Numero registro generale 20281/2024
Numero sezionale 3011/2025
Numero di raccolta generale 27558/2025
Data pubblicazione 15/10/2025

REPUBBLICA ITALIANA

LA CORTE SUPREMA DI CASSAZIONE

PRIMA SEZIONE CIVILE

Oggetto:
TRATTAMENTO DATI PERSONALI
Ud.11/09/2025 CC

Composta dagli Ill.mi Sigg.ri Magistrati:

LAURA TRICOMI	Presidente
GIULIA IOFRIDA	Consigliere
ALESSANDRA DAL MORO	Consigliere
MAURA CAPRIOLI	Consigliere
RITA ELVIRA A. RUSSO	Consigliere Rel.

ha pronunciato la seguente

ORDINANZA

sul ricorso iscritto al n. 20281/2024 R.G. proposto da:
GARANTE PROTEZIONE DATI PERSONALI, in persona del legale rappresentante pro tempore, elettivamente domiciliato in ROMA VIA DEI PORTOGHESI 12, presso l'AVVOCATURA GENERALE DELLO STATO (ADS80224030587) che lo rappresenta e difende

-ricorrente-

contro

PROVINCIA AUTONOMA DI BOLZANO, in persona del Presidente pro tempore rappresentato e difeso dall'avvocato [redacted] unitamente agli avvocati [redacted]

-controricorrente-

avverso la SENTENZA del TRIBUNALE BOLZANO n. 368/2024 depositata il 21/06/2024.
Udita la relazione svolta nella camera di consiglio del 11/09/2025 dal Consigliere RITA ELVIRA A. RUSSO.

FATTI DI CAUSA

In data 21 aprile 2021 l'Azienda Sanitaria della Provincia Autonoma di Bolzano ha trasmesso all'Autorità Garante per la protezione dei dati personali (ai sensi dell'art. 33 del Regolamento (UE) 2016/679) una notifica di violazione dei dati personali, riguardante l'accesso non autorizzato ai documenti sanitari di alcuni assistiti determinato dalla vulnerabilità del servizio relativo al Fascicolo sanitario elettronico (in acronimo, FSE).

L'Azienda indicava quali responsabili del trattamento dei dati personali la società [redacted] s.p.a. [redacted] -designata quale responsabile del trattamento nel 2010- e [redacted] s.p.a. -designata anch'essa responsabile del trattamento nel 2018- nell'ambito del contratto stipulato con [redacted] s.p.a. per conto dell'Azienda Sanitaria della Provincia Autonoma di Bolzano per la fornitura delle componenti software dell'attuale piattaforma per la realizzazione del FSE.

Si evidenziava così una vulnerabilità applicativa del software fornito da [redacted] poiché attraverso l'applicativo [redacted] portale ufficiale della pubblica amministrazione dell'Alto Adige, l'utente, pur dovendosi autenticare tramite SPID, poteva immettere successivamente codici fiscali di altri cittadini e accedere ai loro fascicoli.

Con nota dell'1.03.2022 (doc. 10) il Garante ha notificato la violazione di cui agli artt. 166, comma 5, del Codice e 58, par. 1, lett. d), del Regolamento UE alla Provincia autonoma di Bolzano ritenendola titolare del trattamento di dati personali correlato al *data breach*.

La Provincia autonoma di Bolzano ha quindi proposto opposizione sostenendo che le finalità e i mezzi del trattamento

svolto mediante la piattaforma impiegata per la realizzazione del FSE fossero stati determinati dall'Azienda sanitaria- con affidamento dell'esecuzione tecnica a fornitori del settore [redacted] – alla quale quindi si sarebbe dovuta imputare la titolarità e dunque la responsabilità del trattamento.

Il Tribunale di Bolzano ha accolto l'opposizione ritenendo che titolare del trattamento fosse l'Azienda Sanitaria e non la Provincia, rilevando che nel provvedimento il soggetto sanzionato era individuato come «Amministrazione provinciale», ritenuta una «espressione oscura» e ritenendo: a) che i compiti che il Regolamento (UE) citato assegna al titolare del trattamento si rispecchiano nei compiti e nei poteri assegnati all'Azienda Sanitaria dell'Alto Adige ricavabili, in primis, dal piano di progetto e in particolare a pag. 30, Modulo E – voce "Sicurezza e privacy", cui si rimanda (doc. 16 di parte opponente), nonché dall'Atto di nomina di Responsabile esterno del Trattamento dei dati della azienda Società [redacted] s.p.a. dd. 11.5.2010 (doc. 18 di parte opponente) e la delibera della Giunta Provinciale n. 949 dd. 18.9.2018 (doc. 22 di parte opponente) avente per oggetto la "Realizzazione del Fascicolo sanitario elettronico (FSE) in Alto Adige", cui integralmente si rimanda; b) che l'Azienda sanitaria dell'alto Adige (ASDAA), in qualità di titolare ha individuato quale responsabile del trattamento (esternalizzando questi compiti) le imprese che hanno fornito il software; c) che il provvedimento opposto risulta illegittimo per carenza di motivazione se considerato singolarmente e per motivazione contraddittoria se confrontato ad altro provvedimento sanzionatorio scaturito dal medesimo fatto, ove a soggetti diversi – ovvero all'opponente nel primo caso e all'Azienda Sanitaria dell'Alto Adige nell'altro - viene attribuita la medesima qualifica di titolare del trattamento,

che può essere rivestita da un unico soggetto, integrando pertanto vizio dell'atto riconducibile all'eccesso di potere.

Avverso la predetta sentenza ha proposto ricorso per cassazione l'Autorità Garante per la protezione dei dati personali, affidandosi a un motivo. La Provincia ha svolto difese con controricorso. Entrambe le parti hanno depositato memoria.

RAGIONI DELLA DECISIONE

1.- Con il primo e unico motivo del ricorso si lamenta la violazione e falsa applicazione di norma di diritto ex art. 360 n. 3 c.p.c., con riferimento ai criteri di individuazione della figura del titolare del trattamento in base alle disposizioni degli artt. 4, n.7) e 5, 25, 32 e 33 del Regolamento (UE) 2016/679. L'Avvocatura dello Stato deduce che sulla base del Regolamento (UE) 2016/679 il titolare del trattamento dei dati personali non è il soggetto che materialmente tratta detti dati, bensì il soggetto che determina le finalità e i mezzi del trattamento, essendo titolare del potere decisionale in materia. Rileva che l'art. 4 del Regolamento n. 2016/679/UE (*General Data Protection Regulation*, in acronimo GDPR) definisce il titolare del trattamento dei dati personali al punto 7, nei termini che seguono: «*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 degli Stati membri*»; definisce quindi al punto 8 il «*responsabile del trattamento*» nei seguenti termini: «*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro*

organismo che tratta dati personali per conto del titolare del trattamento».

Titolare e responsabile sono dunque due soggetti diversi con diversi compiti e funzioni ma entrambi hanno delle responsabilità (art. 82) perché il titolare del trattamento dei dati personali risponde direttamente per le proprie scelte in materia di trattamento dei dati personali, mentre i soggetti che abbiano ricevuto istruzioni dal titolare rispondono solo se abbiano agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento. Si deduce quindi che l'attribuzione ad un soggetto diverso di compiti propri del titolare del trattamento dei dati personali non comporta affatto, come ha ritenuto il Tribunale di Bolzano, il venir meno della qualità di titolare del trattamento dei dati personali e l'attribuzione di tale qualità al soggetto che ha ricevuto l'attribuzione di tali compiti, in quanto il titolare resta comunque l'unico soggetto a disporre del potere decisionale sulla materia ed a fornire le istruzioni sull'operato del responsabile. Lamenta l'errore del Tribunale che nell'individuare la Azienda come titolare ha falsamente applicato le disposizioni degli artt. 4, n. 7) e 5, 25, 32 e 33 del Regolamento.

La titolarità dei trattamenti effettuati attraverso il FSE è, infatti, espressamente prevista dal quadro normativo di settore (art. 12, D.L. n. 179/2012 e D.P.C.M. n. 178/2015, all'epoca dei fatti vigente, oggi in parte sostituito dal D.M. 7 settembre 2023) Gli artt. 10 e 11 del D.P.C.M. n. 178/2015, all'epoca dei fatti vigente, attribuivano all'Azienda sanitaria solo la titolarità dei trattamenti dei dati e documenti presenti nel FSE effettuati per le finalità di cui all'articolo 12, comma 2, lettera a) del D.L. n. 179/2012 (finalità di cura) e non anche quelli relativi alle procedure di identificazione e autenticazione informatica al FSE.

Nel caso di specie, invece, si tratta dei trattamenti effettuati nelle procedure di identificazione e autenticazione informatica, nonché di autorizzazione all'accesso alle risorse (dati e documenti) di cui è titolare la Provincia. A riprova di ciò rappresenta che nel Regolamento n. 2016/679/UE, che ha in parte abrogato il D.P.C.M. n. 178/2015, la titolarità dei trattamenti necessari a consentire l'identificazione, l'autenticazione informatica e l'accesso ai dati e documenti del FSE da parte dello stesso è in capo alla Regione/Provincia autonoma di assistenza (art. 11, comma 4 del D.M. 7 settembre 2023). Deduce che le attività di trattamento con riferimento alle quali si è verificata la violazione dei dati personali, a seguito della quale è stato adottato il provvedimento oggetto di impugnazione, rientrano nella sfera di titolarità della Provincia autonoma di Bolzano e non anche della Azienda sanitaria. Il *data breach* non risulta, infatti, essere stato determinato da un'errata identificazione dell'assistito al momento dell'erogazione delle prestazioni sanitarie o da una scorretta associazione dei metadati ai documenti sanitari presenti nel FSE.

2.- Il motivo è fondato.

2.1.- In via preliminare è opportuno precisare che al caso in esame si applica, quanto alle definizioni di responsabile del trattamento e titolare del trattamento, il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (GDPR), entrato in vigore il 25 maggio 2018. Nella legislazione nazionale vengono poi in applicazione l'art.12 del D.L. 18 ottobre 2012, n.179, conv. con mod. dalla legge 17 dicembre 2012, n.221, e il DPCM 29 settembre 2015, n.178, recante il Regolamento in materia di fascicolo sanitario elettronico (*ratione temporis* vigenti).

Nelle more è stato approvato anche il nuovo Regolamento UE 2025/237 (*European Healt Data Space*, in acronimo EHDS) entrato in vigore il 26 marzo 2025, (con applicazione prevista a partire dal 26 marzo 2027) che conferma le definizioni di titolare del trattamento e responsabile del trattamento già date dal GDPR. Per quanto qui di interesse può rilevarsi che il nuovo Regolamento UE persegue tre finalità sinteticamente esposte nel primo considerando: in primo luogo garantire l'uso primario dei dati sanitari migliorando l'accesso delle persone fisiche ai loro dati sanitari elettronici e il controllo su tali dati, ma anche favorire l'uso secondario dei dati sanitari per la realizzazione dell'interesse collettivo a fini di ricerca, innovazione, prevenzione e risposta alle minacce sanitarie, nonché migliorare il funzionamento del mercato interno per quanto riguarda lo sviluppo, la commercializzazione e l'uso di sistemi di cartelle cliniche elettroniche. Queste finalità sono già in certa misura immanenti nella legislazione nazionale in tema di fascicolo sanitario elettronico, ma è evidente che l'esperienza pandemica ha portato a una nuova consapevolezza sulla funzione sociale dei dati sanitari, e sulla necessità di bilanciare il diritto soggettivo alla riservatezza del dato con la necessità di disporre di un accesso tempestivo ai dati sanitari a fini di prevenzione e cura. Da qui l'importanza di individuare correttamente il titolare dei dati sanitari e il responsabile del trattamento, anche in vista dello svolgimento dei compiti che l'EHDS assegna loro, nonché lo sviluppo di sistemi di gestione e di accesso ai dati che ne garantiscano le finalità istituzionali.

2.2-La presente controversia riguarda specificamente la individuazione del titolare del trattamento, essendo pacifico che si è verificato un *data breach* a causa di una specificità vulnerabilità del software che gestiva l'accesso al fascicolo

sanitario elettronico. Pertanto, è infondata la eccezione di inammissibilità del ricorso proposta da parte controricorrente, secondo la quale il ricorso costituirebbe una richiesta di rivalutazione dei fatti di causa. Nel ricorso non si chiede di rivalutare i fatti di causa ma di verificare se è corretta la individuazione del titolare del trattamento dei dati sanitari in base alla normativa europea e alla normativa nazionale interna vigente, considerando che esso va tenuto distinto dal responsabile del trattamento; si tratta quindi, come correttamente espone l'Avvocatura, di una censura per violazione ed erronea applicazione di norme di diritto.

3.- L'istituzione del fascicolo sanitario elettronico trova la sua disciplina nell'art.12 del D.L. 18 ottobre 2012, n.179, conv. con mod. dalla legge 17 dicembre 2012, n.221, e nel D.P.C.M. 29 settembre 2015, n.178, recante il Regolamento in materia di fascicolo sanitario elettronico.

Il fascicolo sanitario elettronico (FSE) è individuale e riguarda il singolo assistito; è costituito dall'insieme dei dati e documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi che riguardano l'assistito, riferiti anche alle prestazioni erogate al di fuori del Servizio sanitario nazionale. Il FSE è istituito dalle Regioni e Province autonome nel rispetto della normativa vigente in materia di protezione dei dati personali, secondo le previsioni di cui all'art.12 cit. e persegue plurime e specifiche finalità, come individuate al comma 2 dello stesso art.12 che nel testo *ratione temporis* vigente così le esplicita: a) prevenzione, diagnosi, cura e riabilitazione; b) studio e ricerca scientifica in campo medico, biomedico ed epidemiologico; c) programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria. I soggetti che possono utilizzare il FSE mutano a seconda della

finalità perseguite, così come mutano la qualità dei dati accessibili per il trattamento e le condizioni per il trattamento.

Le finalità di prevenzione, diagnosi, cura e riabilitazione (lettera a) sono perseguite dai soggetti del Servizio sanitario nazionale e dei servizi socio-sanitari regionali e da tutti gli esercenti le professioni sanitarie che prendono in cura l'assistito secondo le modalità di accesso da parte di ciascuno dei predetti soggetti e da parte degli esercenti le professioni sanitarie, nonché nel rispetto delle misure di sicurezza definite ai sensi del comma 7.

Le finalità di studio e ricerca scientifica in campo medico, biomedico ed epidemiologico (lettera b) e programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria (lettera c) sono perseguite dalle Regioni e dalle Province autonome, nonché dal Ministero del lavoro e delle politiche sociali e dal Ministero della salute nei limiti delle rispettive competenze attribuite dalla legge.

Questa Corte ha già precisato quali sono i limiti per il trattamento «in chiaro» dei dati personali inseriti nel FSE, consentito solo per finalità di prevenzione, diagnosi, cura e riabilitazione dell'assistito stesso (Cass. n.6067 del 06/03/2025).

4.- Ciò premesso, si osserva che la sentenza impugnata, così come censurato dall'Avvocatura dello Stato, non applica correttamente l'art.4 del GDPR per varie ragioni: a)in primo luogo non distingue chiaramente tra titolare del trattamento e responsabile del trattamento; b) non tiene conto di quali sono i soggetti che in base alla normativa interna determinano le finalità e i mezzi del trattamento di dati personali; c)non tiene conto né delle disposizioni del D.L. 179/2012 (art. 12) né del D.P.C.M. 29 settembre 2015, n. 178 (Regolamento in materia di fascicolo sanitario elettronico), che individuano i titolari del

trattamento dati del FSE secondo le funzioni specifiche; d) esamina atti quali il «Piano di Progetto» e l'«Atto di nomina del Responsabile» non esplicitando in motivazione né la loro natura né la loro funzione e per quale ragione essi prevarrebbero -in tesi- su norme di legge e regolamentari.

5.- Il giudice di merito non tiene conto che l'art. 12 del citato D.L. 179/2012, convertito in legge, dispone che il FSE è istituito dalle Regioni e Province autonome, per le finalità di cui sopra si è detto, alcune delle quali pertinenti all'uso primario dei dati, altre all'uso secondario. In relazione a queste finalità è lo stesso art. 12 che individua quali sono i soggetti che le perseguono. Esso infatti prevede infatti che le finalità di cui alla lettera a) del comma 2 (diagnosi cura e riabilitazione) sono perseguite dai soggetti del Servizio sanitario nazionale e dei servizi socio-sanitari regionali e da tutti gli esercenti le professioni sanitarie secondo le modalità di accesso previste e con le relative misure di sicurezza, mentre le finalità di cui alle lettere b) e c) sono perseguite dalle Regioni e dalle Province autonome, nonché dal Ministero del lavoro e delle politiche sociali e dal Ministero della salute nei limiti delle rispettive competenze.

5.1.- Di conseguenza poiché l'art. 4 del GDPR individua il titolare del trattamento nel soggetto che «*singolarmente o insieme ad altri determina le finalità e i mezzi del trattamento di dati personali*», rilievo decisivo ha la circostanza che il FSE è istituito dalle Regioni e dalle Province autonome, nonché l'attribuzione del perseguimento di specifiche finalità a questi enti. Pertanto, in relazione al tipo di *data breach* che nella specie si è consumato, non si può prescindere dalla verifica di chi fosse il soggetto che persegue e determina le finalità e i mezzi del trattamento, nell'ambito del quale l'accesso abusivo si è verificato.

Infine, deve osservarsi che non è di per sé contraddittorio individuare due soggetti da sanzionare posto che lo stesso regolamento UE indica che i titolari del trattamento possono essere anche più soggetti in quanto possono essere più i soggetti che determinano le finalità e i mezzi del trattamento stesso.

Ne consegue, in accoglimento del ricorso la cassazione della sentenza impugnata e il rinvio al Tribunale di Bolzano, in composizione monocratica con magistrato diverso, per un nuovo esame e per la liquidazione delle spese anche del giudizio di legittimità.

P.Q.M.

accoglie il ricorso cassa la sentenza impugnata e rinvia al Tribunale di Bolzano in composizione monocratica con magistrato diverso, per un nuovo esame e per la liquidazione delle spese anche del giudizio di legittimità

Così deciso in Roma, il 11/09/2025.

Il Presidente

LAURA TRICOMI