

3.

SUL TRATTAMENTO DEI DATI PERSONALI  
NELL'AMBITO DELLE NUOVE PROCEDURE  
AUTOMATIZZATE PER IL CONTRASTO  
DELL'EVASIONE FISCALE

di *Giovanni Consolo*

SOMMARIO: 1. Cenni introduttivi sul processo di digitalizzazione dell'Amministrazione finanziaria. — 2. Il nuovo applicativo Ve.R.A. di analisi del rischio fiscale dei contribuenti. — 3. La rilevanza della normativa in tema di protezione dei dati personali e gli interventi del Garante per la protezione dei dati personali con riguardo alle nuove procedure automatizzate di contrasto all'evasione fiscale. — 3.1. Il diritto alla "intelligibilità" dell'algoritmo. — 3.2. Il diritto di non essere sottoposti a decisioni fondate su trattamenti esclusivamente automatizzati. — 3.3. Verifiche sulla qualità dei modelli di analisi, tecniche di pseudonimizzazione dei dati e altre misure di sicurezza per l'elaborazione dei dati. — 4. Considerazioni conclusive.

1. *Cenni introduttivi sul processo di digitalizzazione dell'Amministrazione finanziaria.*

Il giudice della Corte Europea dei Diritti dell'Uomo Louis-Edmond Pettiti, nella sentenza *Malone c. Regno Unito* del 2 agosto 1984 (1), affermava che "*The danger threatening demo-*

---

(1) Testo, con l'aggiunta delle note, della relazione svolta dall'Autore al webinar "*In-Visibili: poteri, dati e modelli di business nella digitalizzazione tributaria*", organizzato dall'Università degli Studi di Torino e svoltosi in data 19 aprile 2023 nell'ambito del PRIN 2020: "*La digitalizzazione dell'Amministrazione finanziaria tra contrasto all'evasione fiscale e tutela dei diritti dei contribuenti*".

CEDU, *Malone c. The United Kingdom Judgment*, ric. n. 8691/79 (1984).

*cratic societies in the years 1980-1990 stems from the temptation facing public authorities to “see into” the life of the citizen*”. In particolare, il giudice Pettiti evidenziava come, “*In order to answer the needs of planning and of social and tax policy, the State is obliged to amplify the scale of its interferences. In its administrative systems, the State is being led to proliferate and then to computerise its personal data-files*” e, infine, “*to build up a “profile” of each citizen*” (2).

Con estrema lungimiranza, già negli anni '80 si anticipava, dunque, il pensiero di quanti oggi ritengono che l'indiscriminata e generalizzata raccolta di dati personali da parte delle autorità pubbliche, accoppiata all'uso delle moderne tecnologie, rischi di dare origine ad un “*panopticum* digitale” e, segnatamente, all'affermazione di un potere pubblico che vede chiunque senza essere visto (3).

Anche se non ancora dotato del crisma della attualità (o così, almeno, potrebbe sembrare a chi normalmente si interfaccia con la realtà operativa di un qualche Ufficio dell'Agenzia delle Entrate o Comando della Guardia di Finanza (4)) questo “rischio” (5) è particolarmente avvertito, nei rapporti tra contribuenti e A.F., per almeno una coppia di ragioni.

---

(2) *Concurring Opinion of Judge Pettiti* (traduzione inglese), nel caso *Malone c. The United Kingdom Judgment*, cit.

(3) Cfr., G. PITRUZZELLA, *Dati fiscali e diritti fondamentali*, in *Dir. prat. trib. int.*, 2, 2022, 666 ss., e, sulla stessa linea, F. FARRI, *Digitalizzazione dell'amministrazione finanziaria e diritti dei contribuenti*, in *Riv. dir. trib.*, 2020, 120-123, il quale, guardando con condivisibile scetticismo al paradigma “fisco amico” (in quanto, sul piano di rapporti concreti tra amministrazione e contribuente, “gli interessi non possono che essere contrapposti, come lo sono quelli di debitore e creditore”), ritiene che “un ‘grande fratello’ che controlla ogni aspetto della vita del contribuente non è una regola desiderabile, neppure se esso mira alla realizzazione di una funzione pubblica di primario rilievo e valore qual è quella tributaria”.

(4) Al riguardo v. anche *infra*, nota 31.

(5) È indubbio che le potenzialità offerte dal progresso tecnologico debbano essere poste a servizio dell'Amministrazione finanziaria (sul collegamento tra l'impiego degli strumenti digitali e il miglioramento dell'efficienza amministrativa, v. gli studi pionieristici di A. PREDIERI, *Gli elaborati elettronici nell'amministrazione dello Stato*, Bologna, 1971, e G. DUNI, *L'utilizzabilità delle tecniche elettroniche nell'ema-*

Innanzitutto, perché per vaste categorie di contribuenti si è gradualmente ridotta ogni possibilità di utilizzo di modalità non digitali nella gestione dei rapporti con il fisco (6), così consentendo all'A.F. di acquisire e conservare in apposite banche dati grandi quantità di informazioni, che possono essere facilmente utilizzate per migliorare, sotto il duplice profilo qualitativo e quantitativo, le attività di controllo e di accertamento. In secondo luogo, perché l'A.F. è oggi in grado di sfruttare l'ampio patrimonio di dati a sua disposizione, mediante metodologie di analisi del rischio dei contribuenti fondate su elaborazioni statistiche e processi automatizzati, che sono divenute sempre più evolute e sofisticate anche mediante lo sfruttamento dell'intelligenza artificiale (7).

---

*nazione degli atti e nei procedimenti amministrativi. Spunti per una teoria dell'atto amministrativo elaborato nella forma elettronica*, in *Riv. Amm.*, 1978, 407 ss.). Tuttavia, gli straordinari sviluppi tecnologici in corso stanno conducendo a risultati dirimpenti e, sino a poco tempo fa, inimmaginabili, che impongono un atteggiamento di "vigile apertura", volto a declinare le regole esistenti per fornire adeguate garanzie all'esercizio del potere in forma automatizzata o semiautomatizzata (cfr. G. AVANZINI, *Decisioni amministrative e algoritmi informatici*, Napoli, 2019, 81), rifuggendo dalla massima "nulla da nascondere, nulla da temere" (su cui si rinvia agli studi sociologici di D. LYON, *The Culture of Surveillance: Watching as a Way of Life*, Cambridge, 2018), sovente impiegata dall'opinione pubblica per legittimare un indiscriminato e massivo impiego di strumenti tecnologici per la tutela di rilevanti interessi pubblici.

(6) Per una panoramica su tali aspetti, e sull'esigenza di tutelare la libertà negativa dei contribuenti di non utilizzare tecnologie digitali, v., in modo particolare, A. CONTRINO, *Digitalizzazione dell'amministrazione finanziaria e attuazione del rapporto tributario: questioni aperte e ipotesi di lavoro nella prospettiva dei principi generali*, in *Riv. dir. trib.*, 2023, 105 ss., nonché, in un contesto più generale, F. PAPARELLA, *L'ausilio delle tecnologie digitali nella fase di attuazione dei tributi*, in *Riv. dir. trib.*, 2022, 617 ss.; M. LOGOZZO, *La centralità della telematica negli adempimenti tributari: la fattura elettronica*, in L. DEL FEDERICO, F. DELFINI (a cura di), *La Digital Economy nel sistema tributario italiano ed europeo*, Padova, 2015, 119 ss.; R. CORDEIRO GUERRA, *L'intelligenza artificiale nel prisma del diritto tributario*, in *Dir. prat. trib.*, 2020, 921.

(7) Cfr., diffusamente, A. CONTRINO, *Banche dati tributarie, scambio di informazioni fra autorità fiscali e "protezione dei dati personali": quali diritti e tutele per i contribuenti?*, in *Riv. telem. dir. trib.*, 2019, 7 ss.

Come emerge dalle prime indagini condotte ad oggi (8), il quadro appena delineato pone anche in materia tributaria numerose questioni con riguardo alla tutela dei diritti fondamentali degli individui e alla disciplina (multilivello) della protezione dei dati personali, soprattutto alla luce di talune criticità (come, ad esempio, l'opacità dei procedimenti di formulazione degli algoritmi, l'esposizione dei dati sensibili o particolari degli individui, i rischi connessi alla profilazione, l'assenza di interventi umani) che inevitabilmente si ricollegano all'utilizzo di procedure automatizzate in ambito amministrativo (9).

---

(8) Oltre agli autori richiamati nelle note 3, 6 e 7, v., senza pretesa di completezza e limitatamente alla dottrina nazionale: A. SANTORO, *Nuove frontiere per l'efficienza dell'amministrazione fiscale: tra analisi del rischio e problemi di privacy*, in G. ARACHI, M. BALDINI, *La finanza pubblica italiana. Rapporto 2019*, Bologna, 2019, 66 ss.; A. CARINCI, *Fisco e privacy: storia infinita di un apparente ossimoro*, in *Il fisco*, 2019, 4407 ss.; A. CONTRINO, S.M. RONCO, *Prime riflessioni e spunti in tema di protezione dei dati personali in materia tributaria, alla luce della giurisprudenza della Corte di Giustizia e della Corte EDU*, in *Dir. prat. trib. int.*, 2019, 599 ss.; M. D'AMBROSIO, *La protezione dei dati personali alla luce della giurisprudenza CEDU e CGUE: aspetti generali e profili di criticità*, in *Dir. prat. trib. int.*, 2019, 970 ss.; G. SALANITRO, *Amministrazione finanziaria e Intelligenza Artificiale, tra titolarità della funzione e responsabilità*, in S. ALEO (a cura di), *Evoluzione scientifica e profili di responsabilità*, Pisa, 2021, 414-423; G. PALUMBO, *Contrasto all'evasione fiscale e impatto sulla privacy dei contribuenti*, in G. PALUMBO (a cura di), *Fisco e privacy. Il difficile equilibrio tra lotta all'evasione e tutela dei dati personali*, Pisa, 2021, 13 ss.; A.S. DORIGO, *L'intelligenza artificiale e i suoi usi pratici nel diritto tributario: Amministrazione finanziaria e giudici*, in R. CORDEIRO GUERRA, S. DORIGO (a cura di), *Fiscalità dell'economia digitale*, Pisa, 2022, 204; A. TOMO, *La "forza centripeta" del diritto alla protezione dei dati personali: la Corte di Giustizia sulla rilevanza in ambito tributario dei principi di proporzionalità, accountability e minimizzazione*, in *Dir. prat. trib. int.*, 2022, 908 ss.; G. ZICCARDI, *Protezione dei dati, lotta all'evasione e tutela dei contribuenti: l'approccio del Garante per la protezione dei dati italiano tra trasparenza, big data e misure di sicurezza*, in G. RAGUCCI (a cura di), *Fisco digitale. Cripto-attività, protezione dei dati, controlli algoritmici*, Torino, 2023, 61 ss.

(9) Per una panoramica generale, v. F. PIZZETTI, *La protezione dei dati personali e la sfida dell'intelligenza artificiale*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, 5 ss. e A. PIERUCCI, *Elaborazione dei dati e profilazione delle persone*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 414-419, 449-451.

Il nuovo fronte del dibattito, oggetto del mio intervento odierno, è rappresentato dall'applicativo noto con l'acronimo "Ve.Ra" (10) che consentirà all'Amministrazione finanziaria di incrociare ed elaborare, anche mediante l'applicazione di tecniche di intelligenza artificiale, tutte le informazioni contenute nell'Archivio dei rapporti finanziari e nelle altre banche dati a sua disposizione, al duplice scopo di selezionare le liste di contribuenti da sottoporre a controllo e di rilevare anomalie fiscali da comunicare ai contribuenti ai sensi dell'art. 1, commi 634-636, L. n. 190/2014 (mediante l'invio delle c.d. "lettere di compliance" o "lettere cambia-verso"), così da favorire l'azione di stimolo dell'adempimento spontaneo.

2. *Il nuovo applicativo Ve.R.A. di analisi del rischio fiscale dei contribuenti.*

L'applicativo Ve.R.A. è gemmato da una serie di disposizioni della Finanziaria per il 2020 (art. 1, comma 682 e ss., legge 27 dicembre 2019, n. 160), attuate, nel giugno dello scorso anno, con un decreto del MEF (11) previamente approvato dal Garante della privacy. Le informazioni disponibili su Ve.R.A. non sono invero moltissime. In alcune recenti interlocuzioni con il citato Garante (su cui ci si soffermerà *infra*), l'Agenzia delle Entrate ha opposto infatti la necessità di preservare la riservatezza e la sicurezza delle relative informazioni, e ciò per la comprensibile esigenza di scongiurare la creazione di software ela-

---

(10) Su cui di recente C. FRANCIOSO, *Intelligenza artificiale nell'istruttoria tributaria e nuove esigenze di tutela*, in *Rass. trib.*, 2023, 47 ss. Per una panoramica più generale, si rinvia alle anticipatorie osservazioni di S. DORIGO, *Intelligenza artificiale e norme antiabuso: il ruolo dei sistemi "intelligenti" tra funzione amministrativa e attività giurisdizionale*, in *Rass. trib.*, 2019, 728 ss.

(11) Cfr. Decreto MEF, 28 giugno 2022 di «Attuazione dell'articolo 1, comma 683, della legge 27 dicembre 2019, n. 160, relativo al trattamento dei dati contenuti nell'archivio dei rapporti finanziari».

borati con tecniche di “ingegneria inversa” che possano consentire ai contribuenti di eluderne la sorveglianza (12).

Ciò lascia intuire le enormi potenzialità di Ve.R.A., che, da un lato, accederà a tutte le banche dati di cui dispone l'A.F. (13) e, dall'altro, sarà in grado di elaborare la vasta mole di informazioni reperibile in tali banche dati, mediante l'impiego delle più moderne tecnologie informatiche, tra cui quelle di apprendimento automatizzato (c.d. *machine learning*), anche al fine di condurre analisi di tipo probabilistico volte ad estrarre i profili fiscali ed economico-finanziari dei “contribuenti-evasori”, muovendo dallo studio delle caratteristiche dei soggetti nei cui confronti è stato già emesso un avviso di accertamento.

In particolare, secondo le informazioni fornite dal MEF (14), il nuovo applicativo dovrebbe impiegare: (i) da un lato, modelli di analisi c.d. “deterministici”, finalizzati a ricostruire, attraverso l'analisi integrata dei dati presenti nell'Archivio dei rapporti finanziari e degli altri elementi informativi in possesso dell'Amministrazione finanziaria, il patrimonio e i flussi finanziari dei singoli contribuenti, al fine di evidenziare eventuali incongruenze tra gli stessi, i redditi dichiarati, il consumo e/o il risparmio; (ii) dall'altro lato, modelli di analisi c.d. probabilistici (o stocastici), basati su processi di osservazione e modellazione dei dati, finalizzati a profilare i singoli contribuenti

---

(12) V., per ulteriori considerazioni, C. FRANCIOSO, *op. cit.*, 65.

(13) Tra cui, a titolo meramente esemplificativo: l'Archivio dei rapporti finanziari ove sono presenti dati contabili di diverse tipologie di rapporti finanziari, come saldi, giacenza media e totale degli accrediti e degli addebiti effettuati in un anno solare; le banche dati ove sono custoditi i dati (c.d. “dati fattura” e i “dati fattura integrati”) delle fatture elettroniche; le banche dati gestite da operatori privati, come Orbis e Aida, ma cui l'A.F. ha normalmente accesso in sede di verifica; il Pubblico Registro Automobilistico (c.d. PRA); i dati delle circoscrizioni aeroportuali; i dati INPS; (vii) i dati di Comuni, Regioni e compagnie assicurative; i dati liberamente accessibili su siti e piattaforme web, tra cui i social network (nei limiti dei contenuti resi pubblici dagli utenti).

(14) V. *supra* nota 11.

e, segnatamente, ad assegnare a ciascun contribuente, su base probabilistica, un determinato “rischio fiscale”.

In definitiva, secondo quanto è dato comprendere dalle (non molte) indicazioni fornite dall’Amministrazione finanziaria, l’applicazione di Ve.R.A. non dovrebbe, a rigore, innescare attività automatizzate di controllo, ma, piuttosto, perseguire l’ambizioso (e auspicabile) obiettivo di allocare le risorse dell’Amministrazione finanziaria in modo più efficiente (intercettando anomalie o disallineamenti sintomatici di un rischio fiscale elevato ed espungendo dalle “liste selettive” contribuenti per i quali tali incongruenze possono essere spiegate già in fase di analisi dei dati o che risultano non significative) e, per l’effetto, di assicurare che le attività di controllo sul campo avvengano sulla base di concrete ed effettive esigenze di indagine, con il minor intralcio per le attività dei contribuenti, in linea con quanto stabilito dall’art. 12 dello Statuto dei diritti del contribuente.

In dottrina, è stato prospettato il rischio che il nuovo applicativo — pur se formalmente volto a coadiuvare l’Agenzia delle Entrate e la Guardia di Finanza nell’elaborazione di “liste selettive” e nell’invio di inviti alla regolarizzazione — possa essere impiegato, nel prossimo futuro, per l’emanazione di “accertamenti automatizzati”, senza alcun intervento umano “a valle” dell’elaborazione algoritmica (15).

Per tale motivo — e muovendo (se non si è frainteso) dall’assunto che la disciplina sulla protezione dei dati personali non predisporrebbe efficaci “anticorpi” contro simili automa-

---

(15) V. G. RAGUCCI, *L’analisi del rischio di evasione in base ai dati dell’archivio dei rapporti con gli intermediari finanziari: prove generali dell’accertamento algoritmico?*, in *Riv. tel. dir. trib.*, 4 settembre 2019, C. FRANCIOSO, *op. cit.*, 82-90 e, da ultimo, M. FASOLA, *Le analisi del rischio di evasione tra selezione dei contribuenti da sottoporre a controllo e accertamento “algoritmico”*, in G. RAGUCCI (a cura di), *Fisco digitale. Cripto-attività, protezione dei dati, controlli algoritmici*, Torino, 2023, 79 ss.

tismi accertativi (16) — la citata dottrina ha ravvisato la necessità di indirizzare il dibattito su Ve.R.A. verso quegli istituti dell'ordinamento tributario (come, ad esempio, le norme che disciplinano la motivazione degli atti impositivi) che dovrebbero impedire un così esteso impiego dell'intelligenza artificiale nell'attività di accertamento.

Muovendo da queste conclusioni, nel prosieguo si tenterà di fornire un contributo al dibattito, ancora agli albori, cercando di dimostrare come, in realtà, anche la disciplina in tema di protezione dei dati personali offra ampie tutele in tema di procedimenti tributari automatizzati, eventualmente anche attraverso quel micro-cosmo di regole che disciplinano la tutela amministrativa e giurisdizionale (davanti al giudice ordinario) dei dati personali (17).

3. *La rilevanza della normativa in tema di protezione dei dati personali e gli interventi del Garante per la protezione dei dati personali con riguardo alle nuove procedure automatizzate di contrasto all'evasione fiscale.*

Come accennato nel precedente paragrafo, dopo l'approvazione del decreto ministeriale con cui sono state adottate le regole tecniche del nuovo applicativo Ve.R.A., l'Agenzia delle Entrate, in qualità di responsabile del trattamento dei dati, ha

---

(16) V., ad esempio, C. FRANCIOSO, *op. cit.*, 78-81 (par “3.3.2. La limitata tutela dei dati personali nei procedimenti automatizzati tributari”).

(17) Su cui v., *ex multis*, G. COSTANTINO, *La tutela giurisdizionale dei diritti al trattamento dei dati personali*, in *Riv. trim. dir. proc. civ.*, 2004, 1221 ss.; E. PELLINO, *Le tutele e il danno risarcibile*, in E. PELLINO, L. BOLOGNINI, C. BISTOLFI (a cura di), *Il regolamento privacy europeo*, Milano, 2016, 579; A. CANDINI, *Gli strumenti di tutela*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla tutela dei dati personali*, Bologna, 2017, 570; A. MARCHESELLI, S.M. RONCO *Dati personali, Regolamento GDPR e indagini dell'Amministrazione finanziaria: un modello moderno di tutela dei diritti fondamentali?*, in *Riv. dir. trib.*, 2022, 112-119.

avviato una serie di interlocuzioni con il Garante della privacy (18).

Tecnicamente, l’Agenzia ha, dapprima, eseguito una “valutazione d’impatto”, ai sensi dell’art. 35 del Regolamento GDPR, e, poi, sottoposto la predetta valutazione al Garante, ai sensi del successivo art. 36 (19). Con provvedimento n. 276/2022, il Garante ha autorizzato l’impiego di Ve.R.A., ponendo, tuttavia, una serie di rilevanti condizioni e riserve.

Innanzitutto, è stata circoscritta la portata dell’autorizzazione ad una mera “fase di test”, da condurre “su un campione casuale rappresentativo della popolazione”. In secondo luogo — ed è questo il profilo di maggior rilievo — il Garante ha esercitato i propri poteri correttivi ai sensi dell’art. 58, par. 1, lett. *d*), del Regolamento GDPR (20), imponendo all’Agenzia delle Entrate l’implementazione (già nella fase di “test” dell’applicativo) di una serie di rilevanti accorgimenti al fine di assicurare il rispetto dei principi di “trasparenza” o “intelligibilità dell’algoritmo”, di “non esclusività della decisione algoritmica” e di “non discriminazione”, già noti alla giurisprudenza amministrativa e che, come chiaramente riconosciuto anche dal Consiglio di Stato (21), discendono direttamente da diverse disposizioni del Regolamento GDPR (22).

---

(18) Cfr., dapprima, Garante per la protezione dei dati personali, provv. 22 dicembre 2021, n. 453 e, da ultimo, Id. provv. 30 luglio 2022, n. 276.

(19) Su tale procedimento, v., per tutti, R. TORINO, *La valutazione d’impatto (Data Protection Impact Assessment)*, in V. CUFFARO, R. D’ORAZIO, V. RICCIUTO (a cura di), *op. cit.*, 855.

(20) Cfr. R. TORINO, *op. ult. cit.*, 874-878.

(21) Cfr., in particolare, Consiglio di Stato, sez. VI, 13 dicembre 2019, n. 8472, ove è stato statuito che; *(i)* “gli articoli 13 e 14 del Regolamento stabiliscono che nell’informativa rivolta all’interessato venga data notizia dell’eventuale esecuzione di un processo decisionale automatizzato”; *(ii)* “L’interesse conoscitivo della persona è ulteriormente tutelato dal diritto di accesso riconosciuto dall’articolo 15 del Regolamento che contempla, a sua volta, la possibilità di ricevere informazioni relative all’esistenza di eventuali processi decisionali automatizzati”; *(iii)* “Sul versante della verifica degli esiti e della relativa imputabilità, deve essere garantita la verifica a valle, in termini di logicità e di correttezza degli esiti. Ciò a garanzia

Chiarita l'assoluta rilevanza della normativa in tema di protezione dei dati personali, occorre ora soffermarsi sui principali accorgimenti tecnici che il Garante ha imposto all'Agenzia e, con riguardo a ciascuno di tali accorgimenti, indagare le finalità perseguite, nonché le disposizioni e i principi del Regolamento GDPR che di volta in volta vengono in rilievo.

### 3.1. *Il diritto alla "intelligibilità" dell'algoritmo.*

Innanzitutto, il Garante ha imposto all'Agenzia di "raccolgere opinioni" sul funzionamento dell'applicativo da parte dei soggetti che saranno "a vario titolo coinvolti nei trattamenti in esame" (come le associazioni di categoria e gli ordini professionali) e di "pubblicare un estratto della valutazione di impatto", con eccezione degli "allegati" e delle "parti che potrebbero compromettere la sicurezza dei trattamenti" (23).

---

dell'imputabilità della scelta al titolare del potere autoritativo, individuato in base al principio di legalità, nonché della verifica circa la conseguente individuazione del soggetto responsabile, sia nell'interesse della stessa p.a. che dei soggetti coinvolti ed incisi dall'azione amministrativa affidata all'algoritmo"; (iv) "dal considerando n. 71 del Regolamento 679/2016 il diritto europeo trae un ulteriore principio fondamentale, di non discriminazione algoritmica, secondo cui è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, mettendo in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali, secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti".

(22) V. anche A. MARRA, *Obsolescenza e attualità della legge n. 241/1990 nell'era dell'amministrazione digitale*, in A. BARTOLINI ANTONIO, T. BONETTI, B. MARCHETTI, B. G. MATTARELLA, M. RAMAJOLI (a cura di), *La legge n. 241 del 1990, trent'anni dopo*, Torino, 2022, 385 ss.

(23) In ottemperanza al citato provv. n. 276/2022 del Garante, l'Agenzia delle Entrate, alla fine di maggio di quest'anno, ha pubblicato sul proprio sito

Questi accorgimenti, se si ragiona secondo gli schemi del diritto tributario, potrebbero risultare non del tutto giustificabili nei limiti in cui l'applicativo Ve.R.A. sia effettivamente utilizzato solamente nella fase di analisi del rischio fiscale. Invero, con riguardo alla selezione dei contribuenti da sottoporre a controllo, l'opacità che contraddistingue le "tecniche impiegate" non dovrebbe destare particolari perplessità, in quanto risulta tutto in linea con la segretezza che contraddistingue questa fase dell'attività amministrativa (24). E ciò vale, a maggior ragione, se si ritiene che quella di "selezione" sia un'attività priva di rilevanza esterna, in cui l'A.F. esercita una propria facoltà di scelta non sindacabile (25).

Per contro, secondo la disciplina sul trattamento dei dati personali, l'interesse fiscale alla segretezza deve essere attentamente bilanciato con i diritti attribuiti ai contribuenti dal Regolamento GDPR e, segnatamente, per quanto qui di interesse, il diritto alla "intelligibilità" dell'algoritmo (rinvenibile negli articoli 13, 14 e 15 del Regolamento GDPR), in base al quale l'interessato nei cui confronti venga svolto un processo basato su trattamenti automatizzati ha il diritto di ricevere informazioni significative sulla logica utilizzata, così da poterla comprendere.

Invero, l'art. 23 del Regolamento GDPR, al pari della

---

istituzionale uno stralcio della valutazione di impatto (cfr. "Documento di Valutazione di Impatto sulla Protezione dei Dati") e un documento in cui vengono descritte le metodologie utilizzate nell'ambito delle attività di analisi del rischio mediante l'applicativo Ve.R.A. (cfr. "Informativa Sulla Logica Sottostante I Modelli Di Analisi Del Rischio Basati Sui Dati Dell'archivio Dei Rapporti Finanziari").

(24) Così C. FRANCIOSO, *op. cit.*, 65.

(25) Cfr. L. SALVINI, *La partecipazione del privato all'accertamento (nelle imposte sui redditi e nell'IVA)*, Padova, 1990, spec. 84, e F. GALLO, *Discrezionalità nell'accertamento e sindacabilità delle scelte d'ufficio*, in *Riv. dir. fin.*, 1992, 656. Sul risalente dibattito in merito alla natura dell'attività amministrativa di selezione dei contribuenti da assoggettare a controllo e, quindi, sulla rilevanza solo interna o anche esterna degli atti ministeriali contenenti i relativi criteri, v., fra gli altri, G. VANZ, *I poteri conoscitivi e di controllo dell'amministrazione finanziaria*, Padova, 232 ss. e G. FRANSONI, *Le indagini tributarie. Attività e poteri conoscitivi nel diritto tributario*, Torino, 2020, 37 ss.

normativa nazionale di attuazione, stabilisce che ogni deroga al diritto in esame, per essere legittima, debba essere compatibile con il principio di proporzionalità.

Tale principio, inizialmente elaborato dalla dottrina tedesca e poi entrato nell'ordinamento eurounitario, nella sua accezione più ampia comporta che il legislatore e l'Amministrazione pubblica non possano imporre obblighi e/o restrizioni ai diritti e alle libertà dei privati sanciti da norme eurounitarie in misura superiore a quanto strettamente necessario per il raggiungimento dello scopo prefissato dall'autorità nazionale (26).

Nella sua formulazione più "pura", invece, il principio di proporzionalità consta di tre requisiti, o "sotto-principi" (c.d. "teoria dei tre gradini"), che devono essere integrati affinché una misura possa dirsi rispettosa di tale principio: la "idoneità", la "necessarietà" e l'"adeguatezza" (o "proporzionalità in senso stretto") (27)-(28).

---

(26) Sulle origini del principio v., per tutti, A. SANDULLI, *La proporzionalità dell'azione amministrativa*, Padova, 1998 e D. U. GALETTA, *Principio di proporzionalità e sindacato giurisdizionale nel diritto amministrativo*, Milano, 1998. Sul principio di proporzionalità, nella dottrina tributaria, v. — oltre agli autori che saranno richiamati *infra* — le opere monografiche di G. MOSCHETTI, *Il principio di proporzionalità come "giusta misura" del potere nel diritto tributario*, Milano, 2017; PETRILLO, *Il principio di proporzionalità nell'azione di accertamento tributario*, Roma, 2015; MONDINI, *Contributo allo studio del principio di proporzionalità nel sistema dell'Iva europea*, cit.

(27) V. A. SANDULLI, voce *Proporzionalità*, in CASSESE (diretto da), *Dizionario di diritto pubblico*, vol. V, Milano, 2006, 4645-4646: "Il concetto giuridico di proporzionalità può definirsi, per certi versi, uno e trino, nel senso che, pur essendo scomponibile in tre elementi costitutivi (l'idoneità, le necessità, l'adeguatezza), questi non sono scindibili tra loro, ma soltanto distinguibili. [...] Questi tre elementi costituiscono i passaggi logici sequenziali attraverso cui deve articolarsi il controllo di proporzionalità". Sul punto v. anche la cristallina ricostruzione operata da BODRITO, *Note in tema di proporzionalità e Statuto del contribuente*, in BODRITO, CONTRINO, MARCHESELLI (a cura di), *Consensus, equità e imparzialità nello Statuto del contribuente*, Torino, 2012, 286-287.

(28) Il modello di sindacato "a tre gradini" proposto dalla dottrina tedesca non sembrerebbe aver mai trovato piena accoglienza nella giurisprudenza dei

Il requisito della “idoneità” richiede di valutare se il mezzo in concreto utilizzato sia suscettibile di conseguire il risultato perseguito; il requisito della “necessarietà” richiede di scegliere, tra i diversi mezzi idonei al raggiungimento dello scopo perseguito, quello che comporta il minimo sacrificio degli interessi confliggenti (*rectius*, dei principi eurounitari); il requisito della “adeguatezza” (o della “proporzionalità in senso stretto”) richiede, infine, una comparazione (o “bilanciamento”) tra l’interesse pubblico, da un lato, e le posizioni individuali, dall’altro, in modo che la misura — pur se “idonea” e “necessaria” — non sia tale da gravare in maniera eccessiva sull’interessato (29).

Se questo è il quadro, gli obblighi imposti all’Agenzia di “raccolgere opinioni” esterne sul funzionamento dell’applica-

---

giudici UE. Con limitate eccezioni, infatti (cfr. Corte di Giustizia 11 luglio 1989, in C-265/87), il sindacato di proporzionalità compiuto dai giudici UE si limita, per lo più, a un sindacato “bifasico” incentrato sulla verifica dei requisiti dell’“idoneità” e della “necessarietà”, oppure avviene alterando la sequenza di applicazione dei suoi elementi costitutivi (v. D.U. GALETTA, *Il principio di proporzionalità*, in M.A. SANDULLI (a cura di), *Codice dell’azione amministrativa*, Milano, 2017, 169 ss.). Nel prosieguo si farà, tuttavia, riferimento anche al requisito dell’“adeguatezza” (o “proporzionalità in senso stretto”). Invero, nel valutare la compatibilità con il principio di proporzionalità di misure di diritto interno limitative del diritto di detrazione, la Corte di Giustizia, in alcune sentenze, sembrerebbe valorizzare la necessità di compiere una valutazione comparativa e multipolare dei vantaggi e degli svantaggi prodotti da tali misure e per l’effetto dare rilievo — pur non menzionandolo espressamente — al requisito dell’“adeguatezza”. La Corte di Giustizia ha, per esempio, stabilito che: (i) i limiti al diritto di rimborso dei crediti Iva devono essere tali da non far incorrere il soggetto passivo in “rischi finanziari” (CGUE, 12 maggio 2011, causa C-107/10, par. 22 e 23); (ii) al contribuente deve sempre essere consentito di ottenere un controllo giurisdizionale “effettivo” sulla legittimità delle misure che pongono tali limiti (CGUE, 18 dicembre 1997, cause riunite C-286/94, C-340/95, C-401/95 e C-47/96, par. 55) e (iii) il rimborso deve, in ogni caso, essere erogato entro “termini ragionevoli” (cfr. CGUE, 10 luglio 2008, causa C-25/07, par. 17).

(29) Per applicazioni nella giurisprudenza nazionale di tale sindacato “trifasico”, cfr., per tutte, Cons. di Stato, sez. VI, 8 febbraio 2008, n. 424 e Cons. di Stato, sez. VI, 1 aprile 2000, n. 1885, con nota di D.U. GALETTA, *Una sentenza storica sul principio di proporzionalità con talune ombre in ordine al rinvio pregiudiziale alla Corte di giustizia*, in *Riv. It. Dir. Pubbl. Comp.*, 2000, 459.

tivo e di “pubblicare un estratto della valutazione di impatto” (con eccezione degli “allegati” e delle “parti che potrebbero compromettere la sicurezza dei trattamenti”) sembrano precisamente volti a salvaguardare la proporzionalità delle misure di segretezza apprestate dal MEF e dall’Agenzia con riguardo alle regole tecniche di Ve.R.A. Segnatamente, posto che la segretezza delle informazioni riguardanti l’applicativo è senz’altro misura “idonea” e “necessaria” ad evitare che i contribuenti possano eluderne la sorveglianza, sfruttando tecniche di “ingegneria inversa”, gli accorgimenti in esame sono finalizzati a consentire il rispetto del “sotto-principio” della “adeguatezza”.

Invero, se rapportati a questo sotto-principio, i tre accorgimenti tecnici imposti dal Garante sembrano ineccepibili, soprattutto se si considera che gli strumenti algoritmici non sono, per opinione comune, strumenti infallibili.

### 3.2. *Il diritto di non essere sottoposti a decisioni fondate su trattamenti esclusivamente automatizzati.*

Il secondo accorgimento tecnico imposto dal Garante all’Agenzia è quello di “formare adeguatamente il personale a vario titolo coinvolto” nell’utilizzo di Ve.R.A.

Questo accorgimento tecnico è volto a salvaguardare il “diritto di non essere sottoposti a decisioni fondate su trattamenti esclusivamente automatizzati” — rinvenibile nell’art. 22 del Regolamento GDPR (e anch’esso derogabile ai sensi del successivo art. 23 se la deroga è “proporzionata” rispetto allo scopo di contrastare l’evasione) — secondo cui nell’ambito di un processo decisionale automatizzato, deve sempre esistere un intervento umano capace di controllare, validare ovvero smentire la decisione resa dalla macchina (c.d. “human in the loop”)

Invero, nonostante il decreto ministeriale recante le regole tecniche di Ve.R.A., così come la stessa valutazione d’impatto sottoposta al Garante dall’Agenzia, prevedano, molto chiara-

mente, che “nei processi di formazione dei dataset di analisi e di controllo è sempre garantito l’intervento umano”, il Garante ha ritenuto che, qualora i soggetti incaricati di interpretare le risultanze di Ve.R.A. non dovessero possedere comprovate competenze nella gestione, nell’analisi e nel monitoraggio di sistemi algoritmici, essi potrebbero “ritenere più prudente non opporsi alle risultanze del sistema, così vanificando la garanzia connessa alla necessità dell’intervento umano nel processo decisionale” (30).

Tuttavia, come accennato all’inizio, resta concreto il rischio che nel prossimo futuro il legislatore possa autorizzare recuperi d’imposta “totalmente automatizzati”.

Avvisaglie in tale senso sono già rinvenibili in un recente atto di indirizzo del MEF (31), ove è stata avanzata la proposta di introdurre “una disposizione volta a prevedere che talune tipologie di «comunicazioni cambia-verso» possano essere titolo idoneo per la riscossione degli importi evasi in caso di inerzia del contribuente a seguito della notifica”. E ciò — si legge ancora nella richiamata relazione — per far fronte, da un lato, “all’aumento esponenziale” delle posizioni “fiscalmente rischiose” che l’A.F. sarà in grado di rilevare grazie all’impiego e allo sviluppo “di metodologie di analisi del rischio sempre più sofisticate” e, dall’altro, alle limitate “capacità operative dell’Agenzia delle Entrate” (e — si soggiunge — della Guardia di Finanza).

Ora, se il legislatore accoglierà la proposta, è verosimile che, per far fronte alle rilevate carenze, il nuovo applicativo Ve.R.A. possa essere impiegato per l’invio di lettere di compliance non accompagnate da un intervento umano a valle

---

(30) Cfr. Provv. Garante per la protezione dei dati personali, 30 luglio 2022, n. 276, cit.

(31) Cfr. MEF, Relazione per orientare le azioni del Governo volte a ridurre l’evasione fiscale derivante da omessa fatturazione. Allegato della proposta di decisione di esecuzione del Consiglio relativa all’approvazione del Piano per la ripresa e la resilienza dell’Italia, 20 dicembre 2021, 36-38.

della decisione algoritmica e, così, eventualmente, per determinare recuperi d'imposta automatizzati.

Il quesito che va risolto (32) è, dunque, se la normativa in tema di protezione dei dati personali possa prevenire un simile, indesiderabile impiego di Ve.R.A.

La risposta al quesito sembra positiva alla luce, ancora una volta, del principio di proporzionalità.

E infatti, seguendo la già ricordata “teoria” dei tre gradini, sembra possibile sostenere che un'eventuale deroga al principio di non esclusività della decisione algoritmica (*rectius*, al “diritto di non essere sottoposti a una decisione basata unicamente sul trattamento automatizzato”) violerebbe il “requisito” o “sotto-principio” dell’“idoneità”, e ciò per almeno una coppia di ragioni.

La prima è che i sistemi algoritmici non sono infallibili, potendo risentire di errori o distorsioni di diversa natura (cc.dd. *bias*) (33); onde l'esclusione dell'intervento umano ben potrebbe condurre a decisioni fallaci e facilmente censurabili dai contribuenti in sede di giudizio (con tutte le conseguenze pregiudizievoli che deriverebbero in capo all'A.F. in termini di spendio di risorse e di eventuale pagamento delle spese processuali).

La seconda ragione è che il perseguimento dell'interesse cui tende l'accertamento, ossia la contribuzione del consociato in ragione della propria capacità contributiva, non è sempre e per ciò stesso facile, venendo non di rado in rilievo fatti di difficile apprezzamento, che implicano giudizi complessi non delegabili ad una macchina, specialmente laddove essi involgano componenti soggettive, elementi di novità, mutamenti di

---

(32) Ma non senza constatare che nell'epoca dell'intelligenza artificiale “troppi dati rischiano di essere come nessun dato”, con l'ulteriore, paradossale rischio di “impantanare gli uffici in una sorta di paralisi da analisi”: così, efficacemente, R. LUPI, *Diritto amministrativo dei tributi*, Roma, 2017, 309.

(33) Come confermano alcune esperienze concrete di impiego di sistemi di intelligenza artificiale, soprattutto all'estero, su cui v. C. FRANCIOSO, *op. cit.*, 73-74.

convincimenti (34) o la necessità di valutare informazioni non conoscibili dall'Amministrazione (35) - (36).

3.3. *Verifiche sulla qualità dei modelli di analisi, tecniche di pseudonimizzazione dei dati e altre misure di sicurezza per l'elaborazione dei dati.*

Da ultimo, il Garante ha imposto all'Agenzia di adottare efficaci processi di verifica della qualità dei modelli di analisi impiegati, tecniche di pseudonimizzazione dei dati, misure di sicurezza per l'elaborazione dei dati relativi alla fatturazione elettronica e processi di verifica della qualità dei modelli di analisi impiegati, documentando adeguatamente, in rapporti periodici, le metriche utilizzate, le attività svolte, le eventuali criticità riscontrate, le misure e le tecniche di sicurezza in concreto adottate.

Questi accorgimenti rispondono all'esigenza di salvaguardare i principi generali fissati dagli articoli 5 e 6 del Regolamento GDPR, tra cui, in particolare, i principi di "minimizzazione", "limitazione della conservazione" e di "integrità e riservatezza" dei dati. Invero, Ve.R.A. tratterà ed elaborerà dati riferibili alla totalità dei contribuenti e, pertanto, è fondamentale che le tecniche e misure di sicurezza di futura implementazione siano in grado di mascherare, in modo par-

---

(34) Cfr. A. GUIDARA, *Accertamento dei tributi e intelligenza artificiale: prime riflessioni per una visione di sistema*, in *Dir. prat. trib.*, 2023, 384 ss.

(35) Cfr. S. DORIGO, *Opportunità e limiti nell'impiego dell'intelligenza artificiale da parte del Fisco*, in *Corr. trib.*, 2022, 965 ss.

(36) Inoltre, se il legislatore dovesse davvero decidere di accogliere la proposta del MEF di assimilare le "lettere di compliance" agli "avvisi bonari" — per far fronte, da un lato, "all'aumento esponenziale" delle posizioni "fiscalmente rischiose" che l'A.F. sarà in grado di rilevare grazie all'impiego di Ve.R.A. e, dall'altro, alle limitate "capacità operative dell'Agenzia delle Entrate" — la limitazione del "diritto a non essere sottoposti a decisioni unicamente automatizzate", scolpito nell'art. 22 del Regolamento, non rispetterebbe, a rigore, nemmeno il "sotto-principio" della "necessarietà".

ticularmente efficace, l'identità delle persone fisiche e di prevenire fughe di dati in caso di accessi abusivi ai sistemi informatici dell'A.F.

Le indicazioni fornite dal Garante in merito alla pseudonimizzazione dei dati e alle altre misure di sicurezza per l'elaborazione dei dati mediante Ve.R.A. non possono essere esaminate in maniera compiuta, in quanto risultano caratterizzate da un elevato grado di tecnicismo informatico. Al riguardo, ci si limita ad osservare che, secondo quanto risulta dalle fonti ufficiali di riferimento, l'Agenzia delle Entrate ha dichiarato che (tra i numerosi accorgimenti adottati): (i) applicherà in modo sistematico tecniche di pseudonimizzazione (37), finalizzate ad impedire “la reidentificazione massiva” dei contribuenti e, segnatamente, “che, tramite l'incrocio tra più variabili non identificate incluse nel dataset di analisi e la banca dati originale, sia possibile ricostruire con una singola operazione tutti i codici fiscali originali (o un numero significativo di essi)” (38); (ii) nella definizione dei modelli di analisi

---

(37) Si rammenta che i processi di pseudonimizzazione [v. art. 4, par. 1, punto 5), del Regolamento GDPR] offrono un tipo di tutela concettualmente diversa rispetto a quella perseguita dai processi di “anonimizzazione”. La pseudonimizzazione consiste, infatti, nel sostituire un attributo di un dato con un altro. Questo accorgimento rende più complessa l'identificazione, richiedendo una “chiave” per risalire a ritroso alla persona cui si riferisce il dato. Conseguentemente, l'associazione biunivoca tra dato e persona non è modificata in alcun modo e il dato pseudonimizzato, una volta impiegato in combinazione con tutti i mezzi necessari per effettuare la sostituzione di attributi a ritroso, resta inequivocabilmente riferibile alla persona. La pseudonimizzazione, dunque, è volta, da un lato, a garantire la confidenzialità dei dati e, dall'altro, come avviene in caso di applicazione di tecniche crittografiche, a garantire l'integrità contro manipolazioni accidentali. Per contro, nel caso di anonimizzazione, la tutela è volta ad impedire, in modo assoluto, la riferibilità di un dato a una persona. Su tema, v. L. TEMPESTINI, G. D'ACQUISTO, *Il dato personale oggi tra le sfide dell'anonimizzazione e le tutele rafforzate dai dati sensibili*, in G. BUSIA, L. LIGUORI, O. POLLICINO (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali. Bilanci e prospettive*, Roma, 2016, 85-91 e S. CALZOLAIO, *Protezione dei dati personali (dir. pubbl.)*, in *Digesto Disc. Pubbl.*, agg. 2017.

(38) Nel Provvedimento n. 276/2022, il Garante ha valutato positivamente taluni accorgimenti (i) di tipo organizzativo (le attività di creazione di dataset di

non saranno utilizzati i dati c.d. “particolari” (art. 9 del Regolamento GDPR), come, ad esempio, quelli riferiti allo stato di salute, all’orientamento sessuale, all’origine etnica, agli orientamenti politici e religiosi (etc.); inoltre non potrà essere in ogni caso utilizzato il dato relativo allo Stato di nascita del contribuente; (iii) nell’adozione di modelli di analisi stocastici-probabilistici (ad esempio, la classificazione di un soggetto come “rischioso” o “non rischioso” in base agli esiti di pregresse attività istruttorie o di accertamento effettuate nei confronti di altri soggetti) saranno utilizzate “solo informazioni storiche relative a processi che hanno esaurito il proprio ciclo di vista amministrativo” ed escluse, dunque, le informazioni ritraibili da atti di accertamento non ancora definitivi o da processi verbali di constatazione; (iv) per assicurare la trasparenza dell’attività di analisi del rischio e delle tecniche di profilazione utilizzate, sarà pubblicata sul sito istituzionale dell’Agenzia delle Entrate — e periodicamente aggiornata — un’apposita nota informativa sulla logica utilizzata dagli algoritmi, nonché sulle banche dati utilizzate nell’analisi di rischio; (v) non sono contemplati trattamenti completamente automatizzati e ciascuna fase del processo di analisi del rischio prevede l’intervento di uno o più operatori.

---

analisi saranno curate da personale differente dagli analisti coinvolti nelle attività di identificazione dei criteri di rischio e di applicazione dei modelli di analisi, mentre le attività di pseudonimizzazione saranno curate da Sogei S.p.A., che dovrebbe essere la sola a conoscere il metodo di associazione che consente di risalire a ritroso agli originali codici fiscali dei contribuenti) e (ii) di tipo tecnico (gli identificativi pseudonimi saranno dotati di una validità temporale limitata per garantire, anche nel tempo, che le informazioni presenti nei diversi dataset non siano attribuiti a una persona fisica identificata o identificabile). Tuttavia, il medesimo ha Garante ha anche prospettato taluni possibili scenari di rischio che potrebbero emergere nell’ambito dei trattamenti “in considerazione della presenza nei dataset di numerose informazioni che, nonostante l’eliminazione dei dati anagrafici e del codice fiscale e l’adozione di tecniche di perturbazione dei dati, continuano ad avere un elevato potere identificativo”.

#### 4. *Considerazioni conclusive.*

Alla luce di quanto osservato nei precedenti paragrafi, è possibile concludere che la normativa in materia di protezione dei dati personali costituisce un importante baluardo a presidio, anche nell'ambito dei procedimenti tributari, dei principi di "trasparenza", di "non esclusività della decisione algoritmica" e di "non discriminazione".

Inoltre, essa dovrebbe consentire di limitare (o, comunque, regolare) l'utilizzo di strumenti di intelligenza artificiale nella fase di selezione dei contribuenti da sottoporre a controllo, e ciò ancorché, ragionando secondo gli schemi del diritto tributario, quella di "selezione" sia un'attività priva di rilevanza esterna e, come tale, non sindacabile dal giudice.

Nonostante, come detto all'inizio, non sembri ancora attuale il rischio che l'Amministrazione finanziaria sia in grado di realizzare un "panopticum digitale", resta sullo sfondo la rilevante questione — che implica riflessioni di carattere non esclusivamente giuridico (39) — se, alla luce degli straordinari e repentini sviluppi tecnologici cui abbiamo assistito nell'ultimo ventennio, sia opportuno promuovere, a livello normativo, un utilizzo "a tutto campo" di tecniche sempre più avanzate di intelligenza artificiale o di tecniche (dal nome sinistramente onomatopeico) di "*data scraping*" volte a rastrellare informazioni dei cittadini sul web. E ciò soprattutto in considerazione del fatto che, come testimoniano alcuni recenti casi di cronaca (soprattutto in tema di riconoscimento facciale), mentre gli Stati discutono attorno alle modalità di utilizzo di simili tecniche, le multinazionali del settore decidono di autolimitarne lo sviluppo e la commercializzazione.

In altri termini, l'impressione è che, seguendo un approccio "machiaavellico" nell'adozione di nuove tecnologie, e con-

---

(39) Cfr., per tutti, M. HILDEBRANDT, S. GUTWIRTH (a cura di), *Profiling the European Citizen*, Springer, 2010.

sentendo a taluni soggetti privati di assumere un ruolo “quasi-pubblicistico” nella dinamica regolatrice, gli Stati possano favorire un “processo di privatizzazione” di importanti diritti fondamentali, la cui tutela dovrebbe, viceversa, essere il ruolo primario dei legislatori nazionali (40)-(41).

---

(40) V., per riflessioni in questo senso, M. BASSINI, *Fundamental Rights and Private Enforcement in the Digital Age*, in *European Law Journal*, 2019, 182-197.

(41) E ciò, a maggior ragione, se si considera che l'esistenza di strumenti di sorveglianza particolarmente sofisticati per la tutela di interessi pubblici è possibile solo perché, nell'ultimo decennio, ci siamo tutti adeguati — più o meno consapevolmente, senza probabilmente avvertirne tutti i possibili sviluppi (v. D.LYON, *op. ult. cit.*) — ad uno “stile di vita” ben distante dalla massima manzoniana “non sempre ciò che viene dopo è progresso” e che ci pone, come afferma la sociologa statunitense S. ZUBOFF, *The Age of Surveillance*, Londra, 2019, 11, su un fiume di dati raccolti “su di noi ma non per noi”.

