queste istituzioni

I ruoli privacy e le responsabilità del titolare e del responsabile del trattamento nell'ambito del rapporto tra PA e società *in-house*

Luca Tufarelli
Maria Lilia La Porta
Gaia Leoncini

Numero 4/2023
31 dicembre 2023

I ruoli privacy e le responsabilità del titolare e del responsabile del trattamento nell'ambito del rapporto tra PA e società *in-house*

di Luca Tufarelli[*], Maria Lilia La Porta[#], Gaia Leoncini[§]

Sommario

Sintesi

Per la fornitura e lo svolgimento di alcuni servizi pubblici, tra cui anche quelli relativi al settore IT, le PA si servono sempre più frequentemente dell'*in-house providing*, ossia l'affidamento diretto a società strumento su cui esercitano un controllo diretto.
Nel caso in cui la realizzazione di tali servizi comporti un trattamento di dati personali, si pone il tema della corretta individuazione dei ruoli privacy in uno schema in cui la PA riveste generalmente il ruolo di "titolare del trattamento" determinando le finalità e le modalità del trattamento, mentre la società strumento quello di "responsabile del trattamento" che, nell'ambito dell'*in-house providing*, effettua le attività tecniche necessarie alla gestione dei dati per conto della PA. Da qui la necessità di ben definire i due ruoli per individuare, nell'ambito dell'*in-house providing*, i diversi e possibili profili e gradi di responsabilità che possono essere addebitati al titolare e al responsabile del trattamento, in particolare con riferimento all'obbligo di adozione di misure di sicurezza,organizzative e tecniche,adeguate al rischio connesso al trattamento di cui all'art. 32 del Regolamento UE n. 679/2016 per la protezione dei dati personali (GDPR).

Abstract

In order to supply some public services, including those relating to the IT sector, the public administrations increasingly use in-house providing, i.e. direct entrustment to instrumental companies over which they exercise direct control.
In the event that the implementation of these services involves the processing of personal data, the issue arises of the correct identification of the privacy roles in a scheme in which the PA

[*] Avvocato del Foro di Roma.
[#] Avvocato del Foro di Roma.
[§] Dottoressa in Giurisprudenza.

generally plays the role of "data controller" determining the purposes and methods of the processing, while the company acts as "data controller" who, in the context of in-house providing, carries out the technical activities necessary for data management on behalf of the PA. Hence the need to clearly define the two roles to identify, in the context of in-house providing, the different and possible profiles and degrees of responsibility that can be attributed to the data controller and data processor, in particular with reference to obligation to adopt security, organizational and technical measures, appropriate to the risk associated with the processing referred to in the art. 32 of EU Regulation no. 679/2016 for the protection of personal data (GDPR).

Parole chiave
Tutela della privacy; Responsabile del trattamento; Affidamento *in-house*; Pubblica amministrazione.

1. Premessa: il rapporto *in-house providing*

Le PA si servono spesso di società strumento per la fornitura e lo svolgimento di alcuni servizi, solitamente nei settori di IT, sempre più utili se non necessari nell'ambito della digitalizzazione dei processi delle PA. Il Piano Triennale per l'Informatica nella Pubblica Amministrazione 2022-2024 (PTI) e il Piano Nazionale di Ripresa e Resilienza (PNRR) prevedono tra i principali obiettivi e *milestone* proprio quello di raggiungere una completa digitalizzazione dei processi della PA.

Con l'espressione "*in-house providing*" si fa riferimento al fenomeno di auto-produzione attraverso cui la PA, per l'approvvigionamento di beni e servizi, ricorre a risorse proprie mediante affidamento diretto ad una società di cui detiene il controllo in deroga alle regole in materia di concorrenza. Come più volte chiarito dal Consiglio di Stato (v. Parere 8 novembre 2018, n. 2583[1]) con tale espressione "*si fa riferimento all'affidamento di un appalto o di una concessione da parte di un ente pubblico in favore di una società controllata dall'ente medesimo, senza ricorrere alle procedure di evidenza pubblica, in virtù della peculiare relazione che sussiste tra l'ente pubblico e la società affidataria*". È questa, infatti, la ratio sottesa all'art. 16 del D.lgs. 19 agosto 2016, n. 175 ("Testo Unico in materia di società a partecipazione pubblica"), secondo cui le società *in house*, ossia le società sulle quali un'Amministrazione esercita il "controllo analogo", possono ricevere affidamenti diretti dall'Amministrazione controllante.

Nonostante la distinta personalità giuridica, la società in house, nella sostanza, si trova in rapporto di immedesimazione organica con l'Amministrazione affidante (sul punto *ex multis* Sentenza C.d.S. 26 maggio 2015, n. 2660[2]), essendo equiparabile ad un suo organo o ufficio interno privo di sostanziale autonomia decisionale. In tale contesto, la società *in-house* che ad

[1] *https://www.moltocomuni.it/wp-content/uploads/parere-2583-2018.pdf.*

[2] *https://www.amministrazioneincammino.luiss.it/wp-content/uploads/2016/04/Consiglio-di-Stato-sez.-VI-26-maggio-2015-n.-2660.pdf.*

esempio fornisce servizi IT all'Amministrazione, quali lo sviluppo e la gestione di sistemi informativi dell'Amministrazione stessa o di enti alla stessa collegati, opera quale *longa manus* tecnica della PA nell'ambito delle attività affidatele *ex lege* e contrattualmente, non sussistendo tra detti soggetti, pur formalmente distinti e dotati di autonoma personalità giuridica, alcuna alterità soggettiva.

Pertanto, nell'ambito del trattamento di dati personali, è possibile ritenere che la società *in-house* effettui operazioni di trattamento di dati per conto dell'Amministrazione titolare e debba essere nominata dalla stessa quale responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE n. 679/2016 (d'ora in poi solo GDPR). La questione che di recente ha comportato l'intervento del Giudice nazionale e di quello europeo, come vedremo nelle sentenze in commento nell'ambito del presente contributo, attiene principalmente alla responsabilità che deve essere riconosciuta e ripartita tra titolare e responsabile in materia di trattamento di dati personali, con particolare riferimento all'adozione di misure di sicurezza tecniche ed organizzative adeguate ai sensi dei principi sanciti dall'art. 32 del GDPR.

2. Il contesto normativo di riferimento.

Al fine di individuare i criteri per la corretta qualificazione di un soggetto come titolare e come responsabile del trattamento in ambito pubblico, è necessario analizzare *in primis* le definizioni generali previste nella normativa in materia di protezione dei dati. Anche le "*Linee Guida dell'EDPB n. 07/2020 sui concetti di titolare e responsabile del trattamento ai sensi del GDPR*"[3] forniscono chiarimenti in merito ai ruoli e le responsabilità di titolare e responsabile del trattamento.

Il titolare del trattamento è definito dal GDPR all'art. 4 par. 1 n. 7 come "*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*".

Secondo l'EDPB, elemento fondamentale per la qualifica di titolare è che il soggetto eserciti un'influenza da un punto di vista concreto determinante sulle finalità e sulle modalità del trattamento dei dati personali, in virtù dell'esercizio di un potere decisionale. Il titolare è tale anche se non ha trattato egli stesso dati personali e non risulta la sua qualifica da alcun atto o contratto scritto, purché partecipi in maniera attiva e concreta nella determinazione delle finalità e dei mezzi del trattamento.

Inoltre, il titolare del trattamentoha la piena responsabilità del trattamento in virtù del principio dell'*accountability*[4], e deve garantire la tutela dei diritti e delle libertà degli interessati.

[3] Rintracciabili in *edpb_guidelines_202007_controllerprocessor_final_it.pdf* (europa.eu).

[4] Per accountability si intende la capacità del titolare del trattamento di adottare misure di sicurezza adeguate ai rischi per i diritti e le libertà degli interessati nonché di render conto della corretta applicazione del

Il responsabile del trattamento è, invece, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organo, quindi un soggetto terzo all'organizzazione del titolare, che tratta dati personali per conto e secondo le istruzioni del titolare stesso[5].

L'EDPB ha individuato due condizioni per aversi la qualifica di responsabile del trattamento: (i) che questo sia un soggetto separato rispetto al titolare; (ii) che il trattamento avvenga per conto del titolarestesso. Il responsabile del trattamento persegue le finalità di trattamento definite dal titolare, sulla base delle istruzioni e indicazioni da quest'ultimo fornite. L'elemento che consente di qualificare un soggetto come responsabile è rappresentato quindi dalla strumentalità della sua attività rispetto alle finalità perseguite dal titolare con il trattamento dei dati personali.

L'art. 28 del GDPR definisce i compiti e gli obblighi del responsabile, tra i quali in particolare l'obbligo di collaborazione e trasparenza nei confronti del titolare e l'obbligo di garantire la sicurezza dei dati. Il responsabilea seguito delle informazioni ed istruzioni ricevute dal titolare ha altresì l'obbligo di adottare le misure di sicurezza concordate e la responsabilità che le stesse siano adeguate a garantire la sicurezza del trattamento, secondo le risultanze dell'analisi dei rischi effettuata con il titolare.

Il GDPR prevede che il titolare del trattamento possa fornire per iscritto le istruzioni al responsabile del trattamento riguardo alla gestione dei dati personali, tramite un accordo che rifletta la natura e lo scopo del trattamento e chiarisca gli obblighi in capo ai soggetti. L'accordo sul trattamento può consistere in un atto o contratto scritto, comprensivo di tutti gli elementi previsti dall'art. 28, par. 3 del GDPR[6] e di eventuali ulteriori elementi concordati tra le parti,

---

regolamento. Cfr. art. 24 GDPR e art. 32 i quali affermano che il titolare, insieme al responsabile, deve mettere in atto "*misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*".

[5] Cfr. art. 4 par. 8 e art. 28 del GDPR.

[6] Art. 28, par. 3, GDPR: "*(…) Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento: a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico; b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza; c) adotti tutte le misure richieste ai sensi dell'articolo 32; d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento; e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III; f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento; g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato. Con riguardo alla lettera h) del primo comma, il responsabile del trattamento*

oppure può essere redatto sulla base delle clausole contrattuali tipo, adottate dalla Commissione Europea.[7]

Le Linee Guida dell'EDPB, tra l'altro, confermano che l'accordo sul trattamento tra titolare e responsabile *"dovrebbe disciplinare in modo più specifico e concreto come saranno soddisfatti i requisiti applicabili e quale sia il livello di sicurezza richiesto per il trattamento dei dati personali oggetto dell'accordo stesso*", e andrà redatto sempre in virtù del principio dell'*accountability*, che deve accompagnare e permeare ogni scelta in merito al trattamento dei dati.

In genere nei rapporti tra una PA e una società *in-house* viene stipulato un atto di designazione del responsabile o l'inserimento di una clausola all'interno del contratto tra le parti che preveda nello specifico i relativi compiti e le rispettive responsabilità nell'ambito del trattamento dei dati personali. In quel caso, non si pongono particolari problemi di individuazione dei ruoli e delle rispettive responsabilità.

Tuttavia, può succedere che l'accordo sul trattamento sia del tutto mancante, oppure, seppure esistente, sia incompleto e insufficiente o carente di istruzioni specifiche da parte del titolare, con magari un generico richiamo ad adottare tutte le opportune misure di sicurezza necessarie ad assicurare la tutela dei dati degli interessati ai sensi dell'art. 32 GDPR. È quindi opportuno esaminare i differenti profili di responsabilità del titolare e del responsabile del trattamento.

3. La responsabilità ai sensi degli artt. 82 e 83 del GDPR.

Nel caso in cui il trattamento posto in essere violi le disposizioni del GDPR, sia il titolare che il responsabile del trattamento possono essere ritenuti responsabili, ma i rispettivi gradi di responsabilità possono variare.

Ai sensi dell'art. 82 del GDPR, il titolare del trattamento "*risponde per il danno cagionato dal suo trattamento che violi il presente regolamento*". Qualora la violazione degli obblighi posti dal GDPR sia stata commessa dal titolare stesso che ha agito con dolo o colpa, egli potrà subire una sanzione amministrativa pecuniaria ai sensi dell'art. 83, par. 4 del GDPR[8]. Tale sanzione

---

informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati".

[7] Ai sensi dell'art. 28 par. 7 del GDPR la Commissione Europea può stabilire clausole contrattuali tipo. Cfr. il parere congiunto 1/2021 dell'EDPB sulle clausole contrattuali tipo tra titolari e responsabili del trattamento *https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12021-standard_en.*

[8] Art. 83, par. 4, lett. a): "*In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore: a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43*". Cfr. altresì Sentenza della Corte di Giustizia Europa del 5 dicembre 2023 analizzata nel p. 7, lett. b.

potrà essere inflitta al titolare altresì in relazione a operazioni di trattamento di dati personali effettuate per suo conto da un responsabile del trattamento, in quanto il titolare è responsabile non solo dei trattamenti di dati personali che effettua direttamente, ma anche di quelli che vengono effettuati "per suo conto" dal responsabile[9].

Il responsabile del trattamento, a sua volta, è sanzionabile e risponde per il danno causato dal trattamento nel caso in cui non abbia adempiuto gli obblighi previsti a suo carico dal GDPR ai sensi dell'art. 28 o abbia agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento[10].

Il GDPR non esclude la possibilità che entrambi possano essere ritenuti responsabili, specialmente se le violazioni derivano dalla mancata adozione di adeguate misure di sicurezza tecniche e organizzative. In tal caso saranno responsabili in solido per l'intero ammontare del danno, a meno che uno dei due, o entrambi, non dimostrino che l'evento dannoso non è in alcun modo a loro imputabile. In tal caso, saranno esonerati dalla responsabilità[11].

Il Regolamento non ha stabilito degli importi fissi per ogni violazione, ma ha previsto degli importi massimi, la cui valutazione è rimessa discrezionalmente all'Autorità Garante, che deciderà se e in che misura infliggere la sanzione applicando i criteri generali elencati al par 2 del medesimo art. 83[12].

I profili di responsabilità del titolare e del responsabile possono variare altresì a seconda dell'esistenza o meno di un accordo sul trattamentoche presenti il contenuto di cui all'art. 28, par. 3, del GDPR, oppure se l'accordo, seppur esistente, sia incompleto e non specifici quali siano gli obblighi e le relative responsabilità dei soggetti coinvolti nel trattamento. Da

---

[9] Cfr. Sentenza della Corte di Giustizia Europa del 5 dicembre 2023 analizzata nel p. 7, lett. b.

[10] Si deve sottolineare il termine "legittime", in quanto il responsabile deve in ogni caso verificare che le istruzioni del titolare non siano contrarie al GDPR o alla normativa nazionale vigente. V. p. 3.1.

[11] Cfr. art. 82, par. 3, GDPR.

[12] Art. 83, par. 2: "*Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure. Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi: a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito; b) il carattere doloso o colposo della violazione; c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati; d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32; e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento; f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi; g) le categorie di dati personali interessate dalla violazione; h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione; i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti; j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione*".

considerare poi le questioni economiche legate alla mancata attribuzione al responsabile di risorse economiche adeguate per l'implementazione delle misure di sicurezza ritenute necessarie. Sembra opportuno analizzare le ipotesi principali.

3.1. Esiste l'atto di designazione del responsabile *ex* art. 28 del GDPR con le istruzioni.

Ove sussista tra le parti un accordo sul trattamento nel quale siano contenute le istruzioni fornite dal titolare al responsabile, comprese quelle legate alle misure di sicurezza, e c'è stata una violazione del GDPR, il responsabile risponde del danno causato dal trattamento se abbia agito in violazione delle istruzioni contenute nell'accordo sul trattamento. Inoltre, qualora egli tratti i dati per il perseguimento di finalità proprie o in modo tale che non si possa ragionevolmente ritenere che il titolare abbia a ciò acconsentito, l'Autorità Garante potrà infliggere nei suoi confronti una sanzione pecuniaria amministrativa come se fosse un titolare[13].

Il responsabile è, in ogni caso, esonerato da responsabilità qualora dimostri che l'evento dannoso da cui deriva il danno non è a lui imputabile o di aver adottato tutte le misure adeguate a proteggere i dati ed al fine di evitare il danno stesso, considerando anche le risorse economiche messe a disposizione dal titolare.[14]

Inoltre, il responsabile è tenuto a controllare, nei limiti delle sue cognizioni, "*la bontà delle istruzioni ricevute dal titolare*". Ne consegue che "*eventuali errori nelle istruzioni impartite dal titolare non hanno efficacia esimente rispetto alla responsabilità del responsabile verso terzi, qualora quest'ultimo non dimostri di aver manifestato il proprio dissenso e di essere stato indotto ad eseguirle, quale* nudus minister*, per le insistenze del titolare e a rischio di quest'ultimo*"[15].

3.2. Manca l'accordo tra titolare e responsabile.

Qualora non sia stato predisposto un accordo sul trattamento e, dunque, il responsabile non sia stato nominato ed istruito dal titolare ai sensi dell'art. 28 del GDPR, elemento dirimente al fine di determinarne o meno la eventuale responsabilità è costituito dal comportamento del responsabile.

Anche in tal caso, fondamentale è lo strumento dell'*accountability* e cioè le risultanze documentali delle valutazioni eseguite dal responsabile del trattamento con riferimento ai trattamenti di dati personali di cui è potuto ragionevolmente venire a conoscenza direttamente eseguendo le attività delegategli dal titolare.

Infatti, deve essere distinto il caso in cui il responsabile con le informazioni oggettive in suo possesso, abbia consapevolezza circa il trattamento e sia in grado di adottare una misura di

[13] Cfr. Sent. della CGUE del 5 dicembre 2023. V. par. 7, lett. b.
[14] Cfr. art. 82 par. 3 del GDPR.
[15] Cfr., ex multis, Cass. Civ. 9 ottobre 2017, n. 23594; Cass. civ. 17 ottobre 2014, n. 22036

sicurezza da quello in cui senza specifiche informazioni relative al trattamento (quali i dati trattati, le finalità, l'ambito di comunicazione e diffusione ecc.) il responsabile non sia in condizioni di conoscere il contesto legato al trattamento e, conseguentemente, di capire e scegliere quali misure di sicurezza adottare.

Nella prima ipotesi, la condotta omissiva del responsabile determinerà responsabilità per inadempimento rispetto a quanto prescritto dalle norme in materia di protezione dei dati personali e sicurezza del trattamento, mentre nel secondo caso il grado di responsabilità del responsabile sarà sicuramente limitato o inesistente.

Nel caso di violazione del trattamento dei dati personali, se il responsabile dimostra di aver sollecitato al titolare la necessità di una propria nomina *ex* art 28 (e ne possa dare dimostrazione) e, addirittura, abbia sottoposto un proprio accordo sul trattamento al titolare, comprensivo delle istruzioni, senza ricevere alcun riscontro o nomina da parte del medesimo, la responsabilità del responsabile sarà sicuramente limitata se non esclusa. A ciò si aggiunga che si avrà una limitazione della responsabilità qualora il responsabile, seppure in assenza di nomina o istruzioni da parte del titolare, si comporti effettivamente come responsabile del trattamento e ponga in essere gli adempimenti e le misure di sicurezza richieste dalla normativa anche se nei limiti delle risorse a sua disposizione[16].

a) Esiste l'accordo ma le istruzioni del titolare sono incomplete.

Un altro scenario che potrebbe configurarsi e comportare problemi di addebito di responsabilità è quello in cui le parti abbiano stipulato un accordo sul trattamento, ma lo stesso sia privo di pattuizioni e istruzioni specifiche. Ai fini della determinazione delle responsabilità, è infatti fondamentale che nell'accordo siano regolati nel dettaglio gli obblighi del titolare e del responsabile, soprattutto in relazione alle misure di sicurezza. Questo scenario può determinare due ipotesi concrete di rischio e addebito di responsabilità:

b) Mancanza di istruzioni specifiche o istruzioni generiche.

Una prima ipotesi potrebbe riguardare la mancata indicazione specifica, nell'accordo sul trattamento, delle istruzioni che deve seguire il responsabile del trattamento, tra cui quelle in merito alle misure di sicurezza da adottare. La questione è dove tracciare la linea di demarcazione tra le decisioni riservate al titolare del trattamento e quelle che possono essere lasciate a discrezione del responsabile.

[16] In tal senso si è espresso il Garante con Ordinanza ingiunzione del 14 gennaio 2021 nei confronti della Regione Lazio (doc. web n. 9542113). Il Garante ha ritenuto sufficiente ammonire il titolare della Cooperativa perché la Società Capodarco aveva più volte rappresentato alla Regione la necessità di essere nominata responsabile del trattamento e messo in atto misure conformi alla disciplina privacy, istituendo, ad esempio, il registro dei trattamenti.

A tal proposito, le Linee Guida dell'EDPB[17] operano una netta distinzione tra "*mezzi essenziali*" (strettamente legati alla finalità e alla portata del trattamento) riservati al titolare e "*mezzi non essenziali*" che riguardano aspetti più pratici legati all'esecuzione del trattamento, quali la scelta di un particolare tipo di hardware o di software o le misure di sicurezza specifiche, che possono essere determinati anche dal responsabile. Il titolare deve fornire al responsabile una descrizione delle attività di trattamento e deve stabilire determinati elementi nell'accordo sul trattamento dei dati quali, ad esempio, il tipo di dati personali trattati, la durata del trattamento, le categorie di interessati e le finalità del trattamento.

In relazione al requisito della sicurezza, il titolare potrebbe dare l'istruzione generica di "*adottare tutte le misure di sicurezza necessarie*" ai sensi dell'art. 32 del GDPR, definendo solo gli obiettivi minimi di sicurezza (sulla base della valutazione del rischio eseguita dallo stesso titolare, anche in collaborazione con il responsabile). In tal caso, il responsabile può avere un margine di discrezionalità in merito alla scelta di misure più idonee legate agli aspetti pratici e tecnici di esecuzione dell'incarico, ma in ogni caso devono essere sottoposte e concordate con il titolare che deve prendere una decisione in merito alla loro implementazione e fornire le risorse economiche necessarie.

È, pertanto, sempre rimesso al titolare il potere decisionale e la conseguente responsabilità in merito alle misure di sicurezza che devono essere adottate dal responsabile o che lo stesso suggerisce e intende implementare. Tuttavia, qualora il responsabile richieda al titolare l'approvazione e l'implementazione di determinate misure e il titolare non fornisca riscontro in un tempo ragionevole, il responsabile è autorizzato a considerare il silenzio quale tacita approvazione e attuare di propria iniziativa le misure, come previsto ai sensi dell'art 1712 c.c.[18] in tema di mandato.

Difatti, lo spontaneo adoperarsi del responsabile, a fronte del silenzio serbato dal titolare, non solo non integra una violazione degli obblighi previsti dall'accordo sul trattamento, in virtù di quanto previsto dall'art. 1712 c.c., ma, a certe condizioni, rappresenta addirittura una condotta doverosa per il responsabile che intenda esimersi dalla responsabilità prevista dall'art. 32 GDPR.

L'art. 32 GDPR, infatti, pone in capo al responsabile un autonomo obbligo di implementare misure di sicurezza adeguate al rischio dei trattamenti effettuati, perciò egli è

---

[17] Cfr. *Linee Guida dell'EDPB 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR.*

[18] Cfr. art. 1712 c.c. "*Il mandatario deve senza ritardo comunicare al mandante l'esecuzione del mandato. Il ritardo del mandante a rispondere dopo aver ricevuto tale comunicazione, per un tempo superiore a quello richiesto dalla natura dell'affare o dagli usi, importa approvazione, anche se il mandatario si è discostato dalle istruzioni o ha ecceduto i limiti del mandato*".

tenuto ad assumere le opportune iniziative quand'anche il titolare non presti la necessaria collaborazione.

L'attivazione del responsabile, a prescindere dalle indicazioni ricevute dal titolare, rappresenta, peraltro, una condizione necessaria ad escluderne la responsabilità sul piano civilistico, prima ancora che della normativa in materia di protezione dei dati personali ed è uno dei criteri indicati al par. 2 dell'art 83 GDPR che il Garante deve considerare per decidere se infliggere una sanzione amministrativa pecuniaria e per determinarne l'eventuale ammontare.

In ogni caso, il titolare deve sempre assicurarsi che l'accordo sia conforme all'art. 28, par. 3, del GDPR e verificare la liceità e correttezza dell'operato del responsabile. Il responsabile non può sostituirsi al titolare nella determinazione delle istruzioni da introdurre nell'accordo sul trattamento.

c) Le misure di sicurezza indicate nelle istruzioni dal titolare non sono conformi al livello di rischio o al GDPR.

Una seconda ipotesi di rischio da prendere in considerazione riguarda il caso in cui il responsabile segnali al titolare che le misure di sicurezza, che lo stesso abbia deciso di adottare, anche discostandosi da quelle suggerite dal responsabile, non risultano conformi al livello di sicurezza previsto dal GDPR o dalla normativa privacy vigente.

Di fatto il responsabile ha l'obbligo di rispettare le istruzioni impartitegli dal titolare, ma anche quello di rispettare la legge.

L'EDPB nelle Linee Guida citate raccomanda alle parti di concordare nell'accordo sul trattamento sia le conseguenze derivanti da una comunicazione con la quale il responsabile avvisi il titolare che una determinata istruzione violi la normativa vigente, sia le conseguenze derivanti dall'inerzia del titolare.

Qualora le parti non abbiano stipulato clausole di tal genere, e il responsabile abbia segnalato al titolare la non conformità delle misure di sicurezza, egli non può invocare *sic et simpliciter* l'inerzia del titolare come giustificazione dell'insufficiente livello di sicurezza dei trattamenti effettuati. Come già evidenziato, il responsabile è gravato, ai sensi dell'art. 32 GDPR, da un autonomo obbligo rispetto alla garanzia della sicurezza dei trattamenti effettuati, di talché per esimersi dalla responsabilità prevista dall'art. 32 GDPR è tenuto a dimostrare di essersi spontaneamente attivato per rimediare alle criticità nel livello di sicurezza riscontrate o riscontrabili secondo i canoni dell'ordinaria diligenza professionale.

In tal caso, il grado di responsabilità del titolare potrebbe configurarsi a livello di dolo o colpa grave e limitare se non escludere di conseguenza la responsabilità del Responsabile, con l'applicazione di una sanzione pecuniaria di importo elevato.

Nell'ipotesi in cui il responsabile non sia in grado di fornire tale prova liberatoria, la violazione dell'art. 32 GDPR, per l'inadeguatezza delle misure di sicurezza adottate, nonché le ulteriori conseguenze dannose verificatesi, sul piano civilistico, nei confronti di terzi saranno imputate alla concorrente responsabilità del titolare e del responsabile.

4. Le misure di sicurezza AgID ed ENISA.

Al fine di comprendere meglio i profili di responsabilità dei soggetti coinvolti nel trattamento, si rende necessario soffermarsi sull'obbligo di adozione di adeguate misure di sicurezza tecniche e organizzative. Infatti, il titolare e il responsabile possono essere esonerati da responsabilità nel caso in cui adottino delle misure che assicurino adeguatamente la sicurezza del trattamento.

La scelta delle misure di sicurezza da adottare dovrà essere svolta caso per caso sulla base di una valutazione di adeguatezza delle misure in rapporto ai rischi specificatamente individuati a seguito di analisi del rischio.

Nel decidere se infliggere la sanzione e nel determinarne l'eventuale misura, l'Autorità Garante valuta positivamente altresì se il titolare e il responsabile abbiano adottato delle misure di sicurezza tecniche e organizzative che abbiano assicurato almeno un livello minimo di protezione dei dati personali.

Nel GDPR non è previsto un elenco dettagliato di misure minime di sicurezza che devono essere obbligatoriamente adottate dal titolare e dal responsabile al fine dell'esonero dalla responsabilità. L'art. 32prevede infatti genericamente che il titolare e il responsabile del trattamento mettano in atto "*misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*", e menziona a titolo esemplificativo alcune misure, quali la pseudonimizzazione e la cifratura, l'utilizzo di tecnologie e procedure in grado di assicurare "*la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento*" e di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.

A tali indicazioni si aggiungono le ulteriori misure menzionate nel Considerando 78, quali la minimizzazione e l'adozione di sistemi in grado di garantire la trasparenza per quanto riguarda le funzioni e il trattamento di dati personali al fine di consentire all'interessato di controllare il trattamento dei dati.

In mancanza di una previsione puntuale delle misure minime di sicurezza nel GDPR, al fine di agevolare le organizzazioni nella scelta delle misure da adottare, l'AgID ha individuato con Circolare n. 2/2017 le "Misure minime di sicurezza ICT per le PA"[19]. Si tratta di un insieme

[19] CircolareAgID_170418_n_2_2017_Mis_minime_sicurezza_ICT_PA-GU-103-050517-2.pdf (cert-agid.gov.it).

ordinato e ragionato di azioni puntuali di natura tecnica od organizzativa che devono essere implementate dalle Pubbliche Amministrazioni, al fine di valutare e innalzare il proprio livello di sicurezza informatica e contrastare le minacce più frequenti.

A seconda della complessità del sistema informativo a cui si riferiscono e della realtà organizzativa dell'Amministrazione, le misure minime possono essere implementate in modo graduale seguendo tre livelli di attuazione (minimo, standard e avanzato):

i. I controlli del primo livello (livello "Minimo") sono quelli strettamente obbligatori ai quali ogni PA, indipendentemente dalla sua natura e dimensione, deve essere conforme in termini tecnologici, organizzativi e procedurali: essi dunque rappresentano complessivamente il livello sotto al quale nessuna Amministrazione può scendere.

ii. I controlli del secondo livello (livello "Standard") rappresentano la base di riferimento per la maggior parte delle Amministrazioni, e costituiscono un ragionevole compromesso fra efficacia delle misure preventive ed onerosità della loro implementazione.

iii. Le misure del terzo livello (livello "Alto") sono previste per le organizzazioni maggiormente esposte a rischi, ad esempio per la criticità delle informazioni trattate o dei servizi erogati, ma anche l'obiettivo ideale cui tutte le altre organizzazioni dovrebbero tendere.

In ogni caso, ciascuna Amministrazione deve adottare almeno le misure previste al livello "Minimo" e comunque le misure che risultano adeguate in esito all'analisi dei rischi effettuata in relazione al trattamento.

A riguardo anche l'Enisa ha predisposto un documento – l'"*Handbook on Security of Personal Data Processing*"[20] – in cui fornisce un quadro dettagliato di misure tecniche e organizzative che occorre adottare suddivise sulla base del livello di rischio per la sicurezza individuato in relazione al trattamento di dati da porre in essere. Nello specifico, le misure ivi elencate nell'Allegato A al predetto documento devono essere adottate sulla base di un criterio di scalabilità: ciò significa che (i) tutte le misure descritte al livello basso (verde) saranno applicabili a tutti i livelli, (ii) le misure presentate sotto il livello medio (giallo) sono applicabili anche al livello alto di rischio, e infine (iii) le misure presentate sotto il livello alto (rosso) sono applicabili a questo livello di rischio.

5. Aspetti economici legati all'adozione delle misure di sicurezza.

Per quanto riguarda gli aspetti economici, è bene precisare che in assenza di una pattuizione specifica all'interno dell'accordo sul trattamento, che preveda la ripartizione dei costi di adeguamento, la valutazione economica dovrà essere necessariamente effettuata sulla base del

[20] Handbook on Security of Personal Data Processing — ENISA (europa.eu).

caso concreto e, dunque, sulla tipologia di misure proposte e sulla loro stretta necessità rispetto ai compiti delegati al responsabile.

Laddove dovesse emergere che le misure che il responsabile intende implementare non siano strettamente necessarie all'esecuzione del proprio incarico o comunque siano eccessive rispetto ad una valutazione di adeguatezza ai sensi dell'art. 32 del GDPR, esse potranno essere economicamente imputabili al responsabile.

Nel caso in cui, invece, nell'accordo sul trattamento il perimetro delle misure di sicurezza sia già stato esattamente delineato, per il responsabile sarà più difficile richiedere al titolare il pagamento dell'*upgrade* di sicurezza. In tal caso, si potrebbe applicare l'art. 1711 c.c. con la conseguenza che, eccedendo il mandato, tali attività siano imputabili al responsabile (mandatario) e i relativi costi siano posti a carico di quest'ultimo.

Diversamente, qualora si tratti di misure che devono essere poste in essere per adempiere l'incarico e siano strettamente necessarie per garantire la *compliance* all'art. 32 del GDPR, potranno essere ragionevolmente poste economicamente a carico del titolare.

È questo il caso in cui il responsabile segnali al titolare che le misure di sicurezza indicate e imposte dal titolare stesso presentino criticità tali da non risultare conformi al livello di sicurezza previsto dal GDPR o dalla normativa privacy vigente e sia necessario procedere con azioni correttive e/o implementazioni di misure di sicurezza ulteriori, che possono comportare dei costi.

In tal caso, il titolare dovrà prendere una decisione con riferimento tanto all'aspetto della sicurezza, quanto a quello economico, effettuare una valutazione costi benefici e, nel caso in cui decida di non adeguare la sicurezza del proprio trattamento, dovrà avere anche la consapevolezza di una sua potenziale responsabilità in caso di danno determinato dal livello basso di sicurezza. Quest'ultima ipotesi è quella più frequente nel rapporto tra pubblica amministrazione e società strumento e, a nostro avviso, importa la mancanza di responsabilità in capo al responsabile giacché nello schema dell' *in house providing* il responsabile è di fatto totalmente dipendente economicamente dalla PA che ne detiene il controllo in un rapporto organico di subalternità.

6. Applicazioni analogiche dei principi giurisprudenziali in tema di responsabilità dei delegati.

Le sopra esposte considerazioni costituiscono una puntuale applicazione dei principi in conformità ai quali la giurisprudenza ripartisce la responsabilità tra delegante e delegato in tutte le ipotesi in cui, nell'ambito di organizzazioni complesse, si realizzi una trasposizione verso il basso delle funzioni dei soggetti apicali, come avviene anche nel caso in cui un ente pubblico deleghi il trattamento dei dati ad una società *in-house*.

Fra tutti è utile richiamare, in via analogica, la disciplina della delega di funzioni rispetto all'adempimento degli obblighi di sicurezza posti in capo al datore di lavoro ai sensi del D.Lgs. n. 81/2008.

In caso di violazioni della normativa antinfortunistica imputabili al delegato, il datore di lavoro non è esonerato da responsabilità qualora non abbia adeguatamente controllato l'attività del delegato o fornito allo stesso idonee istruzioni.

Il consolidato orientamento della corte di legittimità chiarisce, infatti, che "*L'effetto della delega di funzioni non ha mai l'effetto di esautorare l'originario incaricato operando, piuttosto, quale causa dell'addizione di un nuovo centro di responsabilità e poteri*"[21].

Del pari, la nomina di un responsabile del trattamento non comporta il trasferimento in capo a quest'ultimo degli obblighi del titolare, ma ha l'effetto di includere il responsabile tra i destinatari degli stessi.

Il riparto di responsabilità tra titolare e responsabile viene, quindi, a configurarsi nei seguenti termini: il titolare assume una posizione di garanzia rispetto al corretto operato del responsabile e, pertanto, risponde di eventuali violazioni riconducibili alla carenza di misure di sicurezza, per non averne prescritto l'adozione al delegato ovvero per non averle egli stesso implementate, ove raccomandate dal responsabile; il responsabile, invece, risponde dell'inosservanza delle istruzioni ricevute dal titolare, oppure del proprio atteggiamento inerziale, qualora, non avendo ricevuto istruzioni da parte del titolare o avendone ricevute di inadeguate, non lo abbia sollecitato a provvedere[22].

Ne deriva che il titolare incorrerà in una responsabilità omissiva: (i) per non aver adeguatamente istruito il responsabile; (ii) per non aver vigilato sul suo operato o (iii) per non aver dato riscontro alle sue richieste in merito all'adozione delle misure di sicurezza adeguate.

Il responsabile incorrerà, invece, in una responsabilità commissiva, (i) per aver disatteso le legittime istruzioni del titolare oppure (ii) per non aver sollecitato il titolare inerte a fornirgliene di adeguate.

---

[21] Cassazione penale sez. IV, 08/04/2021, n.26332. La Corte ha ritenuto corretto che fosse stata affermata la responsabilità del datore di lavoro, essendosi addebitato a questi, pur in presenza di una delega, l'omesso controllo sull'attività del delegato, in presenza di violazioni alla normativa antinfortunistica non solo evidenti, ma anche espressamente segnalate dal professionista incaricato di redigere il piano operativo di sicurezza.

[22] In tal senso si è espresso il Garante con Ordinanza ingiunzione del 14 gennaio 2021 nei confronti della Regione Lazio (doc. web n. 9542113). Il Garante ha ritenuto sufficiente ammonire il titolare della Cooperativa perché la Società Capodarco aveva più volte rappresentato alla Regione la necessità di essere nominata responsabile del trattamento e messo in atto misure conformi alla disciplina privacy, istituendo, ad esempio, il registro dei trattamenti.

7. La giurisprudenza in materia.

La recente giurisprudenza ha evidenziato come la corretta qualificazione dei ruoli nell'organizzazione del trattamento dei dati personali in ambito pubblico sia caratterizzata da numerose criticità. A riguardo sono rilevanti due recenti sentenze, una del Tribunale di Pordenone del 13 ottobre 2023 e una della Corte di Giustizia dell'Unione Europea (di seguito "CGUE") del 5 dicembre 2023, che hanno fornito ulteriori chiarimenti in merito ai criteri da seguire al fine di individuare il ruolo di titolare del trattamento e di responsabile in ambito pubblico, nonché le rispettive responsabilità, con particolare riferimento alle società strumento della pubblica amministrazione.

a) Sentenza del Tribunale di Pordenone del 13 ottobre 2023.

Il Tribunale di Pordenone con sentenza del 13 ottobre 2023[23] ha fornito dei rilevanti spunti al fine di individuare correttamente i ruoli privacy, in particolare per quanto riguarda i trattamenti di dati personali in ambito sanitario che vedono coinvolti la Regione Friuli e le ASL.

Il caso *de quo* riguarda la decisione della Regione Friuli[24] di sviluppare un progetto di stratificazione statistica di alcune categorie di pazienti in relazione al rischio di avere o meno complicanze in caso di infezione da Covid-19. L'iniziativa si poneva all'interno della Legge FVG 22/2019 secondo la quale il SSR avrebbe avviato modalità organizzative innovative di presa in carico dei pazienti per lo sviluppo della medicina di iniziativa[25].

Il progetto prevedeva il coinvolgimento dei Medici di Medicina Generale (MMG) chiamati a validare attraverso il portale informatico regionale, una lista di utenti/assistiti in relazione alle loro condizioni di salute. Tali dati venivano poi estratti dal *data warehouse* regionale ed elaborati da due società in-house della regione Friuli attraverso un algoritmo di classificazione.

In sostanza, attraverso questo sistema si realizzava, accedendo alle banche date delle ASL e lavorando i dati attraverso un *software* di classificazione, un profilo di rischio dei pazienti prodromico alla successiva presa in carico dei pazienti stessi.

Tale trattamento è stato oggetto di una segnalazione effettuata da un medico di base al Garante per la protezione dei dati personali che rilevava l'illiceità del trattamento di dati personali effettuato dalle ASL sotto vari profili tra i quali (i) mancanza di una idonea base giuridica, (ii) mancanza di una valutazione di impatto, (iii) mancanza dell'informativa, (iv)

---

[23] https://www.gpdp.it/documents/10160/0/Sentenza+del+13+ottobre+2023+-+Tribunale+di+Pordenone.pdf/e95fa647-3de1-0bea-1dc6-f40579647801?version=1.0

[24] Con delibera 20 novembre 2020 n. 1737.

[25] Cfr. Provv. del Garante del 15 dicembre 2022 il quale riporta la definizione di medicina di iniziativa fornita dal Ministero della Salute: "Per medicina d'iniziativa si intende un modello assistenziale orientato alla 'promozione attiva' della salute dell'individuo, specie se affetto da malattie croniche o disabilità, e alla responsabilizzazione delle persone nel proprio percorso di cura".

mancanza del consenso. Al termine dell'istruttoria pertanto il Garante sanzionava le tre aziende sanitarie locali.

In particolare, seppur il trattamento illecito avente ad oggetto l'elaborazione dei dati dei pazienti fragili era stato posto in essere dalla società in house, designata responsabile del trattamento ai sensi dell'art. 28 del GDPR, il Garante riconosceva comunque la responsabilità all'Azienda sanitaria, proprietaria della banca dati, in quanto assumeva il ruolo di titolare del trattamento ai sensi dell'art. 24 del GDPR. Pertanto secondo il Garante, la circostanza che un soggetto terzo (la Regione), chieda a un titolare (Azienda sanitaria), anche per il tramite del responsabile (la società *in house*) di effettuare operazioni di trattamento su dati personali, non esclude che spetti comunque al titolare, anche in base al principio di responsabilizzazione (artt. 5, par. 2 e 24 del Regolamento), valutare la legittimità della richiesta e, in particolare, la sussistenza di una idonea base giuridica per effettuare le operazioni di trattamento richieste, tanto più che, nel caso di specie, le predette operazioni hanno riguardato dati sulla salute di migliaia di assistiti a livello regionale attraverso l'uso di algoritmi.

Tale provvedimento del Garante è stato poi impugnato avanti al Tribunale di Pordenone da parte dell'Azienda sanitaria del Friuli.

L'Azienda in particolare affermava di non assumere il ruolo di titolare del trattamento perché non aveva posto in essere il potere di determinare le finalità del trattamento (nella specie pertinenti alla programmazione e valutazione dell'assistenza sanitaria) e i mezzi del trattamento (nella specie: applicazione dell'algoritmo ACG alle banche dati presenti nel c.d. *datawarehouse* regionale), come previsto dall'art. 24 del GDPR. Infatti nel caso in esame le finalità e i mezzi sono stati interamente stabiliti dalla Regione, mentre l'Azienda non ha assunto alcuna decisione in relazione al trattamento né svolto alcuna attività specifica in materia di trattamento. Inoltre non aveva alcun potere nei confronti della Regione dalla quale, anzi, dipende, come pure la società *in house*, che ha proceduto autonomamente in diretta esecuzione delle direttive regionali. A riprova di ciò la società *in house* non ha mai neanche acquisito alcuna autorizzazione dell'Azienda, essendo legittimata ad agire da una delibera regionale.

Su queste basi il Tribunale di Pordenone ha annullato il provvedimento del Garante, accogliendo l'assunto secondo cui è la Regione ad essere titolare del trattamento, avendo deciso le finalità e i mezzi del trattamento con la citata delibera regionale. L'Azienda sanitaria non è stata ritenuta responsabile delle violazioni privacy commesse dalla società *in house* nell'attuazione di progetti decisi dalla Regione, anche se realizzate con la banca dati di titolarità dell'ASL.

Sulla base di questa decisione, ai fini della qualificazione di un soggetto come responsabile e come titolare, non può prescindersi quindi da una valutazione concreta delle attività condotte da tale soggetto. Infatti, qualora il responsabile in concreto tratti i dati per fini e mezzi ulteriori

e diversi da quelli indicati dal titolare e dai compiti dallo stesso assegnatigli, questo assumerà il ruolo di titolare del trattamento o, a seconda dei casi, di contitolare (Art. 28, par. 10 GDPR). Dall'altro lato, il titolare del trattamento sarà tale se in concreto decida il motivo e le modalità del trattamento, senza ricevere istruzioni da altri. In particolare, nel caso di specie, al Giudice non è apparso corretto attribuire la qualifica di titolare del trattamento al soggetto che si occupa della gestione dei dati ed è titolare delle banca dati oggetto di trattamento (ASL), in quanto occorre verificare l'attività che egli ha svolto in concreto nell'ambito del trattamento stesso.

b) Sentenza della CGUE del 5 dicembre 2023.

La CGUE ha pubblicato in data 5 dicembre 2023 la sentenza nella causa C-683/21[26] che fornisce alcune importanti precisazioni (i) sulla corretta qualificazione dei ruoli di titolare e di responsabile del trattamento ai sensi del GDPR in ambito pubblico, nonché (ii) sul tema, strettamente correlato, delle sanzioni amministrative previste in caso di violazione della normativa privacy, ai sensi dell'art. 83 del GDPR.

Per quanto riguarda i fatti oggetto della sentenza, il caso fa riferimento all'avvio di un progetto di sviluppo di un'applicazione per la registrazione e il monitoraggio delle persone affette da Covid-19 (in seguito, anche "App"), commissionata dal Ministero della Salute lituano ad un fornitore di servizi privato.

Il Ministero della Salute e il *provider* del *software* informatico sono stati entrambi designati come "responsabili del trattamento", come risulta nell'informativa sulla privacy rilasciata agli interessati. A seguito del lancio dell'applicazione, gli utenti che si sono iscritti hanno fornito molteplici dati personali, tra cui soprattutto dati particolari *ex* art. 9 del GDPR (dati relativi alla salute).

L'Autorità locale per la protezione dei dati lituana (di seguito "Autorità lituana") ha pertanto avviato un'indagine all'esito della quale ha ritenuto che il Ministero della Salute e il provider assumessero la qualifica di contitolari del trattamento ai sensi dell'art. 26 del GDPR. Pertanto, ha sanzionato i due contitolari sotto diversi profili e in particolare per: (i) violazione dei principi di trattamento dei dati; (ii) non aver fornito agli interessati le informazioni necessarie sul trattamento; (iii) non aver adottato misure tecniche, organizzative e di sicurezza per conformarsi al GDPR; (iv) non aver effettuato una valutazione d'impatto sulla protezione dei dati.

Il Ministero della Salute ha impugnato il provvedimento dell'Autorità lituana innanzi al Tribunale lituano, sostenendo che il *provider* era l'unico soggetto "responsabile" della conformità al GDPR; dall'altro lato, quest'ultimo sosteneva di aver agito secondo le istruzioni

[26] https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62021CJ0683&qid=1703173698231.

del Ministero della Salute e quindi che fosse quest'ultimo responsabile del rispetto della normativa sulla protezione dei dati personali.

Il Tribunale ha preliminarmente evidenziato che il *provider* ha realizzato l'applicazione su istruzioni del Ministero della Salute che però non aveva autorizzato la pubblicazione dell'App sugli store. Da qui il dubbio pregiudiziale del Tribunale sottoposto alla CGUE circa la corretta qualificazione dei ruoli rivestiti dai due soggetti e sulla relativa responsabilità per la mancata compliance al GDPR.

In primo luogo, la CGUE ha chiarito che un soggetto potrebbe essere considerato un titolare del trattamento anche se (i) non ha trattato direttamente i dati; (ii) non ha fornito il suo esplicito consenso al trattamento effettuato per suo conto; (iii) le finalità e i mezzi del trattamento, seppur non risultanti da atto scritto, sono state determinate dal punto di vista concreto. Ciò che conta ai fini della qualifica di un soggetto come titolare è che partecipi in maniera attiva e concreta nella determinazione delle finalità e dei mezzi del trattamento, a nulla rilevando che nella informativa privacy tale soggetto sia designato come "responsabile del trattamento".

Sul tema la CGUE ha quindi affermato che un ente pubblico che ha incaricato un'impresa di sviluppare un'applicazione informatica può essere considerato titolare del trattamento se ha partecipato alla determinazione delle finalità e dei mezzi del trattamento dei dati personali effettuato mediante tale applicazione, anche se tale ente non ha proceduto a operazioni di trattamento di tali dati e non ha dato esplicitamente il proprio consenso alla realizzazione delle operazioni concrete di un siffatto trattamento. Nel caso invece in cui il suddetto ente si sia espressamente opposto alle operazioni di trattamento poste in essere, egli non sarà più titolare del trattamento perché non si potrebbe ritenere che il trattamento in questione sia stato effettuato per suo conto.

Sotto il profilo della responsabilità, la CGUE ha affermato che la sanzione amministrativa pecuniaria prevista per violazioni della normativa privacy può essere comminata al titolare del trattamento nelle seguenti ipotesi:

(i) In primo luogo, qualora la violazione degli obblighi posti dal GDPR sia stata commessa dal titolare stesso in modo illecito, ossia dolosamente o colposamente, quindi nel momento in cui il titolare del trattamento non poteva ignorare l'illiceità del suo comportamento;

(ii) In secondo luogo, tale sanzione può essere inflitta a un titolare del trattamento in relazione a operazioni di trattamento di dati personali effettuate per suo conto da un responsabile del trattamento, in quanto il titolare del trattamento è responsabile non solo dei trattamenti di dati personali che effettua direttamente, ma anche di quelli che vengono effettuati per suo conto dal responsabile.

Tuttavia, tale sanzione potrà essere inflitta nei confronti del responsabile del trattamento, (i) qualora egli tratti i dati per il perseguimento di finalità proprie, (ii) ovvero in modo contrario o difforme alle indicazioni fornite dal titolare (iii) o in modo tale che non si può ragionevolmente ritenere che tale titolare abbia a ciò acconsentito. In tale ipotesi il responsabile deve infatti essere considerato titolare del trattamento ai sensi dell'art. 28, paragrafo 10 del GDPR.

8. Conclusioni

In conclusione, nell'ambito di un trattamento di dati personali è importante individuare correttamente il soggetto che assume la qualifica di titolare del trattamento e quello che, invece, è il responsabile, al fine non solo di comprendere l'effettiva portata degli obblighi che gli stessi dovranno porre in essere nell'ambito di tale trattamento, ma al fine altresì di riconoscere correttamente la responsabilità nel caso in cui ci sia una violazione della normativa sulla protezione dei dati.

Tali tematiche sono rilevanti soprattutto nell'ambito del rapporto di *in-house providing* dove generalmente la PA assume il ruolo di "titolare del trattamento", in quanto determina le finalità e le modalità di tale trattamento, mentre la società strumento quello di "responsabile del trattamento" in quanto effettua, per conto della prima,le attività tecniche necessarie alla gestione dei dati. La società *in-house* opera perciò come "*longa manus*" dell'Amministrazione, in un rapporto di immedesimazione organica e di subordinazione come sottolineato dal Consiglio di Stato.

È frequente che in tali tipi di rapporti si creino situazioni conflittuali nel caso in cui si verifichi una violazione del GDPR per comprendere chi sia il soggetto responsabile e i criteri sulla base dei quali poter attribuire le diverse responsabilità.

Qualora la PA e la società *in-house* abbiano stipulato un accordo sul trattamento, o abbiamo inserito delle clausole contrattuali all'interno del contratto che disciplinino nello specifico gli elementi relativi al trattamento e i rispettivi obblighi, allora sarà più semplice comprendere chi sia il soggetto a cui possa essere addebitata la responsabilità in caso di violazione e la conseguente applicazione del rimedio sanzionatorio. Sanzione la cui determinazione spetta all'Autorità Garante per la protezione dei dati personali tenendo in considerazione di tutti gli elementi di cui all'art. 83, par. 2 del GDPR.

Nel caso in cui tale accordo non sia stato stipulato, oppure se esistente, preveda delle istruzioni generiche o incomplete,oppure ancora preveda l'adozione di misure di sicurezza contrarie al GDPR, o non adeguate al rischio, allora occorre tener presente degli elementi generali attinenti al comportamento posto in essere dal titolare e dal responsabile, nonché al

grado di conoscibilità del trattamento da parte del responsabile, e al grado di responsabilità di quest'ultimo, che devono essere valutati secondo i principi dell'*accountability.*

Altro elemento rilevante ai fini del riconoscimento della responsabilità è l'aspetto economico relativo ai costi di attuazione delle misure. Quando il responsabile faccia presente al titolare che occorre adottare delle misure di sicurezza atte a garantire la *compliance* all'art. 32 del GDPR, e il titolare non fornisca al responsabile le risorse economiche sufficienti, la responsabilità per la mancata adozione delle misure sarà attribuibile al titolare, in quanto comunque il responsabile non avrebbe potuto adottare tali misure giacché dipendente economicamente in tutto e per tutto dall'amministrazione proprio in ragione del rapporto di immedesimazione organica di cui abbiamo già parlato. Infatti, nello schema dell'*in house providing* il responsabile è di fatto totalmente dipendente economicamente dalla PA che ne detiene il controllo in un rapporto organico di subalternità. Quando la PA non fornisce adeguate risorse economiche e la società strumento si trova impossibilitata a mettere in atto le misure di sicurezza ritenute necessarie e adeguate, va di pari passo che la responsabilità in caso di violazione dei dati dovrà essere attribuita alla PA titolare del trattamento.