveva raccomandato di escludere dal novero delle informazioni utilizzabili proprio quelle "pubblicamente disponibili"**, ritenendole **prive dei necessari requisiti di affidabilità e raccolte per finalità originarie incompatibili con il nuovo trattamento**[1].

Nonostante ciò, nel testo definitivo del decreto l'uso di tali dati aperti è stato mantenuto, sebbene subordinato al rispetto della normativa privacy, prevedendo inoltre che un futuro decreto attuativo del MEF, da emanarsi sentito il Garante Privacy, stabilisca "*misure adeguate a tutela dei diritti e delle libertà degli interessati*" in modo da assicurare che l'utilizzo degli algoritmi anti-evasione avvenga nel rispetto dei principi di necessità e proporzionalità.

---

[1] Scrive in Garante: "*In tale prospettiva, sotto il primo profilo, all'articolo 2, comma 3, andrebbero espunte le informazioni "pubblicamente disponibili" dal novero di quelle suscettibili di utilizzo, da parte dell'Agenzia delle entrate, mediante interconnessione con altre, in quanto prive dei necessari requisiti di affidabilità e raccolte per finalità diverse da quelle sottese al trattamento considerato.*"

Invero i rischi dell'accesso alle fonti aperte riguardano essenzialmente tre aspetti: il "nutrimento" dell'algoritmo, la cd. "discriminazione algoritmica" e la tutela dei dati personali.

A. Il nutrimento dell'algoritmo

Sino a che l'impiego dell'intelligenza artificiale (che come opportunamente ci ricorda il legislatore delegato è un agente ad "intelligenza zero", in grado solo di effettuare calcoli statistici inferenziali) viene limitato all'interconnessione di dati qualificati e verificati, contenuti in banche dati di cui si conoscono le finalità, le modalità di raccolta e trattamento, e la certa riferibilità al soggetto interessato, vi è la ragionevole certezza che il risultato dell'elaborazione sia sufficientemente attendibile - al netto di allucinazioni dell'algoritmo - perché le fonti di approvvigionamento dei dati sono esse stesse "attendibili".

Quando però si esce da questa area di controllo e si pesca (letteralmente) nella rete o in altre fonti aperte quali notizie di stampa o social media ecc. si entra inevitabilmente in un terreno minato, in cui la qualità del dato non è in alcun modo garantita, né sotto il profilo della certezza dell'evento che descrive, né sotto il profilo della concreta rilevanza ai fini dell'analisi del rischio.

Sia ben chiaro, l'utilizzo delle fonti aperte per le attività di intelligence non è affatto una novità, né un portato dell'intelligenza artificiale.

La cosiddetta Open Source Intelligence, (OSINT), ossia quella branca che si occupa della ricerca, raccolta e analisi di dati e notizie tratte da fonti aperte (giornali, riviste, televisione, radio, siti web e social network), da fonti pubbliche ufficiali (rapporti dei governi, piani finanziari, dati demografici, dibattiti legislativi, conferenze stampa, discorsi), da fonti professionali o scientifiche (conferenze, lezioni universitarie, pubblicazioni scientifiche) o ancora da osservazioni dirette (fotografie amatoriali, ascolto di conversazioni radio e osservazione di fotografie satellitari ecc.) è un'attività introdotta durante la seconda guerra mondiale dalle agenzie di sicurezza

di molte nazioni che, nel corso del tempo, è diventata prassi operativa ordinaria, anche per il contrasto e per la repressione dei reati.

Tuttavia, altro è impiegare a livello investigativo tali fonti per individuare rapporti fra soggetti, frequentazioni, per geolocalizzare in un certo momento un soggetto di interesse ecc. altro è pretendere di impiegare quelle stesse fonti per determinarne - in definitiva - la capacità contributiva…

Al netto del fatto che le informazioni raccolte sul web possono essere incomplete, non verificate o addirittura false, un conto è esaminare una foto e dedurre che fra due soggetti ritratti vi sono rapporti personali di un qualche tipo, o che un soggetto in una certa data si trovava in un luogo specifico, altro è impiegare quei dati estrapolandoli dal contesto, per dedurne fatti fiscalmente rilevanti.

Sotto tale profilo, il Garante della Privacy aveva già avuto modo di osservare nella propria Relazione 2023 che "*basare le procedure di accertamento su dati "rastrellati dal web – spesso in larga misura inesatti – è estremamente rischioso, potendo produrre* ***ricostruzioni distorte della reale capacità contributiva dei contribuenti****. Le garanzie di protezione dei dati rappresentano quindi anche in questo ambito, presupposti di efficacia dell'azione di contrasto dell'evasione fiscale*".

Invero, in un epoca delle "apparenze" amplificate dall'utilizzo dei social network, il cd. "***web scraping***", ossia l'estrazione di dati dalle fonti presenti su web, rischia di fornire all'analisi dell'intelligenza artificiale una base di elementi non rilevanti se non addirittura fuorvianti ai fini della determinazione del rischio fiscale o della capacità contributiva di un soggetto.

Il fatto di pubblicare regolarmente proprie foto accanto ad auto sportive, o manifestare interesse o competenza per il mercato degli orologi di lusso non significa in alcun modo che un soggetto ne abbia effettiva disponibilità, o che possegga realmente orologi di lusso, né tantomeno offre seri elementi per ritenere che presenti - sulla base di tali elementi - un elevato rischio fiscale.

Anche laddove gli elementi acquisiti avessero un maggior grado di rilevanza (es. se una serie di immagini potessero davvero confermare nel tempo la disponibilità di determinati beni di lusso, la frequentazione di determinati locali esclusivi o di mete turistiche VIP ecc.) quel semplice dato non sarebbe ancora sufficiente per motivare in concreto un rischio attuale ed effettivo, perché:

- nulla potrebbero dire circa il titolo da cui deriva quella disponibilità (acquisto, noleggio, comodato, eredità di un congiunto…),
- nulla potrebbero dire circa il fatto che nel tal locale sia entrato a sue spese o invitato da terzi,
- nulla potrebbero dire sul fatto che nella tal località abbia davvero soggiornato o solo fatto un giro turistico e qualche foto;
- nulla infine potrebbero dire sui "tempi" della disponibilità reddituale (se oggi sono in vacanza su uno Yacht a Porto Cervo, questa informazione non ha necessariamente rilievo ai fini di stabilire la mia capacità contributiva di quattro anni fa).

E ciò a tacere dei casi, ben possibili, di omonimia che - in mancanza di riferimenti certi (date e luoghi di nascita, codice fiscale ecc.) - potrebbero viziare alla radice l'impiego dello strumento.

In questo senso l'accesso indiscriminato ed incontrollato alle fonti aperte espone ad un rischio di falsi positivi di evasione, che non è ovviabile, se non con un attento e laborioso processo di verifica e pulizia dei dati, per assicurare che solo informazioni esatte, pertinenti e rilevanti rispetto alle finalità stabilite (accertamento della capacità contributiva) alimentino gli algoritmi fiscali.

➡ Sotto tale aspetto, la preoccupazione del Garante appare più che mai fondata e condivisibile e **sarebbe auspicabile che l'UNCAT facesse sentire la propria voce al fine di ottenere l'espunzione della locuzione "*ovvero pubblicamente disponibili*" dal testo normativo**.

B. La discriminazione algoritmica

Un secondo profilo critico riguarda la possibile "***discriminazione algoritmica***" e la mancanza di trasparenza del modello.

I modelli di AI, specialmente quelli di machine learning, apprendono da grandi quantità di dati storici e potrebbero ereditare *bias* o pregiudizi presenti nei dati stessi.

Anzi, è lecito sospettare che taluni *bias* siano proprio strutturalmente previsti dal sistema, come già avviene nel sistema VE.RA. che, secondo quanto indicato "*Informativa sulla logica sottostante i modelli di analisi del rischio basati sui dati dell'Archivio dei rapporti finanziari*" del 19 maggio 2023, considera espressamente quali ipotesi aggravamento del fattore di rischio il fatto che in passato il contribuente abbia definito controlli e/o accertamenti, si sia avvalso di sanatorie/regolarizzazioni messe a disposizione dal legislatore fiscale, o anche semplicemente che sia stato destinatario di un PVC, abbia in corso contenziosi o sia stato coinvolto in schemi fraudolenti.

La previsione di specifici indici di rischio insiti in comportamenti pregressi, uniti alla capacità del sistema di machine learning di "imparare" dai dati, creare relazioni fra gli stessi, generare inferenze e rilevare frequenze statistiche, oggettivamente preoccupa non poco: la capacità di auto apprendimento della macchine, in ambito fiscale ciò potrebbe tradursi, ad esempio, in un algoritmo che segnala preferenzialmente contribuenti di determinate aree geografiche o categorie socio-professionali semplicemente perché sovra-rappresentati nei dataset di evasori noti, finendo per creare disparità di trattamento non giustificate.

Un uso acritico dell'IA potrebbe dunque minare il principio di uguaglianza e imparzialità dell'azione amministrativa.

Ma come si fa ad evitare questo uso "acritico" dell'algoritmo? Innanzitutto occorrerebbe conoscere come funziona.

E’, anche questo, un tema noto e ricorrente quando si parla di intelligenza artificiale: la “trasparenza” sui criteri algoritmici è fondamentale per prevenire discriminazioni occulte.

In Italia, peraltro, la questione è stata notoriamente (e meritoriamente) affrontata dalla giurisprudenza amministrativa che ha ravvisato nella “conoscibilità dell’algoritmo”, la condizione di legittimità per ogni decisione automatizzata della P.A., al fine di evitare di consentire al fine di consentire ai destinatari (ma ancor prima agli utilizzatori) di verificare che non vi siano esiti arbitrari o discriminatori.

Qui sorge un’altro aspetto critico della normativa italiana: dell’algoritmo che governerà le analisi probabilistiche, ad oggi non si sa praticamente NULLA…

Il decreto in esame non prevede la pubblicazione dell’“algoritmo” che gestirà le analisi probabilistiche nell’ambito della “analisi di rischio”, il che significa che i contribuenti difficilmente potranno conoscere *ex ante* le logiche selettive e decisionali applicate.

Questo è un tema che pone evidenti problemi anche in ottica di difesa e di motivazione della scelta: un contribuente selezionato dall’AI per un accertamento potrebbe non essere in grado di comprendere perché è finito sotto la lente del Fisco, né quali elementi contestare per discolparsi.

Il rischio, in sostanza, è quello di un “presunto evasore” designato da una cd. “black box”[2] automatica, privo degli strumenti informativi per confutare gli indizi a suo carico.

Il che denuncerebbe peraltro anche l’incoerenza di un sistema che - dichiaratamente - vuole imporsi quale fattore di incentivo alla compliance…

[2] Il termine designa, per l’appunto sistemi di intelligenza artificiale in cui i processi interni rimangono nascosti agli utenti, rendendo estremamente difficile se non impossibile comprendere come vengono prese le decisioni.

L'unico presidio di garanzia (a condizione che non diventi un simulacro di pigra sottomissione alla decisione automatizzata) potrebbe essere dato dalla previsione che gli esiti dell'analisi di rischio automatizzata siano reinterpretati criticamente da funzionari, prima di dar luogo ad atti impositivi, garantendo il contraddittorio e la motivazione dell'atto in termini comprensibili.

Ma anche tale auspicio rischia di risultare vano, posto che se l'algoritmo non fosse trasparente per il contribuente, non si comprende come potrebbe esserlo per il funzionario che lo impiega… salvo obbligare i dipendenti dell'amministrazione finanziaria al segreto!

C. Il problema della tutela dei dati personali

La terza criticità dell'estensione alle fonti aperte attiene alla privacy e alla tutela dei dati personali, sollevando seri interrogativi di compatibilità con il GDPR e con il regime di protezione nazionale.

Il trattamento di informazioni personali per finalità fiscali ***diverse da quelle originarie*** costituisce infatti una forma di profilazione massiva, potenzialmente incidente sui diritti e le libertà degli interessati.

Il GDPR (Reg. UE 2016/679) consente sì, all'art. 6, par.1, lett. e), il trattamento di dati per l'esecuzione di un compito di interesse pubblico, quale è la lotta all'evasione, ma impone che ciò avvenga nel rispetto dei principi di "***liceità, correttezza, necessità e proporzionalità***" (artt. 5 e 23 GDPR).

Nel caso in esame, il legislatore, come detto, ha in previsione di disciplinare questo aspetto in un apposito decreto ministeriale che, tuttavia, sin dalla lettura della disposizione normativa, non lascia spazio a troppo ottimismo…

Il testo del quarto comma dell'art. 2 citato è il seguente:
"4. *Limitatamente alle attività di analisi del rischio condotte dall'Agenzia delle entrate, d'intesa con il Dipartimento delle finanze del Ministero dell'economia e delle finanze,*

nel rispetto delle disposizioni di cui agli articoli 2-undecies, comma 3, del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196, nonché dell'articolo 23, paragrafo 1, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, ***considerati i principi di necessità e di proporzionalità, con regolamento del Ministro dell'economia e delle finanze****,* ***sentito*** ***il Garante*** *per la protezione dei dati personali,* ***sono definite****:*
a) le specifiche ***limitazioni e le modalità di esercizio dei diritti*** *di cui agli articoli 15, 17, 18, 21 e 22 del predetto regolamento (UE) 2016/679, del Parlamento europeo e del Consiglio, del 27 aprile 2016, in modo da assicurare che tale esercizio non possa arrecare un pregiudizio effettivo e concreto all'obiettivo di interesse pubblico;*
b) le ***disposizioni specifiche relative al contenuto minimo essenziale di cui all'articolo 23****,* ***paragrafo 2****, del predetto regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016;*
c) le ***misure adeguate a tutela dei diritti e delle libertà degli interessati****.*

Se ragioniamo sul testo, appare evidente che la preoccupazione del legislatore è quella di dotare il MEF e l'agenzia delle entrate di uno **strumento non concertato con il Garante** ("sentire", non è evidentemente decidere assieme, o concordare) **diretto in primo luogo a limitare i diritti dei soggetti interessati** al trattamento -

ossia i contribuenti - e definire il “contenuto minimo” dell’art. 23[3] paragrafo 2 GDPR, vale a dire definire minimamente la portata delle limitazioni, le categorie di dati interessate dal trattamento, le garanzie contro abusi e trasferimenti illeciti dei dati, i periodi di conservazione e le altre garanzie per gli interessati tenuto conto della natura dei dati, delle categorie di trattamento e delle relative finalità.

---

[3] ***Articolo 23 GDPR*** **- Limitazioni (C73)**

1. Il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento ***può limitare, mediante misure legislative****,* ***la portata degli obblighi e dei diritti*** *di cui agli articoli da 12 a 22 e 34, nonché all'articolo 5, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22,* ***qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare****:*

a) la sicurezza nazionale;

b) la difesa;

c) la sicurezza pubblica;

d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;

e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale*;*

f) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari;

g) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate;

h) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere da a), a e) e g);

i) la tutela dell'interessato o dei diritti e delle libertà altrui;

j) l'esecuzione delle azioni civili.

2. *In particolare qualsiasi* ***misura legislativa di cui al paragrafo 1 contiene disposizioni specifiche riguardanti almeno, se del caso:***

a) le finalità del trattamento o le categorie di trattamento;

b) le categorie di dati personali;

c) ***la portata delle limitazioni introdotte****;*

d) ***le garanzie per prevenire abusi o l'accesso o il trasferimento illeciti****;*

e) l'indicazione precisa del titolare del trattamento o delle categorie di titolari;

f) i ***periodi di conservazione e le garanzie applicabili tenuto conto della natura, dell'ambito di applicazione e delle finalità del trattamento o delle categorie di trattamento****;*

g) i rischi per i diritti e le libertà degli interessati; e

h) il diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità della stessa.

E’ pur vero che alla lettera c) si prevede altresì di stabilire “***misure adeguate a tutela dei diritti e delle libertà degli interessati***”, ma resta il fatto che - quantomeno dal punto di vista linguistico - tali misure sembrano l’ultima delle preoccupazioni del legislatore, riconosciute peraltro non in forma assoluta, ma “*considerati i principi di necessità e di proporzionalità*” del trattamento.

Due considerazioni si pongono in relazione a tale punto.

La prima: è conforme al diritto dell’Unione - che parla espressamente “***misure legislative***” - una disposizione che delega ad Decreto Ministeriale la determinazione delle disposizioni limitative ai diritti contemplate nell’art. 23 GDPR?

La seconda: può considerarsi sempre e comunque “***proporzionata***” l’acquisizione indiscriminata di informazioni sui social media, molte delle quali eccedenti eccedenti

gli scopi tributari? **O tale trattamento viola il principio di "minimizzazione" dei dati e il principio di "esattezza"**?[4]

Su tali aspetti, come visto, il Garante Privacy ha già ha espresso timori proprio avvertendo che l'acquisizione indiscriminata di dati eterogenei e non filtrati rischia di produrre effetti distorsivi.

Ma le criticità della disposizione in esame in relazione al GDPR non sono ancora terminate.

---

[4] ***Articolo 5 GDPR - Principi applicabili al trattamento di dati personali***

1. I dati personali sono: (C39)

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

c) ***adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);***

d) ***esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»)****;*

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).

Un ulteriore aspetto, che non si comprende bene come il legislatore intenda affrontare, è il diritto a non essere sottoposto a decisioni automatizzate sancito dall' **art. 22 GDPR**[5].

In forza di tale disposizione individuo avrebbe diritto a che decisioni che producono effetti giuridici significativi su di lui non siano basate unicamente su un trattamento automatizzato (profilazione inclusa), salvo specifiche eccezioni previste dalla legge e con adeguate garanzie (ad es. intervento umano, possibilità di contestare la decisione).

Il punto è che la garanzia dell'intervento umano e la possibilità di contestare la decisione è prevista solo per i casi delle lettere a) (trattamento necessario per la conclusione di un contratto tra l'interessato e il titolare del trattamento) e c) (trattamento che avvenga su consenso esplicito) mentre nel caso sub b), ossia nell'ipotesi in cui il processo decisionale automatizzato sia autorizzato dal diritto dell'Unione **o dello Stato membro non vi è un contenuto minimo di "diritti" riconosciuto all'interessato** e il trattamento automatizzato può comunque avvenire sulla base di "***misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato***", che tuttavia non necessariamente devono prevedere

---

[5] ***Articolo 22 Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione*** *(C71, C72)*

1. L'interessato ***ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona****.*

2. Il paragrafo 1 ***non si applica*** *nel caso in cui la decisione:*

a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;

b) ***sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato****;*

c) si basi sul consenso esplicito dell'interessato.

3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

l'intervento umano o il diritto ad essere sentito, ovvero ancora il diritto di contestare la decisione…

Ebbene, tale è il caso che ci occupa, posto che **l'art. 2 comma 4** demandando alla normativa regolamentare la disciplina delle limitazioni ai diritti degli interessati **cita espressamente oltre agli articoli 15, 17, 18, 21 anche l'art. 22 del Regolamento UE.**

In altri termini la normativa delegata **di per sé potrebbe consentire che il trattamento avvenga in deroga al diritto di opposizione e persino al divieto di decisioni interamente automatizzate ex art. 22 GDPR**, e il fatto che la disciplina di tali aspetti sia demandata ad un decreto ministeriale dai confini quantomai incerti lascia alquanto perplessi sulla reale tutela dei diritti dei contribuenti…

Si potrebbe materializzare pertanto, a seguito del D. Lgs. 13/2024 e nel momento in cui entrerà in vigore il Decreto Ministeriale di cui al comma 4, quello spettro delle decisioni automatizzate, generate interamente da un algoritmo, che vanno ad incidere sui diritti di un soggetto senza che questi abbia potuto esercitare sui propri dati i diritti di accesso, rettifica o opposizione prima che il trattamento produca effetti, in aperto contrasto anche con la giurisprudenza del Consiglio di Stato che, sino ad oggi, anche sulla scorta dell'art. 22 GDPR, ne aveva eslcuso la legittimità.

➡ Sotto tale profilo si ritiene opportuno che UNCAT, nell'ambito delle sue funzioni istituzionali:

- ✓ preliminarmente solleciti una **modifica del comma 4 con la previsione di un intervento legislativo e non meramente regolamentare delle limitazioni previste dall'art. 23 GDPR**
- ✓ monitori in sede ministeriale l'iter approvativo del Decreto, caldeggiando l'adozione di un sistema di tutele che:
  - **A. preveda sempre e comunque il controllo umano sull'esito dell'elaborazione algoritmica;**

B. **preveda la possibilità di conoscere la base di dati impiegata in sede di elaborazione, l'origine degli stessi e le modalità di reperimento;**
C. **preveda l'obbligo di un contraddittorio sulla decisione algoritmica con l'interessato e la possibilità di un accesso immediato al giudice, anche in via d'urgenza, per poter contestare l'esisto dell'analisi del rischio, prima che l'attività istruttoria finalizzata all'accertamento (accessi, ispezioni, verifiche ecc.) sia conclusa;**
D. **preveda comunque, anche in sede di ricorso, la possibilità di contestare l'esattezza dei dati acquisiti ai fini della selezione del contribuente, con la previsione di inutilizzabilità dei dati acquisiti nell'accertamento, laddove il processo preliminare di selezione sia stato condizionato o falsato da una non corretta analisi del rischio.**

L'ACCERTAMENTO NELL'ECOSISTEMA DEL "AI ACT"

L'Unione Europea ha preteso di assumere, a livello mondiale, il ruolo di leader della regolazione dell'Intelligenza Artificiale, producendo un testo che all'esito di mesi di elaborazione e di contrasti protratti sino alla vigilia dell'approvazione, è divenuto un punto di riferimento a cui tutti gli stati europei debbono guardare: il Regolamento (UE) 2024/1689 del Parlamento e del Consiglio del 13 giugno 2024, meglio noto come "AI ACT".

Si tratta di un testo certamente pregevole e all'avanguardia, che, tuttavia, sotto l'angolo visuale che oggi trattiamo, lascia abbastanza perplessi.

La sensazione è ahimè che i diritti dei contribuenti, nella lettura europea, siano diritti di serie "C"… e che le tutele che giustamente si impongono quando l'intelligenza artificiale impatta sui diritti fondamentali, sulla giustizia, sulla vita privata delle

persone, sulla loro proprietà, siano molto più diluite, per non dire evanescenti, quando si tratta il tema fiscale.

Il tema è chiaro sin dalle premesse, ed è espresso senza mezzi termini nel Considerando n. 59.

"*Tenuto conto del loro ruolo e della loro responsabilità, le azioni delle autorità di contrasto che prevedono determinati usi dei sistemi di IA sono caratterizzate da un livello significativo di squilibrio di potere e possono portare alla sorveglianza, all'arresto o alla privazione della libertà di una persona fisica, come pure avere altri impatti negativi sui diritti fondamentali garantiti nella Carta. In particolare,* ***il sistema di IA, se non è addestrato con dati di elevata qualità, se non soddisfa requisiti adeguati in termini di prestazione, accuratezza o robustezza, o se non è adeguatamente progettato e sottoposto a prova prima di essere immesso sul mercato o altrimenti messo in servizio, può individuare le persone in modo discriminatorio o altrimenti errato o ingiusto****. Potrebbe inoltre essere ostacolato l'esercizio di importanti diritti procedurali fondamentali, quali il diritto a un ricorso effettivo e a un giudice imparziale, nonché i diritti della difesa e la presunzione di innocenza, in particolare nel caso in cui tali sistemi di IA non siano sufficientemente trasparenti, spiegabili e documentati.* ***È pertanto opportuno classificare come ad alto rischio, nella misura in cui il loro uso è consentito dal pertinente diritto dell'Unione e nazionale, una serie di sistemi di IA destinati a essere utilizzati nel contesto delle attività di contrasto, in cui l'accuratezza, l'affidabilità e la trasparenza risultano particolarmente importanti per evitare impatti negativi, mantenere la fiducia dei cittadini e garantire la responsabilità e mezzi di ricorso efficaci****. In considerazione della natura delle attività e dei rischi a esse connessi,* ***tra tali sistemi di IA ad alto rischio è opportuno includere****, in particolare,* ***i sistemi di IA destinati*** *a essere utilizzati dalle autorità di contrasto, o per loro conto, o dagli organi o organismi dell'Unione a sostegno delle autorità di contrasto per valutare il rischio per una persona fisica di diventare vittima di reati, come poligrafi e strumenti analoghi,* ***valutare l'affidabilità degli elementi probatori nel corso dell'accertamento e del perseguimento di reati****, e, nella misura in cui*

non è vietato a norma del presente regolamento, determinare il rischio di reato o recidiva in relazione a una persona fisica non solo sulla base della profilazione delle persone fisiche, ma anche della valutazione dei tratti e delle caratteristiche della personalità o del comportamento criminale pregresso delle persone fisiche o dei gruppi, ai fini della profilazione nel corso dell'indagine, dell'accertamento e del perseguimento di reati. ***I sistemi di IA specificamente destinati a essere utilizzati per procedimenti amministrativi dalle autorità fiscali e doganali****, come pure dalle unità di informazione finanziaria che svolgono compiti amministrativi di analisi delle informazioni conformemente al diritto dell'Unione in materia di antiriciclaggio,* ***non dovrebbero essere classificati come sistemi di IA ad alto rischio utilizzati dalle autorità di contrasto a fini di prevenzione, accertamento, indagine e perseguimento di reati****. L'utilizzo degli strumenti di IA da parte delle autorità di contrasto e delle altre pertinenti autorità non dovrebbe diventare un fattore di disuguaglianza o esclusione. L'impatto dell'utilizzo degli strumenti di IA sul diritto alla difesa degli indagati non dovrebbe essere ignorato, in particolare la difficoltà di ottenere informazioni significative sul funzionamento di tali sistemi e la difficoltà che ne risulta nel confutarne i risultati in tribunale, in particolare per le persone fisiche sottoposte a indagini.*

Insomma, in un contesto in cui si denunciano i rischi di un sistema di AI "*se non è addestrato con dati di elevata qualità, se non soddisfa requisiti adeguati in termini di prestazione, accuratezza o robustezza*" e si caldeggia l'inserimento fra le attività ad "alto rischio" quei sistemi impiegati per attività di contrasto criminale, per l'accertamento e la valutazione delle prove ecc., si consente poi, senza mezzi termini, che i sistemi di AI specificamente destinati a essere utilizzati per **procedimenti amministrativi dalle autorità fiscali e doganali**, come pure dalle UIF in materia di antiriciclaggio, **non dovrebbero essere classificati come sistemi di AI ad alto rischio!**

La scelta - per quanto non sorprenda - lascia legittimi dubbi circa il concreto inserimento della disposizione nel contesto generale delle attività disciplinate dall'AI ACT.

La normativa europea, infatti sembra ipotizzare un procedimento amministrativo tributario di acquisizione di dati (ma in fondo, di "prove") non assortito dalle garanzie dei sistemi ad alto rischio, trascurando che tale procedimento è solo il primo *step* di una procedura più complessa che porta:

A) all'irrogazione di sanzioni tributarie che - nella definizione ormai pacificamente accolta dalla Corte EDU, dalla Corte di Giustizia e dalla stessa Corte Costituzionale - sono a tutti gli effetti "***materia penale***";

B) all'utilizzo di quel materiale in sede giudiziaria, posto che - nel nostro come in altri ordinamenti - oggetto del giudizio tributario è in sostanza l'esame del corredo probatorio raccolto dall'Amministrazione Finanziaria per sostenere la propria tesi circa l'infedeltà del contribuente e la necessità di recuperare materia imponibile ed imposta.

Atteso che queste due ultime attività sono pacificamente ricomprese fra le attività "ad alto rischio", come si può ammettere che la fase istruttoria che porta alla definizione della pretesa statuale, sia assortita da minori garanzie?

Il tema, purtroppo, non è secondario perché ammette che in materia fiscale venga adottato uno standard qualitativo decisamente inferiore e per nulla garantista in relazione alla posizione del contribuente, avvalla l'utilizzo di sistemi di AI cd. "***per finalità generali***".

Qualificare infatti un sistema AI "***ad alto rischio***" significa imporre che tale sistema risponda a tutta una serie di caratteristiche tecniche e di cautele che non sono solo limitate alla gestione e prevenzione dei rischi, ma che impattano direttamente anche sul rapporto con i soggetti interessati dal trattamento automatizzato, con l'obbligo di trasparenza e di controllo umano da parte di operatori formati e qualificati, che nello specifico ambito tributario sarebbero parimenti necessari.

In particolare, i sistemi "ad alto rischio":

A) Devono essere progettati e sviluppati in modo tale da garantire che **il loro funzionamento sia sufficientemente trasparente da consentire ai deployer di**

interpretare l'output del sistema e utilizzarlo adeguatamente (art. 13 - Trasparenza e fornitura di informazioni ai deployer[6])

B) Devono essere progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter **essere efficacemente supervisionati da persone fisiche durante il periodo in cui sono in uso** (art. 14 - Sorveglianza umana)

C) I deployer affidano **la sorveglianza umana a persone fisiche che dispongono della competenza, della formazione e dell'autorità necessarie nonché del sostegno necessario** (art. 26 - Obblighi dei deployer dei sistemi di IA ad alto rischio)

In tale prospettiva, pertanto, soltanto ove fosse qualificato "ad alto rischio" il sistema di IA garantirebbe darebbe garanzie di trasparenza e di sorveglianza umana "qualificata" che sono due fra gli elementi di garanzia fondamentali per un esercizio effettivo dei diritti di difesa (anche) del contribuente.

Una sorveglianza ed una trasparenza, che, come visto *supra*, sarebbero tanto più necessarie laddove l'impiego dell'algoritmo fosse esteso - come prevede la normativa - alle fonti "pubblicamente disponibili".

L'AI MADE IN ITALY CHE VERRÀ: IL DDL 1146 APPROVATO IL 20/03/2025

Se da Bruxelles non sembrano giungere notizie confortanti, una volta tanto è da Roma che qualcosa di più rassicurante si sta delineando nell'orizzonte della AI "*made in Italy".*

[6] Art. 2 Definizioni - "*n. 4 «deployer»: una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale*"

E’ notizia recente che dopo mesi di stallo, l’iter parlamentare del DDL 1146 rubricato “*Disposizioni e delega al Governo in materia di intelligenza artificiale*” ha subito una improvvisa accelerazione ed è stato approvato nella notte del 20/03/2025.

Si tratta di una notizia positiva ai nostri fini, atteso che il testo dell’ “AI ACT italiano”, che pure si inserisce dichiaratamente nel quadro dell’attuazione della normativa regolamentare europea, contiene disposizioni specifiche per l’uso dell’AI in ambito amministrativo dal contenuto condivisibile ed incoraggiante.

Il testo dell’art. 13 del DDL prevede infatti che:
“1. Le pubbliche amministrazioni utilizzano l’intelligenza artificiale allo scopo di incrementare l’efficienza della propria attività, di ridurre i tempi di definizione dei procedimenti e di aumentare la qualità e la quantità dei servizi erogati ai cittadini e alle imprese, assicurando agli interessati ***la conoscibilità del suo funzionamento e la tracciabilità del suo utilizzo.***
2. L’utilizzo dell’intelligenza artificiale avviene in ***funzione strumentale e di supporto all’attività provvedimentale****, nel rispetto dell’****autonomia e del potere decisionale della persona*** *che resta l’unica responsabile dei provvedimenti e dei procedimenti in cui sia stata utilizzata l’intelligenza artificiale.*
3. Le pubbliche amministrazioni adottano misure tecniche, organizzative e formative finalizzate a garantire un utilizzo dell’intelligenza artificiale responsabile e a sviluppare le capacità trasversali degli utilizzatori.
4. Le pubbliche amministrazioni provvedono agli adempimenti previsti dal presente articolo con le risorse finanziarie, umane e strumentali disponibili a legislazione vigente.”

Innanzitutto appare rilevante l’affermazione secondo cui la Pubblica Amministrazione “***assicura la conoscibilità***” del funzionamento del sistema di intelligenza artificiale che impiega, e che comunque detto impiego è unicamente attuato in **funzione strumentale e di supporto all’attività provvedimentale**.

Ciò dovrebbe significare che, da un lato, la Pubblica Amministrazione (e quindi anche l’Amministrazione Finanziaria) dovrebbe autorizzare solo sistemi di cui possa

essere assicurata la “conoscibilità” del funzionamento, con esclusione dunque delle “black box”.

Dall’altro, che l’impiego di tali sistemi dovrebbe essere confinato a funzioni “ancillari” di organizzazione dei dati, analisi, interconnessione, con certa esclusione dell’impiego nella fase decisionale: in sostanza dovrebbe essere solo uno strumento di gestione del corredo documentale ed informativo che porta poi il funzionario - inteso come persona fisica - ad adottare un provvedimento di cui ha la piena responsabilità.

Se questo è il quadro normativo generale in cui si muoverà anche l’analisi del rischio sarebbe certamente una buona notizia: il punto è che non vi è nessuna certezza che ciò accadrà realmente, atteso che l’intervento del D. Lgs. 13/2004 è - anche per ragioni cronologiche - del tutto avulso dal contesto del disegno di legge *in itinere*, e sembra dover giungere ad attuazione indipendentemente dal prosieguo parlamentare di quest’ultimo.

Peraltro sembra singolare che il legislatore del DDL non si sia posto minimamente la questione degli impieghi dell’AI in ambito tributario: nel testo normativo approvato dal Senato non si menziona mai né l’Amministrazione Finanziaria, né il diritto tributario, né l’ “accertamento” in quanto tale… che sia un buon segno o meno, purtroppo, ce lo dirà solo l’esperienza.

➡ Sotto tale profilo si ritiene opportuno che UNCAT, nell’ambito delle sue funzioni istituzionali, monitori in sede ministeriale l’iter approvativo del Disegno di Legge, caldeggiando l’adozione di un sistema di tutele che:

A. preveda sempre il controllo umano sull’esito dell’elaborazione algoritmi;

B. preveda la possibilità di conoscere la base di dati impiegata in sede di elaborazione, l’origine degli stessi e le modalità di reperimento;

C. preveda, nello specifico ambito fiscale, l’obbligo di un contraddittorio sulla decisione algoritmica con l’interessato e la

possibilità di un accesso immediato al giudice, anche in via d'urgenza, per poter contestare l'esisto dell'analisi del rischio, prima che l'attività istruttoria finalizzata all'accertamento (accessi, ispezioni, verifiche ecc.) sia conclusa;

D. **preveda comunque, sempre in ambito fiscale, anche in sede di ricorso avverso l'avviso di accertamento, la possibilità di contestare l'esattezza dei dati acquisiti ai fini della selezione del contribuente, con la previsione di inutilizzabilità dei dati acquisiti, laddove il processo preliminare di selezione sia stato condizionato o falsato da una non corretta analisi del rischio.**

LA SENTENZA ITALGOMME: UNA TRINCEA DIFENSIVA ANCHE CONTRO L'ASSALTO DELL'AI?

Mentre il legislatore italiano era tutto intento ad immaginare il futuro dell'accertamento fra banche dati interconnesse e intelligenza artificiale a sopperire le oggettive difficoltà di destreggiarsi fra l'enorme mole di dati disponibili, ecco che un fantasma dal passato è giunto a turbarne le notti, minando alla base le fondamenta stesse di uno degli strumenti più importanti ed invasivi previsti dalla legge per la fase istruttoria: l'accesso.

La sentenza Italgomme Pneumatici Srl ed altri contro Italia, pronunciata lo scorso 6 febbraio 2025 - al momento della redazione di questo documento non ancora definitiva, stante il mancato decorso del termine di impugnazione previsto dall'art. 44 comma 2 lettera b) della CEDU - per quanto (ovviamente) ben lontana dai temi dell'intelligenza artificiale fissa alcuni principi che il legislatore dovrà tenere ben presenti nell'ottica di un ripensamento generale del sistema di accertamento, anche con l'impiego delle nuove tecnologie.

La Corte EDU ha sostanzialmente ravvisato che il sistema fiscale Italiano, che attribuisce all'Amministrazione Finanziaria un vastissimo potere di accedere ai luoghi di esercizio dell'attività imprenditoriale o professionale, mediante "autorizzazioni"

sommariamente motivate, sostanzialmente prive di un controllo preventivo o successivo di legittimità, e che permette, in occasione dell'accesso, una acquisizione indiscriminata ed incontrollata di elementi utili all'accertamento, sia lesivo dei principi fissati dall'art. 8 CEDU[7].

Si tratta, dice la Corte EDU, di una **violazione strutturale**, in relazione alla quale, tuttavia, "*la Corte ritiene che* ***la maggior parte delle misure necessarie siano già previste nella legislazione nazionale, in particolare negli articoli 12 e 13 della Legge n. 212/2000*** *(vedi paragrafo 53 sopra), ma i principi generali affermati in questa legislazione devono essere* ***attuati mediante regole specifiche nella legge statutaria nazionale, mentre la giurisprudenza dovrebbe essere allineata a questi principi e a quelli stabiliti dalla Corte***".

Avete le potenzialità - insomma - ma non le sfruttate…

Partendo da questo assunto, la Corte delinea una serie di criticità insite nel nostro ordinamento:

- gli accessi sono dotati di una motivazione scarna e per nulla idonea: nella specie non vengono adeguatamente motivate le effettive esigenze di una verifica in loco, nonostante la normativa lo preveda;
- l'accesso ai locali commerciali non è sottoposto - in concreto - ad alcuna specifica autorizzazione motivata (prassi avvallata dalla Cassazione) in quanto per la giurisprudenza interna, tali luoghi non rilevano ai fini della tutela del "domicilio" (la cui estensione è molto più circoscritta rispetto all'ambito di applicazione dell'art. 8 CEDU)
- solo nei casi di accesso a luoghi di privata dimora è previsto l'intervento del Pubblico Ministero che tuttavia deve motivare l'autorizzazione con la presenza di

---

[7] *ARTICOLO 8 Diritto al rispetto della vita privata e familiare*

1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.

2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.

gravi indizi di violazioni fiscali solo per l'accesso a luoghi esclusivamente residenziali (non ad uso promiscuo)

- non è in concreto disponibile un rimedio giudiziario per contestare la legittimità dell'accesso, neppure nei casi in cui vi sia autorizzazione del PM;
- il sistema consente l'accesso esplorativo, effettuato al solo fine di ottenere elementi probatori finalizzati all'accertamento: il sistema non prevede che sia richiesto di precisare che cosa ci si aspetta di trovare in sede di accesso in relazione agli anni dell'accertamento
- in sede di accesso qualsiasi elemento e documento - tanto di carattere contabile, quanto di carattere extracontabile, riferito o meno all'annualità oggetto di controllo - può essere acquisito, anche se estraneo alle motivazioni che avevano originato la misura;
- non è consentito ottenere la rimozione o far dichiarare altrimenti inammissibili i documenti non connessi all'accertamento fiscale come prova a carico del contribuente;
- non è consentito un controllo giurisdizionale o comunque indipendente di tali misure che garantiscano sufficientemente dal rischio di abusi e/o arbitrarietà: non è previsto alcun controllo ex post circa la legittimità, la necessità e la proporzionalità delle suddette misure.

E, una volta diagnosticata la malattia, suggerisce le seguenti cure:

- *il quadro giuridico nazionale, se necessario mediante pertinenti direttive interne di prassi amministrativa, dovrebbe* ***indicare chiaramente le circostanze in cui e le condizioni alle quali le autorità nazionali sono autorizzate ad accedere a locali e ad effettuare verifiche fiscali in loco e controlli fiscali presso sedi commerciali*** *e locali adibiti ad attività professionali;*
- *il quadro giuridico nazionale* ***dovrebbe imporre alle autorità nazionali l'obbligo di motivare e, di conseguenza, giustificare la misura in questione alla luce di tali criteri;***
- *dovrebbero essere stabilite garanzie per evitare accessi indiscriminati o, quantomeno, la conservazione e l'utilizzo di documenti e oggetti non pertinenti allo scopo della misura in questione, fatti salvi i poteri delle autorità di avviare separati procedimenti amministrativi;*

- *il contribuente, al più tardi all'avvio della verifica, deve avere il diritto di essere informato delle ragioni che giustificano la verifica e la sua portata, del suo diritto di essere assistito da un professionista, e delle conseguenze del rifiuto di consentire la verifica. Quanto precede si intende fatto salvo il potere delle autorità di accedere a dati relativi al contribuente che siano stati legittimamente acquisiti mediante accesso a banche dati fiscali, banche dati bancarie e finanziarie, e tramite cooperazione con altre autorità, anche su base transfrontaliera.*

Il Governo Italiano, in sede contenziosa ha difeso i criteri selettivi dei contribuenti ai fini dell'accertamento, osservando (punti 90 e 111 della motivazione) che il MEF individua precise linee guida e parametri oggettivi per la selezione dei soggetti da accertare e che la stessa Circolare 4/E del 7 maggio 2021 dell'agenzia delle Entrate, chiarisce che la priorità venga assegnata a quei contribuenti che abbiano dimostrato un più alto rischio, che si siano comportati in modo non collaborativo o non trasparente ecc.

Per la precisione, nel punto 90, per sostenere la sufficiente delimitazione del potere discrezionale ad opera della normativa interna sostiene espressamente che l'impiego delle misure contestate "***(ii) doveva soddisfare i criteri di legalità, efficacia, e trasparenza sulla base di una "analisi dei rischi" effettuata nel rispetto dei principi di proporzionalità ed adeguatezza***"

Sul punto la Corte è netta: "*112.* ***La Corte è disposta ad accettare che, quando le misure in questione sono attuate ai fini di un accertamento fiscale (v. punto 99), condizioni come quelle stabilite negli orientamenti presentati dal Governo potrebbero essere sufficienti*** *a integrare le disposizioni nazionali applicabili al fine di delimitare l'ambito di discrezionalità conferito alle autorità nazionali e prevenire abusi e arbitrarietà,* ***a condizione che siano vincolanti per le autorità****. Tuttavia la Corte rileva che* ***non è possibile alcun controllo sulla base dei soli criteri di selezione sopra menzionati ed in assenza di informazioni pubbliche trasparenti*** *su quali locali commerciali sono ispezionati nel tempo e quali no, e non si può escludere la possibilità che gli agenti fiscali esercitino un margine di discrezionalità illimitato dietro l'apparente rispetto di tali criteri* ".

Perché tali principi impattano anche sul tema dell'intelligenza artificiale?

Perché le argomentazioni della Corte richiamano proprio quegli stessi criteri di analisi del rischio e trasparenza del processo selettivo e decisionale che sono alla base anche dell'impiego degli strumenti di AI.

L'esigenza di tutelare il diritto fondamentale al rispetto della vita privata - e quindi, nel caso specifico, a non subire accessi pressoché immotivati, finalizzati ad una sorta di *fishing expedition*, con il salvacondotto di una giurisprudenza che in ogni caso, alla fine "salva" sempre gli elementi raccolti in quella sede - valorizza proprio il tema dell'analisi del rischio quale attività prodromica, non invasiva e utile per motivare l'impiego delle misure più impattanti come l'accesso.

E in questo senso Corte EDU, ammette senza particolari riserve la possibilità di utilizzare "*dati relativi al contribuente che siano stati legittimamente acquisiti mediante accesso a banche dati fiscali, banche dati bancarie e finanziarie, e tramite cooperazione con altre autorità, anche su base transfrontaliera*"; sembra anzi suggerire che proprio tale legittima attività debba essere eseguita in via preliminare, relegando gli accessi ai locali commerciali solo in presenza di circostanze ben determinate, al ricorrere di determinate condizioni e previa motivazione in ordine alla ricorrenza dei detti criteri nel caso concreto.

Ma appunto, a ben guardare, **quell'accesso preliminare alle banche dati, altro non è che una forma di "analisi del rischio" come definita dall'art. 2 D. Lgs. 13/2024**: ossia un "*processo*" che "*tramite modelli e tecniche di analisi deterministica ovvero probabilistica", "utilizza, anche attraverso la loro interconnessione, le informazioni presenti nelle basi dati dell'Amministrazione finanziaria, ovvero pubblicamente disponibili*".

Il suggerimento che si può trarre dalle indicazioni della Corte EDU, è pertanto nel senso di creare un sistema graduato, in cui a partire da una analisi preliminare del rischio (anche con l'impiego dell'AI, ai fini della lettura e della valutazione degli

elementi derivanti dalle banche dati a disposizione dell'Amministrazione Finanziaria), si ottengano elementi idonei a giustificare e motivare livelli di controllo più invasivi, sulla base di poteri e criteri che vengano predeterminati dalla legge e che abbiano comunque la possibilità di essere sindacati in sede giurisdizionale, prima che si giunga alla definizione dell'accertamento.

Ma, avverte la Corte, anche questo sistema, **di per sé non è sufficiente se non viene attuato in un contesto di "trasparenza".**

Gli elementi di valutazione impiegati nell'analisi del rischio devono essere conoscibili e devono essere lavorati in modo da comprenderne la logica, perché sia rispettata la regola dell'effettività del controllo: "***non è possibile alcun controllo (…omissis…) in assenza di informazioni pubbliche trasparenti".***

Anche sotto tale profilo nell'ottica di progettare un sistema conforme ai principi espressi dalla Corte, si rende del tutto necessario che - come previsto dal DDL 1146 - non solo vi sia trasparenza dei dati (inteso come possibilità di conoscere da dove siano stati acquisiti e come siano stati trattati), ma che gli stessi sistemi di AI impiegati possano assicurare la "conoscibilità" e la "verifica" del loro funzionamento, con esclusione dunque delle cd. "black box".

L'INTELLIGENZA ARTIFICIALE COME STRUMENTO PER UNA NUOVA STRUTTURA DELL'ACCERTAMENTO.

L'utilizzo dell'intelligenza artificiale nell'ambito dell'accertamento non è un vezzo, ma una reale necessità per poter gestire una mole di dati contenuti in una miriade di banche dati pubbliche, individuando in maniera più agevole quelle anomalie che possono lasciare emergere dubbi sulla "fedeltà" di un determinato contribuente, nell'ottica di rendere il sistema dei controlli più efficace, ma anche, sperabilmente, più imparziale e più "giusto".

La condizione essenziale perché tali obiettivi possano essere realizzati, nel rispetto dei diritti del contribuente e con la stretta applicazione del principio di capacità contributiva, è che i dati sui quali l'analisi viene effettuata provengano da **fonti certe e certificate**, rispetto alle quali siano chiare anche le finalità del trattamento in un'ottica di piena conformità alla normativa nazionale sulla protezione dei dati e al GDPR.

Ciò porta ad esprimere contrarietà e - quantomeno - cautela rispetto all'impiego paventato delle fonti aperte che nessuna garanzia possono fornire in ordine alla genuinità del dato e che, comunque, contengono, evidentemente, dati del tutto avulsi dal contesto fiscale e trattati per finalità affatto diverse (come tali - si dovrebbe ritenere - non utilizzabili sulla base del principio di minimizzazione e di esattezza dei dati imposti dall'art. 5 GDPR).

Al netto di tali cautele, anche nella prospettiva di un ripensamento generale della disciplina dell'accertamento, indicata anche dalla Corte EDU, l'intelligenza artificiale può realmente costituire un mezzo che coniughi la legittima aspirazione ad un sistema efficace ed efficiente, alla tutela in concreto dei diritti del contribuente.

Il suo impiego in sede di analisi del rischio potrebbe costituire idealmente il primo livello di controllo, una sorta di pre-istruttoria che abbia la funzione di selezionare, nell'ambito delle direttive stabilite a livello centrale, regionale o provinciale, i contribuenti a maggior rischio, non sulla base di elementi presuntivi teorici, ma sulla base di elementi certi derivanti dall'interconnessione dei dati contenuti nelle banche dati pubbliche - e solo da quelle!

L'esito della analisi del rischio in sede pre-istruttoria, potrebbe, previo controllo dell'operatore umano, consentire di formulare una adeguata motivazione alla decisione di procedere con una vera e propria istruttoria che, nei casi a minor indice di rischio, potrebbe limitarsi all'invio di questionari o inviti e solo nei casi più gravi e rilevanti, accessi, ispezioni e verifiche (in tali ipotesi, sempre previa autorizzazione motivata analiticamente da parte di un superiore gerarchico, o dal Pubblico Ministero, nei casi in cui richiesto).

Tale sistema dovrebbe presupporre, in ogni caso, la possibilità per il contribuente, nel caso in cui all'esito di tale analisi venissero avviate ulteriori attività di approfondimento, di poter conoscere:

- le fonti specifiche alle quali il sistema ha attinto i dati;
- i dati che sono stati ritenuti rilevanti dal sistema nell'evidenziare un rischio;
- le logiche con cui i dati sono stati processati

E ciò anche al fine di un controllo giurisdizionale sulla sussistenza dei presupposti per l'avvio di una vera e propria istruttoria, che dovrebbe sempre essere riconosciuto, anche eventualmente affidandolo ad autorità indipendenti (come il Garante del Contribuente), a condizione di dotarle sul punto di poteri effettivi e cogenti.

Tale controllo dovrebbe essere strutturato in modo da consentire di contestare l'esito dell'analisi del rischio, la ricorrenza dei presupposti di legge per l'impiego delle forme più invasive di controllo, la verifica dell'idoneità della motivazione dell'atto che li dispone, prima della conclusione dell'istruttoria e dalla chiusura del PVC (nell'ottica di non pregiudicare la difesa del contribuente mediante accesso agli istituti definitori previsti dalla recente riforma).

Un simile ricorso giurisdizionale, tuttavia, non dovrebbe limitarsi alla fase dell'istruttoria: le contestazioni sugli esiti dell'analisi del rischio e sui presupposti per le forme ulteriori di controllo (diverse dall'interconnessione delle banche dati) dovrebbe sempre essere consentita anche in sede di impugnazione dell'accertamento per garantire comunque - anche in una fase "postuma" - il controllo giudiziale sulla legittimità e sulla proporzionalità rispetto ai rischi individuati del procedimento di acquisizione delle "prove".

In questo senso l'ausilio dell'intelligenza artificiale come strumento al servizio dell'operatore umano dovrebbe semplificare l'onere motivazionale che, anche nella giurisprudenza della Corte EDU (ed in conformità con quanto previsto dalla normativa interna troppo spesso "svalutata") deve essere considerato un cardine

imprescindibile della tutela del contribuente, sin dalle fasi dell'accesso, del controllo e della verifica.

Avv. Alberto Michelis

Vice-Presidente Camera degli Avvocati Tributaristi della Liguria