Rivista Telematica di
Diritto Tributario
Pacini Giuridica

Sulla responsabilità dell'Amministrazione finanziaria come «titolare del trattamento» in caso di *data breach* per «attacco *hacker*» di terzi: profili critici e sistematici (*)

On the responsibility of the Financial Administration as "data controller" in the event of a data breach due to a "hacker attack" by third parties: critical and systematic profiles

(commento a/*notes to* CGUE, 14 dicembre 2023, *VB c. Natsionalna agentsia za prihodite*, c. 340/21)

di Filippo Castagnari - 7 novembre 2024

Abstract
La CGUE affronta nuovamente il delicato tema dell'applicazione delle norme contenute nel GDPR a tutela della persona fisica (contribuente) in caso di divulgazione non autorizzata dei propri dati personali, a séguito di un attacco informatico nei confronti dei *databases* dell'Amministrazione finanziaria ("AF"), da parte di soggetti esterni ("terzi") all'AF. I giudici europei concentrano l'attenzione su tre profili di particolare interesse: anzitutto, la verifica e la valutazione di quali elementi integrino la responsabilità dell'AF quale titolare del trattamento dei dati personali del contribuente e, in particolare, se la clausola di esonero da responsabilità sia validamente invocabile sulla scorta dell'avvenuta divulgazione dei dati personali da parte di terzi e non di dipendenti dell'AF. Successivamente, se si configuri un'ipotesi di risarcibilità del danno immateriale sofferto dal contribuente a séguito del *data breach* occorso ai sistemi informatici dell'AF e segnatamente consistente nel timore di un potenziale utilizzo abusivo dei dati personali da parte di terzi. In ultima istanza, a quali parametri e in conformità a quali criteri debba informarsi il ruolo del giudice chiamato a decidere sulla responsabilità dell'AF e sulla risarcibilità, da parte dell'AF e in favore del contribuente, del danno immateriale anzidetto.
Parole chiave: GDPR, violazione dei dati personali dei contribuenti, responsabilità dell'AF come titolare del trattamento, danno immateriale, proporzionalità

Abstract
By the judgment at hand, the ECJ is concerned with the critical analysis of the application of the relevant rules enshrined in the GDPR aimed at safeguarding the natural person (taxpayer) in the case of unauthorised disclosure of his personal data

(*) Il saggio è stato sottoposto a *double blind peer review* con valutazione positiva. Esso confluirà nel fascicolo n. 2/2024 (semestrale) della *Rivista telematica di diritto tributario*.

because of hacking into domestic Tax Authority («TA») databases by third parties. In this regard, the ECJ pointed out a three-tailored approach to the evaluation of such an issue: firstly, by verifying and assessing what elements would be suitable to make TA liable as controller of the processing of taxpayers' personal data for compensation in favour of taxpayers who claim suffering damage from a data breach occurred by third parties against TA databases, and, above all, whether the latter fact may be enough to consider TA exempt from such a liability. Secondly, whether the requirements for compensation by TA of a non-material damage aligned with the risk of an abusive use of taxpayers' personal data by third unauthorised parties are met in the case of the afore-mentioned data breach. Last but not least, the ECJ scrutinised what parameters as well as criteria should be taken into account by judges when such a suit is brought before domestic courts by taxpayers who claim having suffered a non-material damage and, therefore, is demanded TA to be pronounced liable for data breach.
Keywords: *GDPR, taxpayers' personal data breach, TA liability as controller, non-material damage, proportionality*

SOMMARIO: 1. *Data breach* di terzi nei sistemi informatici tributari. La materialità dei fatti di causa nel procedimento principale. - **2.** Il primo *cluster* di questioni pregiudiziali. Assenza di un profilo di responsabilità oggettiva dell'AF per inadeguatezza del *cyber risk management system* adottato e ripartizione dell'onere della prova. – **3.** Responsabilità dell'AF quale "titolare del trattamento" e risarcibilità del danno per utilizzo abusivo, da parte dei terzi, dei dati personali del contribuente illecitamente divulgati. - **4.** Osservazioni conclusive. La "proporzionalità" delle misure tecniche ed organizzative adottate dal "titolare del trattamento" come metro di giudizio nella valutazione della clausola di esonero da responsabilità dell'AF

1. La sentenza in commento riporta al centro dell'attenzione della CGUE il complesso tema della concreta assoggettabilità dell'AF ai principi e regole stabiliti dal Reg. UE 2016/679 del 27 aprile 2016 (di séguito, "GDPR"), nella misura in cui tale Autorità pubblica "processi" dati personali dei contribuenti in funzione strumentale all'esercizio dell'attività di accertamento e controllo (cfr. CONTRINO A., *Banche dati, scambio di informazioni fra autorità fiscali e "protezione dei dati personali": quali diritti e tutele per il contribuente?*, in *Riv. tel. dir. trib.*, 2019, 1, 7 ss.; CONTRINO A. - RONCO S.M., *Prime riflessioni e spunti in materia 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, 3, 599 ss.; WÖHRER V., WÖHRER V., *Data Protection and Taxpayers' Rights: Challenges Created by Automatic Exchange of Information*, Amsterdam, 2018).
Di qui, la domanda di pronuncia pregiudiziale (cfr. CGUE, c. 340/21, *VB c. Natsionalna agentsia za prihodite*, ECLI:EU:C:2023:986, parr. 1 e 2; di séguito "la

sentenza") s'incentra sull'interpretazione degli artt. 5, par. 2, 24, 32, e 82, parr. 1-3, GDPR e trae origine da una controversia tra "*VB*" (persona fisica ricorrente nel procedimento principale; di séguito, "la ricorrente"), e la *Natsionalna agentsia za prihodite* (Agenzia per le entrate pubbliche, in Bulgaria; di séguito, "NAP") in merito al risarcimento del danno immateriale che la ricorrente sostiene di aver subìto a causa di una presunta violazione da parte della NAP dei suoi obblighi legali in qualità di "titolare del trattamento"[1] dei "dati personali"[2].

Piú in dettaglio, dai fatti di causa (cfr. par. 10 ss. della sentenza) emerge che tra i compiti istituzionali della NAP si annoverano la raccolta, la conservazione, il trattamento e l'analisi di dati personali dei contribuenti, al fine della identificazione e salvaguardia del recupero dei crediti fiscali. Il 15 luglio 2019 i *media* hanno rivelato al pubblico l'avvenuto accesso non autorizzato al sistema informatico della NAP da parti di "terzi"[3] ("attacco *hacker*"), e, a séguito di tale *data breach*, taluni dati personali (di interesse e natura economico-finanziaria, nonché tributaria di piú di sei milioni di persone fisiche, di nazionalità bulgara o straniera) contenuti in detto sistema sono stati illecitamente sottratti e pubblicati su *Internet*.

Ciò posto, la ricorrente ha adito l'*Administrativen sad Sofia-grad* (Tribunale amministrativo della città di Sofia, Bulgaria) citando in giudizio la NAP e sostenendo di aver subìto un danno immateriale (cfr. par. 13 della sentenza) derivante, in particolare, da una "violazione di dati personali"[4] causata da una condotta negligente perpetrata dalla NAP e non conforme agli obblighi imposti su di essa *ex* art. 5, par. 1, lett. *f*, nonché dagli artt. 24 e 32, GDPR.

1 Ai sensi dell'art. 4, par. 1, n. 2, GDPR si considera "trattamento" qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione. Di conseguenza, è "titolare del trattamento" la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (cfr. art. 4, par. 1, n. 7, GDPR).

2 Con tale espressione, l'art. 4, par. 1, n. 1, GDPR qualifica «*qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o piú elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*».

3 Con tale terminologia, riferendosi al contesto definitorio intessuto dal GDPR, si suole riferirsi a la/e persona/e fisica/che o giuridica/che, l'Autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'Autorità diretta del titolare o del responsabile (cfr. art. 4, par. 1, n. 10, GDPR).

4 Ai sensi dell'art. 4, par. 1, n. 12, GDPR, tale è la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Diversamente argomentando, la NAP appuntava le sue difese facendo leva su due profili principali (cfr. par. 14 della sentenza): *in primis*, la NAP ha prodotto in giudizio documenti volti a dimostrare di aver adottato tutte le misure tecniche ed organizzative necessarie, a monte, per prevenire la violazione dei dati personali contenuti nel suo sistema informatico nonché, a valle, per limitare gli effetti di tale violazione e per rassicurare i cittadini, ottemperando al disposto dell'art. 32, parr. 1 e 2, GDPR. *In secundis*, secondo la NAP, non si rilevavano elementi atti a dimostrare l'esistenza del nesso di causalità tra il danno immateriale lamentato e il *data breach* subìto (*ex* art. 82, par. 3, GDPR), giacché quest'ultimo risultava in conseguenza di un danno doloso causato alla NAP stessa da parte di "terzi" non soggetti al suo diretto controllo, e, quindi, essa non può ritenersi responsabile delle relative conseguenze dannose.
L'*Administrativen sad Sofia-grad* accoglie i motivi sollevati dalla NAP (cfr. par. 15 della sentenza) e, di conseguenza, la ricorrente propone ricorso per cassazione avverso detta decisione dinanzi al *Varhoven administrativen sad* (Corte Suprema amministrativa, Bulgaria), lamentando l'errore di diritto commesso dal giudice di primo grado nella ripartizione dell'onere della prova relativo alle misure di sicurezza adottate dalla NAP e che quest'ultima non abbia parimenti dimostrato la sua assenza di inerzia al riguardo. Inoltre, la ricorrente sostiene che il timore di possibili utilizzi abusivi dei suoi dati personali nel futuro costituisce un danno immateriale attuale, e non ipotetico (cfr. par. 16 della sentenza).
Il giudice di legittimità, in qualità di organo giudicante di ultima istanza ed in conformità all'art. 267, par. 3, TFUE, ha ritenuto necessario un pronunciamento pregiudiziale della CGUE in ordine all'autentica interpretazione delle norme del GDPR applicabili al caso di specie, rimettendole, quindi, il caso.

2. Il giudice remittente richiede alla CGUE, in via principale, se gli artt. 24 e 32, GDPR debbano essere interpretati nel senso che una divulgazione o un accesso non autorizzati ai dati personali, da parte di soggetti non dipendenti della NAP, e, pertanto, non riferibili in modo alcuno al suo controllo, sia sufficiente per ritenere che le misure tecniche e organizzative adottate non siano adeguate (cfr. par. 21, p.to n. 1 e par. 22 della sentenza).
In subordine a ciò (cfr. par. 21, p.ti nn. 2 e 3 della sentenza), e solo in caso di risposta negativa all'anzidetta questione, il giudice remittente domanda quale debba essere l'oggetto e la portata del controllo giurisdizionale di legittimità nell'esame dell'adeguatezza delle misure tecniche e organizzative adottate dal titolare del trattamento e, in particolare, se incomba su quest'ultimo l'onere di provare l'effettiva e concreta adeguatezza di siffatte misure.
La *ratio decidendi* avallata dalla CGUE parte dalla ricognizione degli obblighi che l'art. 5, § 1, lett. *f* e § 2, GDPR[5] impone sul titolare del trattamento. Dapprima, si sancisce l'obbligo di trattare i dati personali in maniera da garantirne un'adeguata sicurezza e protezione, mediante misure tecniche e organizzative adeguate, da

5 Cfr., in tal senso, il disposto del considerando n. 83, GDPR.

trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (c.d. "integrità e riservatezza dei dati personali", come rilevato da RENNA M., *Sicurezza e gestione del rischio nel trattamento dei dati personali*, in *Resp. civ. prev.*, 2020, 4, 1343 ss. e ID., *Violazione dei dati personali, sicurezza del trattamento e protezione dai rischi*, in *Dir. mercato ass. fin.*, 2020, 2, 197 ss.; FEDI A., *Commercial Law and Corporate Aspects of Personal Data Protection*, in *Riv. dir. impresa*, 2018, 3, 741 ss.). Di conseguenza, il titolare del trattamento è responsabile dell'osservanza dei principi anzidetti e su costui incombe l'onere di dimostrare in concreto l'effettiva adozione delle misure tecniche e organizzative idonee a garantire l'integrità e la sicurezza dei dati personali trattati (c.d. "responsabilizzazione [*i.e.* "*accountability*"] del titolare del trattamento", come osservato da VANEGAS J.S., *La violazione dei requisiti di sicurezza informatica di cui all'articolo 32 del GDPR*, in *Riv. it. inf. dir.*, 2020, 2, 5 ss.).

Ciò posto, l'"integrità e riservatezza dei dati personali" sono definiti negli artt. 24 e 32, GDPR, facendo emergere la necessità di una lettura a ciclo combinato delle rispettive disposizioni. Difatti, l'art. 24, par. 1, GDPR prevede un obbligo generale, gravante sul titolare del trattamento, di attuare misure tecniche e organizzative adeguate a garantire che detto trattamento sia effettuato conformemente a principi e regola stabilite dal GDPR (cfr. par. 25 della sentenza), e di poterlo dimostrare (cfr. par. 32 della sentenza). Mentre, il successivo art. 32, par. 2, GDPR dispone che, nel valutare l'adeguato livello di sicurezza (cfr. par. 32 della sentenza), debbano considerarsi quei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso non autorizzato, in modo accidentale o illegale, a dati personali.

Nel caso di specie, in capo alla NAP si pone, quindi, l'obbligo di predisporre a monte, e di attuare in concreto a valle, l'adozione di un sistema di analisi, valutazione e gestione del rischio connesso al trattamento dei dati personali dei contribuenti, mediante il ricorso a misure tecniche e organizzative verificabili e dimostrabili. Siffatto *cyber risk management system* (MAGUIRE M. - STUTTARD N. - A. MORRIS A. - HARVEY E., *A Review of Behavioural Research on Data Security*, in *Eur. J. Priv. Law & Techn.*, 2018, 1, 16 ss.; PIVA D., *Cybersecurity e corporate governance tra valutazioni top-down e tecniche bottom-up*, in *Corp. Gov.*, 2022, 4, 525 ss.) risulterebbe funzionale a far sí che il titolare del trattamento appresti un sistema di gestione del rischio che abbia come obiettivo il raggiungimento di un "livello di sicurezza adeguato al rischio" (*ex* art. 32, parr. 1 e 2, GDPR), senza che ciò implichi, tra le sue finalità, la necessaria eliminazione dei rischi di violazione dei dati personali (cfr. par. 29 della sentenza).

Di conseguenza, la CGUE ritiene che non sia identificabile un profilo di responsabilità oggettiva della NAP, dato che gli artt. 24 e 32, GDPR non debbono essere intesi nel senso che una divulgazione non autorizzata di dati personali o un accesso non autorizzato a tali dati da parte di un terzo siano sufficienti per concludere che le misure adottate dal titolare del trattamento (la NAP) non fossero

appropriate, ai sensi di tali disposizioni, senza neppure consentire a quest'ultimo di fornire la prova contraria (cfr. par. 30 della sentenza).
Il percorso argomentativo tracciato dalla CGUE è, quindi, volto a definire il contenuto e l'oggetto del giudizio di adeguatezza delle misure tecniche ed organizzative adottate dal titolare del trattamento. Si precisa, pertanto, che un siffatto esame richiede al giudice remittente di procedere ad un'analisi *case-by-case* della natura e del contenuto di tali misure, del modo in cui queste sono state applicate e dei loro effetti pratici sul livello di sicurezza che il titolare del trattamento è tenuto a garantire, considerati i rischi inerenti a tale trattamento (cfr. par. 42 della sentenza).
Con riferimento, invece, alla ripartizione dell'onere della prova – tra la ricorrente e la NAP – circa la concreta ed effettiva attuazione da parte del titolare del trattamento delle misure tecniche ed organizzative anzidette, la CGUE ritiene che dal combinato disposto degli artt. 5, par. 2, 24, par. 1, e 32, par. 1, GDPR risulti «[…] *senza ambiguità che l'onere di provare che i dati personali sono trattati in modo tale da garantire una loro adeguata sicurezza incomba al titolare del trattamento in parola*» (cfr. par. 52 della sentenza e, per analogia, CGUE, c. 60/22, *Bundesrepublik Deutschland*, EU:C:2023:373, parr. 52 e 53, e CGUE, c. 252/21, *Meta Platforms et al.*, EU:C:2023:537, par. 95).
Del resto, se si dovesse ritenere che l'onere della prova riguardo all'adeguatezza di dette misure gravi sulla ricorrente, ne conseguirebbe che il diritto al risarcimento previsto *ex* art. 82, par. 1, GDPR risulterebbe potenzialmente compromesso nella sua concreta esperibilità. Difatti, poiché il "livello di protezione" garantito dal GDPR dipende dalle misure di sicurezza adottate dai titolari del trattamento, è dunque ragionevole che quest'ultimi siano chiamati, sopportando l'onere di dimostrare l'adeguatezza di tali misure, a fare tutto il possibile per prevenire operazioni di trattamento non conformi a tale regolamento (cfr. parr. 55-56 della sentenza)[6].

3. Partendo dalle considerazioni di cui sopra, la CGUE si confronta con il secondo ordine di questioni pregiudiziali sollevate dal giudice remittente, e segnatamente coincidente nella valutazione dell'astratta configurabilità, in capo alla ricorrente, di un danno risarcibile a séguito della divulgazione non autorizzata dei propri dati personali. Difatti, l'art. l'art. 82, par. 2, GDPR, che pone in capo al titolare del trattamento l'obbligazione al risarcimento del danno cagionato da tale attività, qualora realizzata in violazione delle disposizioni del regolamento stesso (cfr. TOSI E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale. Oggettivazione del rischio e riemersione del danno morale con funzione deterrente-sanzionatoria alla luce dell'art. 82, GDPR*, Milano, 2019; BRAVO F., *Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali*, in ZORZI GALGANON., a cura di, *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019 e ZENO-ZENCOVICH V.,

6 Il *dictum* giudiziale espresso dalla CGUE pare allinearsi con un'interpretazione delle disposizioni del GDPR atte a conferire piena attuazione al disposto dei considerando nn. 74 e 76, GDPR.

ZENO-ZENCOVICH V., *Liability for Data Loss*, in V. MAK, E. TJONG TJIN TAI e A. BERLEE (a cura di), *Research Handbook in Data Science and Law*, Cheltenham, 2018).

Tale regime di responsabilità codifica l'insorgenza di un'obbligazione *ex lege* in capo al titolare del trattamento (cfr. IORIO C., IORIO C., *Legal Issues Concerning the Circulation and Processing of Data in the Digital Age*, in *Eur. J. Priv. Law & Techn.*, 2022, 2, 153 ss.; ZECCHIN F., *Molteplicità delle fonti e tutela dei diritti. Il danno non patrimoniale nella lesione della proprietà e dei dati personali*, in *Eur. dir. priv.*, 2022, 3, 517 ss.; SERRAVALLE S., *Il danno da trattamento dei dati personali nel GDPR*, Napoli, 2020; CATERINA R. - THOBANI S., *Il diritto al risarcimento dei danni*, in CATERINA R., a cura di, *GDPR tra novità e discontinuità*, in *Giur. it.*, 2019, 12, 2805 ss.; VIVARELLI A., *Il consenso al trattamento dei dati personali nell'era digitale. Sfide tecnologiche e soluzioni giuridiche*, Napoli, 2019), da ricondursi al regime delle c.dd. «*variae causarum figurae*»[7] e con ciò ammettendosi, in caso di violazioni commesse da quest'ultimo, la configurabilità di un'ipotesi di responsabilità per inadempimento di obbligazioni (*ex* art. 1218 c.c.).

In generale, la CGUE rileva che l'art. 82, par. 2, GDPR impone un'interpretazione secondo cui, da un lato, il titolare del trattamento è chiamato a risarcire un danno causato da una violazione del GDPR connessa a tale trattamento e, dall'altro, costui può essere esonerato da siffatta responsabilità solo provando la non imputabilità a sé del fatto che ha provocato tale danno (art. 82, par. 3, GDPR, su cui cfr. par. 70 della sentenza).

In riferimento al caso di specie, è acclarato che l'evento generatore del *data breach* è stato commesso da criminali informatici, cioè da "terzi" rispetto alla NAP. La CGUE puntualizza (cfr. par. 74 della sentenza), tuttavia, che la NAP non può essere esonerata dall'obbligo di risarcire il danno subìto dalla ricorrente per il solo fatto che tale danno deriva da una divulgazione non autorizzata di dati personali o da un accesso non autorizzato a tali dati da parte di "terzi", dato che si richiede, allora, la dimostrazione *per tabulas* che il fatto che ha provocato il danno in questione non sia in alcun modo imputabile alla NAP.

Pertanto, nell'inquadramento dei profili determinativi dell'esistenza di un danno potenzialmente sofferto dal contribuente-persona fisica, l'art. 82, par. 1, GDPR radica un approccio multilivello alla risarcibilità di questo da parte della NAP, basato su tre condizioni cumulative (cfr. par. 72 della sentenza e, recentemente, CGUE, c. 300/21, *Österreichische Post*, EU:C:2023:370, par. 32): l'esistenza di un danno subìto, materiale o immateriale, dalla ricorrente; l'esistenza di una violazione delle disposizioni del GDPR da parte della NAP; la rilevazione di un nesso di causalità tra tale danno e tale violazione. È doveroso puntualizzare, in ogni caso, che la CGUE individua nell'art. 82, GDPR una funzione non punitiva, bensí compensativa, contrariamente a quanto disposto dagli artt. 83 e 84, GDPR, che svolgono, dal canto loro, una finalità sostanzialmente punitiva, dato che consentono

7 Ai sensi dell'art. 1173 c.c. le obbligazioni derivano, tra le altre ipotesi, anche «[…] *da ogni altro atto o fatto idoneo a produrle in conformità dell'ordinamento giuridico*».

di infliggere, rispettivamente, sanzioni amministrative pecuniarie ed altre sanzioni (cfr. CGUE, c. 687/21, *BL c. MediaMarktSaturn Hagen-Iserlohn GmbH*, ECLI:EU:C:2024:72, par. 47, e CGUE, c. 667/21, *Krankenversicherung Nordrhein*, ECLI:EU:C:2023:1022, par. 85).
Nel caso di specie, la ricorrente lamentava di aver subìto un danno immateriale consistente nel timore di un potenziale utilizzo abusivo dei suoi dati personali da parte di terzi, a séguito del *data breach* occorso ai sistemi informatici della NAP. Il "danno immateriale" sofferto dalla ricorrente è, quindi, collegato a un utilizzo abusivo da parte di terzi dei suoi dati personali che si è già prodotto, alla data della sua domanda di risarcimento, oppure, e su un piano di parità effettuale, è collegato alla paura percepita da tale persona che un siffatto utilizzo possa prodursi in futuro (cfr. par. 79 della sentenza). Di conseguenza, conclude la CGUE, l'art. 82, par. 1, GDPR può ricomprendere, tra le ipotesi di risarcibilità del danno immateriale, il timore paventato dalla ricorrente di un potenziale utilizzo abusivo dei propri dati personali illecitamente sottratti da parte di terzi, purché il giudice nazionale verifichi in concreto, sulla base degli elementi addotti dalla parte e in relazione alle circostanze del caso, che tale "timore" sia effettivamente fondato (cfr. parr. 13, 84-86 della sentenza).

4. Le considerazioni espresse dalla CGUE consentono di mettere in luce, per quanto di rilievo ai fini tributari, la configurabilità in capo all'AF della qualifica di titolare del trattamento qualora quest'ultima organizzi, gestisca e impieghi nell'esercizio dell'"azione impositiva" (cfr. CALIFANO C., *La motivazione degli atti impositivi*, Torino, 2012) *datasets* informativi ove confluiscano dati fiscali rilevanti (e sensibili) trasmessi dalla massa dei contribuenti e/o da intermediari qualificati, a tal fine conservati, analizzati e processati.
Di conseguenza, alla considerazione dell'AF quale titolare del trattamento dei dati fiscali dei contribuenti, si allinea, in conformità con il dato interpretativo sostenuto dalla CGUE, il correlato regime di responsabilità derivante da violazioni nei propri sistemi informatici, con conseguente sottrazione e divulgazione non autorizzata da parte di terzi dei suddetti dati personali (fiscali) dei contribuenti. Del resto, nel contesto delle pur ammesse "limitazioni" al sistema di protezione dei dati personali degli interessati[8], qualora un'"Autorità pubblica" (tra cui certamente è ricompresa l'AF) persegua «*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*» (art. 23, par. 1, n. 5, GDPR), non si annoverano quelle disposizioni disciplinanti il regime di responsabilità del titolare del trattamento.
Pertanto, si afferma anche in riferimento alla funzione di controllo da parte dell'AF, e dei relativi strumenti applicativi, la centralità della tutela del trattamento dei dati personali di fronte ad esigenze prettamente pubblicistiche. Ciò, a ben vedere, «*non può che passare dal principio di "proporzionalità": vi deve sempre essere "proporzionalità" fra trattamento del dato alla luce dell'obiettivo perseguito ed*

8 V. *supra* nota n. 2.

esigenza di minimizzare l'acquisizione, il trattamento e la conservazione dei dati personali dei contribuenti» (cfr. similmente, PAPARELLA F., *Procedimento tributario, algoritmi e intelligenza artificiale: potenzialità e rischi della rivoluzione digitale*, in CONTRINO A. - MARELLO E., a cura di, *La digitalizzazione dell'amministrazione finanziaria tra contrasto all'evasione e tutela dei diritti del contribuente*, vol. II, Milano, 2023; PITRUZZELLA G., *Dati fiscali e diritti fondamentali*, in *Dir. prat. trib. int.*, 2022, 2, 666 ss.; FARRI F., *Digitalizzazione dell'Amministrazione finanziaria e diritti dei contribuenti*, in *Riv. dir. trib.*, 2020, 6, 115 ss.).

Piú in dettaglio, è il giudizio di proporzionalità ed effettività delle misure adottate dal titolare o responsabile[9] del trattamento che, anzitutto, pone in evidenza la nuova rilevanza della protezione dei dati personali in materia fiscale e «*fa sorgere la questione dei limiti che il relativo diritto pone all'acquisizione, al trattamento e alla conservazione dei suddetti dati da parte dell'AF*» (cfr. CONTRINO A. - RONCO S.M., cit.; in ciò ricomprendendosi, altresí, il diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento, garantito dall'art. 79, par. 1, GDPR, su cui si v. par. 63 della sentenza e, parimenti, CGUE, c. 132/21, *Nemzeti Adatvédelmi és Információszabadság Hatóság*, ECLI:EU:C:2023:2, par. 50; CGUE, c. 175/20, "*SS*" *SIA c. Valsts ieņēmumu dienests*, ECLI:EU:C:2022:124, par. 83; CGUE, c. 741/21, *GP v. juris GmbH*, ECLI:EU:C:2024:288, par. 51, e CGUE, c. 293/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238, parr. 60-61). Ed è parimenti tale giudizio di proporzionalità ed effettività ad indirizzare il necessario bilanciamento con l'adozione di strumenti e mezzi sempre piú efficienti ed interconnessi a disposizione delle AF degli Stati membri, per far sí di costituire *datasets* informativi completi ed integrati, al fine di intercettare con maggior tempestività ed efficienza potenziali operazioni di significativa rischiosità fiscale.

Quanto poc'anzi espresso produce un significativo impatto, in via di primo approccio, con riferimento tanto alla disciplina dello scambio di informazioni fiscali tra AF degli Stati membri, quanto alle problematiche di natura formale e sostanziale che il reperimento legittimo del dato fiscale e la parimenti legittima condivisione dello stesso da parte dell'"AF destinataria della richiesta" all'"AF richiedente" comporta (cfr. SAPONARO F., *L'attuazione amministrativa del tributo nel diritto dell'integrazione europea*, Milano, 2017; MARINO G., *Beyond the Automatic Exchange of Information: DAC 6, Its Strengths and Its Achilles Heels*, in *Riv. dir. trib. int.*, 2020, 1/3, 203 ss; JACKSON G. - BROWN H., *The Role of Context in Interpreting International Tax Instruments: A Solution to the Erosion of Internal Cohesion of Domestic Tax Systems by International Directive on Administrative Cooperation Version 6 (DAC6) - A Case Study*, in *Bull. int. tax.*, 2022, 2; MONTANARI F., *Gli obblighi di comunicazione in capo agli intermediari ed al contribuente*, in CORDEIRO GUERRA R. - DORIGO S. - VIOTTO A. (a cura di),

9 Con "*responsabile del trattamento*", s'intende «*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*» (art. 4, par. 1, n. 8, GDPR).

L'attuazione della DAC 6 nell'ordinamento italiano. Profili teorici e prospettive future, Torino, 2023).

Appellandosi ancora all'anzidetto principio di proporzionalità, pare condivisibile l'approccio sostenuto in dottrina (CONTRINO A., *Digitalizzazione dell'amministrazione finanziaria e attuazione del rapporto tributario: questioni aperte e ipotesi di lavoro nella prospettiva dei princìpi generali*, in *Riv. dir. trib.*, 2023, 2, I, 105 ss) e volto ad attribuire centralità – oltre alla disciplina e regolamentazione della raccolta e conservazione, a monte, dei dati fiscali dei contribuenti da parte dell'AF – anche alla chiara individuazione di presidi di garanzia sostanziali e procedimentali in capo al contribuente i cui dati fiscali richiedono di essere processati ragionevolmente e proporzionalmente rispetto agli obiettivi e finalità della funzione di accertamento e controllo (preservando, del pari, il diritto alla riservatezza del contribuente in relazione alle potenziali illegittime intrusioni nella vita privata).

Ciò posto, la CGUE conferma e rafforza il principio interpretativo secondo cui l'integrazione dei requisiti previsti dalla clausola di esonero dalla responsabilità di cui all'art. 82, par. 3, GDPR non può ragionevolmente verificarsi *a priori* in sede legislativa. Tale attività interpretativa invoca un'analisi del caso di specie, conseguente a una ponderazione critica e proporzionata degli elementi sostanziali della fattispecie concreta. A Siffatta attività corrisponde un ruolo attivo da parte del giudice adito, volto a valutare quali misure tecniche e organizzative sono state realizzate e, soprattutto, se tali misure possano considerarsi proporzionali ed effettivamente idonee (cfr. par. 60 della sentenza; similmente, cfr. CGUE, c. 817/19, *Ligue des droits humains*, ECLI:EU:C:2022:491, par. 297, e CGUE, c. 300/21, *Österreichische Post*, ECLI:EU:C:2023:370, par. 54) ad escludere la configurabilità di una responsabilità in capo all'AF per *data breach* di terzi.

BIBLIOGRAFIA ESSENZIALE

BESHKARDANA K., *Reversing the Irreversible: Mitigating Legal Risks of Blockchain-Based Data Breach through Corporate Governance*, in *Hastings Sc. & Techn. Law J.*, 2023, 1, 175 ss.

BILOTTA F., *La responsabilità civile nel trattamento dei dati personali*, in PANETTA R. (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Milano, 2019

BRAVO F., *Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali*, in ZORZI GALGANON. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019

BUCCICO C., *Il principio di proporzionalità*, in CARINCI A. - TASSANI T. (a cura di), *I diritti del contribuente. Principi, tutele e modelli di difesa*, Milano, 2022

CALIFANO C., *La motivazione degli atti impositivi*, Torino, 2012

CARINCI A., *Il sistema multilivello dei diritti del contribuente, tra pluralità di fonti e molteplicità dei modelli di tutela*, in CARINCI A. - TASSANI T. (a cura di), *I diritti del contribuente. Principi, tutele e modelli di difesa*, Milano, 2022
CATERINA R. – THOBANI S., *Il diritto al risarcimento dei danni*, in CATERINA R. (a cura di), *GDPR tra novità e discontinuità*, in *Giur. it.*, 2019, 12, 2805 ss.
CONTRINO A. - RONCO S.M., *Prime riflessioni e spunti in materia 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, 3, 599 ss.
CONTRINO A., *Banche dati, scambio di informazioni fra autorità fiscali e "protezione dei dati personali": quali diritti e tutele per il contribuente?*, in *Riv. tel. dir. trib.*, 2019, 1, 7 ss.
CONTRINO A., *Digitalizzazione dei poteri tributari e tutela dei diritti dei contribuenti: osservazioni generali sulle problematiche e sulle prospettive come introduzione al progetto di ricerca PRIN 2020*, in CARPENTIERI L. - CONTE D. (a cura di), *La digitalizzazione dell'amministrazione finanziaria tra contrasto all'evasione e tutela dei diritti del contribuente*, vol. I, Milano, 2023
CONTRINO A., *Digitalizzazione dell'amministrazione finanziaria e attuazione del rapporto tributario: questioni aperte e ipotesi di lavoro nella prospettiva dei princìpi generali*, in *Riv. dir. trib.*, 2023, 2, I, 105 ss.
CONTRINO A., *Protezione dei dati personali e pervasività delle banche dati fiscali: quale contemperamento?*, in CONTRINO A. - MARELLO E. (a cura di), *La digitalizzazione dell'amministrazione finanziaria tra contrasto all'evasione e tutela dei diritti del contribuente*, vol. II, Milano, 2023
CONTRINO A., *Spinte evolutive (sul piano sovranazionale) e involutive (a livello interno) in tema di bilanciamento fra diritto alla protezione dei dati dei contribuenti ed esigenze di contrasto all'evasione fiscale*, in *Riv. tel. dir. trib.*, 2023, 2, 533 ss.
DEL FEDERICO L., *Tutela del contribuente ed integrazione giuridica europea*, Milano, 2010
FARRI F., *Digitalizzazione dell'Amministrazione finanziaria e diritti dei contribuenti*, in *Riv. dir. trib.*, 2020, 6, 115 ss.
FEDI A., *Commercial Law and Corporate Aspects of Personal Data Protection*, in *Riv. dir. impresa*, 2018, 3, 741 ss.
GRAETZ M.J. – WARREN A.C., *Income Tax Discrimination and the Political and Economic Integration of Europe*, in *Riv. dir. trib. int.*, 2007, 1, 1186 ss.
HADWICK D., *Behind the One-Way Mirror: Reviewing the Legality of EU Tax Algorithmic Governance*, in *EC Tax Rev.*, 2022, 4, 184 ss.
IORIO C., *Legal Issues Concerning the Circulation and Processing of Data in the Digital Age*, in *Eur. J. Priv. Law & Techn.*, 2022, 2, 153 ss.
JACKSON G. - BROWN H., *The Role of Context in Interpreting International Tax Instruments: A Solution to the Erosion of Internal Cohesion of Domestic Tax Systems by International Directive on Administrative Cooperation Version 6 (DAC6) – A Case Study*, in *Bull. int. tax.*, 2022, 2

LASINSKI-SULECKI K., *Legal Certainty in Tax and Customs Judgments of the Court of Justice*, in *EC Tax Rev.*, 2024, 2, 68 ss.
MAGUIRE M. - STUTTARD N. - MORRIS A. - HARVEY E., *A Review of Behavioural Research on Data Security*, in *Eur. J. Priv. Law & Techn.*, 2018, 1, 16 ss.
MÄIHÄNIEMI B. - SCHÜTTE B., *Damages Liability Regimes for Unfair Data Gathering in the EU*, in *Concorrenza & Mercato*, 2023, 29, 133 ss.
MAJORANA D., *Evoluzione dello scambio delle informazioni: principio di proporzionalità, tutela del contribuente e diritto al contraddittorio*, in *Dir. prat. trib. int.*, 2020, 3, 993 ss.
MANZO V. - BERGAMO M., *From Information Privacy to Emergency Privacy*, in *Eur. J. Priv. Law & Techn.*, 2020, 1, 83 ss.
MARCHESELLI A. - RONCO S.M., *Dati personali, Regolamento GDPR e indagini dell'Amministrazione finanziaria: un modello moderno di tutela dei diritti fondamentali*, in *Riv. dir. trib.*, 2022, 2, I, 97 ss.
MARINO G., *Beyond the Automatic Exchange of Information: DAC 6, Its Strengths and Its Achilles Heels*, in *Riv. dir. trib. int.*, 2020, 1/3, 203 ss.
MERCURI G., *Spunti ricostruttivi in tema di Dac-6: pianificazione fiscale aggressiva, ragionevolezza e profili sanzionatori*, in *Riv. dir. fin.*, 2021, 2, I, 247 ss.
MONTANARI F., *Gli obblighi di comunicazione in capo agli intermediari ed al contribuente*, in CORDEIRO GUERRA R. - DORIGO S. - VIOTTO A. (a cura di), *L'attuazione della DAC 6 nell'ordinamento italiano. Profili teorici e prospettive future*, Torino, 2023
ORTOLEVA M.G., *The Employment of AI by the Italian Tax Administration to Fight Tax Relief Abuse: The Difficult Balance Between Public Interest and Taxpayer Rights*, in *Dir. proc. trib.*, 2022, 3, 351 ss.
PAGALLO U. - CASANOVAS P. - MADELIN R., *The Middle-out Approach: Assessing Models of Legal Governance in Data Protection, Artificial Intelligence, and the Web of Data*, in *Theory & Pract. Leg.*, 2019, 1, 1 ss.
PAPARELLA F., *Procedimento tributario, algoritmi e intelligenza artificiale: potenzialità e rischi della rivoluzione digitale*, in CONTRINO A. - MARELLO E. (a cura di), *La digitalizzazione dell'amministrazione finanziaria tra contrasto all'evasione e tutela dei diritti del contribuente*, vol. II, Milano, 2023
PERRONE A. - SELICATO G., *L'Attività istruttoria*, in DEL FEDERICO L. - PAPARELLA F. (a cura di), *Diritto tributario digitale*, Pisa, 2023
PITRUZZELLA G., *Dati fiscali e diritti fondamentali*, in *Dir. prat. trib. int.*, 2022, 2, 666 ss.
PIVA D., *Cybersecurity e corporate governance tra valutazioni top-down e tecniche bottom-up*, in *Corp. Gov.*, 2022, 4, 525 ss.
PURPURA A., *Protection of Taxpayers' Personal Data and National Tax Interest: A Misstep by the European Court of Human Rights?*, in *Intertax*, 2021, 12, 1044 ss.
RENNA M., *Sicurezza e gestione del rischio nel trattamento dei dati personali*, in *Resp. civ. prev.*, 2020, 4, 1343 ss.

RENNA M., *Violazione dei dati personali, sicurezza del trattamento e protezione dai rischi*, in *Dir. mercato ass. fin.*, 2020, 2, 197 ss.
SAPONARO F., *L'attuazione amministrativa del tributo nel diritto dell'integrazione europea*, Milano, 2017
SAPONARO F., *Lo scambio di informazioni tra amministrazioni finanziarie e l'armonizzazione fiscale*, in *Rass. trib.*, 2005, 2, 453 ss.
SCARCELLA L., *The Implications of Adopting a European Central Bank Digital Currency: A Tax Policy Perspective*, in *EC Tax Rev.*, 2021, 4, 177 ss.
SERRANO ANTÓN F., *Artificial Intelligence and Tax Administration: Strategy, Applications and Implications, with Special Reference to the Tax Inspection Procedure*, in *World Tax J.*, 2021, 4, 575 ss.
SERRAVALLE S., *Il danno da trattamento dei dati personali nel GDPR*, Napoli, 2020
TOMO A., *Tax Information, Third Parties and GDPR: Legal Challenges and Hints from the Court of Justice*, in *EC Tax Rev.*, 2023, 4, 144 ss.
TOSI E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale. Oggettivazione del rischio e riemersione del danno morale con funzione deterrente-sanzionatoria alla luce dell'art. 82, GDPR*, Milano, 2019
VANEGAS J.S., *La violazione dei requisiti di sicurezza informatica di cui all'articolo 32 del GDPR*, in *Riv. it. inf. dir.*, 2020, 2, 5 ss.
VIVARELLI A., *Il consenso al trattamento dei dati personali nell'era digitale. Sfide tecnologiche e soluzioni giuridiche*, Napoli, 2019
WÖHRER V., *Data Protection and Taxpayers' Rights: Challenges Created by Automatic Exchange of Information*, Amsterdam, 2018
ZECCHIN F., *Molteplicità delle fonti e tutela dei diritti. Il danno non patrimoniale nella lesione della proprietà e dei dati personali*, in *Eur. dir. priv.*, 2022, 3, 517 ss.
ZENO-ZENCOVICH V., *Liability for Data Loss*, in MAK V. - TJONG TJIN TAI E. - BERLEE A. (a cura di), *Research Handbook in Data Science and Law*, Cheltenham, 2018