Deliberazione della formazione ristretta n. SAN-2024-013 del 5 settembre 2024 relativa alla società CEGEDIM SANTÉ

La Commissione nazionale per l'informatica e le libertà, riunita in formazione ristretta, è composta da Philippe-Pierre CABOURDIN, presidente, Vincent LESCLOUS, vicepresidente, Isabelle LATOURNARIE-WILLEMS e Laurence FRANCESCHINI e Alain DRU, membri;

Visto il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione dei dati personali e alla libera circolazione di tali dati;

Vista la legge n. 78-17 del 6 gennaio 1978 sull'informatica, i file e le libertà, in particolare gli articoli 20 e seguenti;

Visto il decreto n. 2019-536 del 29 maggio 2019 adottato per l'attuazione della legge n. 78-17 del 6 gennaio 1978 sull'informatica, i file e le libertà;

Vista la deliberazione n. 2013-175 del 4 luglio 2013 che adotta il regolamento interno della Commissione nazionale per l'informatica e le libertà;

Vista la decisione n. 2020-085C del 12 maggio 2020 del Presidente della Commissione nazionale per l'informatica e le libertà di incaricare il Segretario generale di effettuare o far effettuare una missione di verifica dei trattamenti

effettuate dalla società CEGEDIM LOGICAL MEDICAUX FRANCE, dalle sue filiali o per suo conto, ovunque siano interessate dalla loro attuazione;

Vista la decisione del Presidente della Commissione nazionale per l'informatica e le libertà di nominare un relatore del comitato ristretto il 2 marzo 2023;

vista la relazione del Commissario relatore François Pellegrini, notificata alla società CEGEDIM SANTÉ il 12 ottobre 2023;

Viste le osservazioni scritte presentate dalla società il 17 novembre 2023, l'8 gennaio e il 21 maggio 2024;

Viste le risposte del relatore a tali osservazioni, notificate alla società l'8 dicembre 2023 e il 15 marzo 2024;

Vista la scadenza del mandato del Commissario François PELLEGRINI il 1° febbraio 2024;

Vista la decisione del Presidente della Commissione nazionale per l'informatica e le libertà di nominare un nuovo relatore, Claude CASTELLUCCIA, per il collegio ristretto del 31 gennaio 2024;

A conclusione dell'istruttoria, notificata all'azienda il 28 maggio 2024; Alla

luce dei commenti orali espressi durante la sessione di formazione ristretta;

Alla luce degli altri documenti del fascicolo;

La riunione della sessione ristretta di formazione del 13 giugno 2024 era

presente: Claude CASTELLUCCIA, Commissario, ascoltato nella sua

relazione;

In qualità di rappresentanti di CEGEDIM SANTÉ:

- ...;

La società CEGEDIM SANTÉ ha avuto la parola per

ultima; La formazione ristretta ha adottato la seguente

decisione:

I. Fatti e procedure

1. La società CEGEDIM LOGICIELS MEDICAUX FRANCE, con sede in 137, rue d'Aguesseau a Boulogne-Billancourt (92100), è una società per azioni semplificata con socio unico. Nel 2020 e 2021, ha realizzato un fatturato di [..... e un risultato netto di ... e [.....

2. L'azionista unico di CEGEDIM LOGICALS MEDICAUX FRANCE è la società CEGEDIM SANTÉ (di seguito "la società"), una società per azioni semplificata, con sede legale al 137, rue d'Aguesseau, 92100 Boulogne-Billancourt.

3. 3. In qualità di azionista unico, CEGEDIM SANTÉ ha deciso di sciogliere anticipatamente senza liquidazione la società CEGEDIM LAWICIELS MEDICAL FRANCE da
22 novembre 2021. CEGEDIM SANTÉ ha rilevato l'intera attività di CEGEDIM LOGICIELS MEDICAUX FRANCE e il trattamento dei dati personali da essa effettuato.

4. La società CEGEDIM SANTÉ fa parte del gruppo CEGEDIM, specializzato nella gestione dei flussi digitali dell'ecosistema sanitario tra professionisti e nella progettazione di software aziendali, in particolare per i professionisti della sanità. Nel 2022, il fatturato del gruppo CEGEDIM è stato pari a ... e il suo risultato netto a [.....

5. L'attività di CEGEDIM SANTÉ consiste nella pubblicazione e nella vendita di software gestionali ai medici di città che lavorano in studi medici e centri sanitari. Circa 25.000 studi medici e 500 centri sanitari utilizzano il software.

offerti dall'azienda. In particolare, pubblica il software CROSSWAY, che consente ai medici di gestire l'agenda, le cartelle cliniche e le prescrizioni.

6. L'azienda offre a un panel di medici cittadini che utilizzano questo software, idonei in base a criteri geografici, di età e di specialità, di entrare a far parte di un osservatorio per raccogliere dati dalle cartelle cliniche dei pazienti. In caso di adesione all'osservatorio, i dati contenuti nei software dei medici vengono estratti nel flusso CROSSWAY per essere utilizzati in studi e statistiche nel campo della salute condotti dai clienti della società CEGEDIM SANTÉ, tra cui le aziende... e [Per esempio,
I clienti di CEGEDIM SANTÉ realizzano studi sulla gestione dei pazienti in base alle loro patologie, alle disparità demografiche e regionali e ai profili di assistenza dei medici e alla misurazione del consumo di cure. Entro il 2021, circa... medici hanno aderito all'osservatorio.

7. In cambio, i medici del panel beneficiano di uno sconto sulla licenza d'uso del software CROSSWAY e l'azienda dà loro accesso agli studi statistici condotti dalla società, nonché a dashboard personalizzati.

8. Con decisione n. 2020-085C del 12 maggio 2020, il presidente della Commissione nazionale dell'informatica e delle libertà (di seguito "Commissione" o "CNIL") ha incaricato il segretario generale di svolgere o far svolgere una missione di verifica delle retribuzioni effettuate dalla società CEGEDIM LOGICAL MEDICAUX FRANCE, dalle sue filiali o per suo conto, ovunque possano essere interessate dalla loro attuazione.

9. Il 30 marzo 2021, una delegazione della CNIL ha effettuato un controllo nei locali della società per verificare la conformità alle disposizioni della legge n. 78-17 del 6 gennaio 1978 sull'informatica, i file e le libertà (di seguito "legge sull'informatica e le libertà" o "legge del 6 gennaio 1978" e successive modifiche) e del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 sulla protezione dei dati personali.

10. Il 12 aprile 2021 e il 16 febbraio 2023, la società ha fornito ulteriori elementi richiesti dalla delegazione durante il controllo in loco.

11. Ai fini dell'esame, il 2 marzo 2023 il Presidente della Commissione ha nominato François PELLEGRINI relatore sull'articolo 39 del decreto n. 2019-536 del 29 maggio 2019 adottato per l'applicazione della legge sull'informatica e le libertà.

12. Il 12 ottobre 2023, al termine della sua indagine, il relatore ha notificato alla società una relazione che illustrava in dettaglio le violazioni dell'articolo 5, paragrafo 1, lettera a), del GDPR e dell'articolo 66 della legge sulla protezione dei dati che riteneva costituissero il caso in questione. La relazione proponeva che la formazione ristretta emettesse una multa amministrativa contro la società e un'ordinanza con una penalità periodica per conformarsi alle carenze riscontrate. Proponeva inoltre che la decisione fosse resa pubblica.

13. Il 17 novembre 2023, la società ha presentato le proprie osservazioni in risposta al rapporto sulle sanzioni.

14. Il relatore ha risposto alle osservazioni della società l'8 dicembre 2023.

15. L'8 gennaio 2024, la società ha presentato le sue seconde osservazioni in risposta.

16. Poiché il commissario François PELLEGRINI è scaduto il 1° febbraio 2024, il presidente della CNIL ha nominato Claude CASTELLUCCIA come relatore il 31 gennaio 2024, ai sensi dell'articolo 40 I, paragrafo 5, del decreto n. 2019-536 del 29 maggio 2019.

17. Il 15 marzo 2024, il relatore ha presentato una risposta alle seconde osservazioni della società.

18. Il 21 maggio 2024, la società ha presentato le sue terze osservazioni.

19. Con lettera del 27 maggio 2024, il relatore ha informato la società e il presidente della formazione a responsabilità limitata che l'indagine è stata chiusa ai sensi dell'articolo 40 del decreto 2019-536.

20. Con lettera del 27 maggio 2024, la società è stata informata che la pratica era all'ordine del giorno della formazione ristretta del 13 giugno 2024.

21. Il 12 giugno 2024 la società, tramite il suo legale, ha chiesto di rinviare la chiusura dell'istruttoria alla riunione della formazione ristretta prevista per il giorno successivo, per poter versare un ulteriore documento, ovvero la copia di una lettera inviata dalla società CEGEDIM LOGICALS MEDICAUX alla CNIL il 25 aprile 2013. Il presidente della formazione ristretta ha dato seguito alla richiesta.

22. Il relatore e la società hanno presentato osservazioni orali durante la sessione di formazione ristretta.

II. Motivi della decisione

A. La denuncia di una mancanza di consapevolezza dei diritti della difesa e del diritto a un giusto processo

23. La società sostiene che i suoi diritti di difesa sono stati violati in quanto, con lettera del 21 dicembre 2023, il presidente della formazione ristretta ha rifiutato di prorogare il tempo richiesto per produrre le sue seconde osservazioni, in violazione del diritto a un equo processo, a suo parere. Essa afferma che, per poter rispondere alle nuove argomentazioni avanzate dal relatore, riguardanti in particolare l'analisi del rischio di reidentificazione, la società ritiene che siano necessarie ulteriori analisi, ha dovuto ricorrere a un esperto, che è stato in grado di formulare le sue conclusioni solo a metà gennaio 2024, mentre il suo termine per rispondere è scaduto l'8 gennaio 2024.

24. L'azienda sostiene inoltre che le prove essenziali che ha invocato in difesa per dimostrare la natura anonima dei dati di flusso CROSSWAY non sono state prese in considerazione dal relatore, mettendo così in dubbio l'effettiva considerazione delle sue argomentazioni e quindi il rispetto dei suoi diritti di difesa e la garanzia di un processo equo.

25. In primo luogo, la formazione ristretta sottolinea che i termini che sono stati applicati nell'ambito del contraddittorio sono quelli previsti dall'articolo 40 I del decreto n. 2017-536 sopra citato. Rileva inoltre che la società ha concesso ulteriori cinque giorni per presentare le sue prime osservazioni difensive, conformemente alla sua richiesta al presidente della formazione ristretta.

26. In secondo luogo, la formazione ristretta sottolinea che il rapporto di sanzione è stato notificato alla società già il 12 ottobre 2023. Pertanto, non vi era alcun ostacolo alla nomina di un esperto a partire da tale data, poiché, sin dal verbale di sanzione, il relatore ha ritenuto che i dati trattati dalla società non fossero anonimi ma pseudonimi. L'analisi e la posizione del relatore su questo punto erano costanti nel contesto della procedura sanzionatoria e sono state esposte fin dalla presentazione del rapporto sanzionatorio. La società avrebbe quindi potuto richiedere un esperto molto prima di ricevere la risposta del relatore alle sue prime osservazioni difensive.

27. In terzo luogo, la formazione ristretta osserva che la società è stata in grado di produrre le conclusioni della perizia rilevanti per la sua difesa, poiché il relatore non ha chiuso l'indagine al termine delle seconde osservazioni in difesa della società. Ha deciso di inviare una seconda risposta alle osservazioni della società, che ha avuto due mesi e sette giorni per presentare le sue terze osservazioni in risposta.

28. Infine, se la società ritiene che il relatore non abbia tenuto sufficientemente conto delle argomentazioni addotte nei suoi vari scritti e abbia commesso diversi errori di valutazione, la formazione ristretta fa presente che tutti gli scritti e i documenti prodotti sia dalla società che dal relatore sono stati portati in aula.

alla sua attenzione, e che quindi dispone degli elementi necessari per esprimere il proprio punto di vista sul trattamento in questione. La formazione ristretta rileva inoltre che l'azienda ha potuto presentare le proprie osservazioni a difesa nelle tre partite scritte, essendosi svolti diversi cicli di contraddittorio nell'ambito di tale procedura, nonché oralmente nella sessione di formazione ristretta del 13 giugno 2024.

29. La formazione ristretta ritiene quindi che la denuncia di ignoranza dei suoi diritti di difesa e del diritto a un processo equo debba essere annullata.

B. Sul trattamento in questione e sulla responsabilità del trattamento

30. Al momento del controllo effettuato dalla CNIL e fino al 2022, la società ha raccolto una certa quantità di dati dagli esperti che hanno aderito al suo osservatorio. Questi dati riguardavano sia le cartelle amministrative dei pazienti (numero del paziente, anno di nascita, sesso, categoria socio-professionale, codice della regione, data della consultazione), sia le cartelle cliniche (allergie, anamnesi del paziente, anamnesi familiare, altezza, peso, polso, pressione sanguigna, diagnosi diurna, ecc.), le prescrizioni farmaceutiche (farmaci, durata, ecc.) e altre prescrizioni (interruzione del lavoro, vaccini, risultati di esami biologici, ecc.)

31. Tutti questi dati sono criptati e collegati a un identificativo unico per ogni paziente, che non si basa su alcun tratto di identità del paziente. I dati dei pazienti vengono estratti periodicamente dal flusso CROSSWAY per formare un file sullo studio medico del panelista. Quando si genera questo file, i numeri dei pazienti del flusso vengono nuovamente crittografati. Il file viene quindi instradato tramite un canale crittografato HTTPS al server che ospita il database, il quale aggrega e archivia i dati in modo transitorio. In questo modo, anche se a ogni paziente vengono assegnati identificativi diversi nel flusso CROSSWAY e nei file trasmessi dai medici alla società CEGEDIM SANTÉ, tutti i dati relativi allo stesso paziente dello stesso medico sono sempre associati a questo secondo identificativo nell'insieme dei dati comunicati alla società CEGEDIM SANTÉ. D'altro canto, allo stesso paziente che si reca in un altro studio medico verrà assegnato un altro

identificativo univoco specifico di quell'altro studio. Poiché l'identificativo è collegato ai dati medici e amministrativi dello stesso paziente, consente di monitorare la storia del paziente per un singolo studio.

32. Le righe presenti nel database sono composte dagli identificativi del paziente e del medico consultato, oltre che da vari codici. . . . Secondo le cifre fornite dalla società, il numero di righe raccolte tra il 1° gennaio 2021 e il 2 aprile 2021 dalla società CEGEDIM SANTÉ è superiore a EUR [....

33. I dati vengono conservati per tre mesi dalla data di ricezione nel flusso CROSSWAY. Vengono poi trasmessi ai clienti dell'azienda, tra cui la società che realizza studi e statistiche nel campo della salute. Sebbene i dati siano conservati nel flusso per soli tre mesi, alcuni hanno una profondità storica maggiore. Ad esempio, i dati del teleservizio HRi, di cui si parlerà più avanti, vengono scaricati automaticamente con una profondità di 12 mesi quando il medico li consulta.

34. CEGEDIM SANTÉSIRB ritiene che i dati che sta trattando siano anonimi e pertanto non sono più soggetti alle norme applicabili sulla protezione dei dati personali.

35. Il relatore ritiene che la società abbia creato un magazzino di dati sanitari pseudonimi sulla base dei dati forniti dai medici panelisti, al fine di metterli a disposizione dei suoi clienti - alcuni dei quali appartengono allo stesso gruppo - che realizzano studi e statistiche nel campo della salute. Il relatore ritiene che CEGEDIM SANTÉ sia tenuta a rispettare le norme sulla protezione dei dati personali per trattare tali dati e, in particolare, a disporre di un'autorizzazione a farlo.

36. In difesa, l'azienda sostiene anche di aver implementato nuove misure di esaurimento dei dati in fase di estrazione dal 2022, dati che da allora sono meno accurati. Per esempio, non raccoglie più le informazioni dei pazienti il cui anno di nascita è stato

è inferiore o uguale a 1920 o se il paziente ha più di 95 anni, non raccoglie più il numero esatto di figli dei pazienti (0 se nessun figlio, 1 se 1 figlio o più, e se il paziente ha meno di 18 anni il numero di figli è sistematicamente 0) o non raccoglie più informazioni dai pazienti con sesso sconosciuto.

37. La formazione ristretta ritiene che la natura dei dati trattati e la qualificazione del trattamento debbano essere esaminate prima di poter determinare le responsabilità associate.

1) Sulla natura dei dati trattati nel flusso CROSSWAY

(a) Il quadro giuridico applicabile

38. L'articolo 4, paragrafo 1, del GDPR definisce il concetto di dati personali come qualsiasi informazione riguardante una persona fisica identificata o identificabile ...; si considera identificabile una persona fisica che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento a un identificatore, come un nome, un numero di identificazione ... .

39. L'articolo 4, paragrafo 15, del GDPR stabilisce che i dati personali relativi alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi sanitari, che rivelano informazioni sullo stato di salute di tale persona, costituiscono dati sanitari.

40. L'articolo 4, paragrafo 5, del GDPR definisce la pseudonimizzazione come il trattamento dei dati personali in modo tale che non possano più essere attribuiti a un soggetto specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative per garantire che i dati personali non siano attribuiti a una persona fisica identificata o identificabile.

41. La formazione limitata sottolinea il fatto che, contrariamente al concetto di pseudonimizzazione, il concetto di anonimizzazione non è definito dal GDPR.

42. Il considerando 26 del GDPR afferma che i dati personali che sono stati pseudonimizzati e che potrebbero essere attribuiti a una persona fisica mediante l'uso di informazioni aggiuntive dovrebbero essere considerati come informazioni relative a una persona fisica identificabile. Nel determinare se una persona fisica è identificabile, occorre prendere in considerazione tutti i mezzi ragionevolmente utilizzabili dal titolare del trattamento o da qualsiasi altra persona per identificare direttamente o indirettamente la persona fisica, come ad esempio il targeting. Nel determinare se è ragionevolmente probabile che i mezzi siano utilizzati per identificare una persona fisica, occorre prendere in considerazione tutti i fattori oggettivi, come il costo dell'identificazione e il tempo necessario per la stessa, tenendo conto delle tecnologie disponibili al momento del trattamento e della loro evoluzione. Non è pertanto necessario applicare i principi relativi alla protezione dei dati alle informazioni anonime, ossia alle informazioni che non si riferiscono a una persona fisica identificata o identificabile, né ai dati personali resi anonimi in modo tale che l'interessato non sia o non sia più identificabile. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche a fini statistici o di ricerca.

43. Nella sentenza Breyer, pronunciata ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (CGUE, Seconda Sezione, 19 ottobre 2016, C-582/14), la Corte di giustizia dell'Unione europea (in prosieguo: la "CGUE") ha affermato che il considerando 26 della direttiva 95/46 stabilisce che l'intervento del responsabile del trattamento o di un'altra persona per l'identificazione di tale persona (par. 42) e, nella misura in cui tale considerando fa riferimento ai mezzi che possono essere ragionevolmente attuati sia dal responsabile del trattamento sia da un'altra persona, la formulazione del responsabile del trattamento suggerisce che, affinché un dato possa essere qualificato come elemento di identificazione, è necessario che il responsabile del trattamento sia in grado di

farlo. 42) e nella misura in cui tale considerando si riferisce ai mezzi che possono essere ragionevolmente attuati sia dal responsabile del trattamento che da un'altra persona, la formulazione del responsabile del trattamento suggerisce che, affinché un dato possa essere qualificato come dato personale ...,

non è necessario che tutte le informazioni che consentono l'identificazione dell'interessato si trovino nelle mani di una persona interessata.

44. Questa giurisprudenza è stata confermata nella causa OC/Commissione europea (CGUE, Sesta Sezione, 7 marzo 2024, C-479/22). In quel caso, la CGUE ha affermato che il fatto che siano necessarie informazioni aggiuntive per identificare l'interessato non è in grado di escludere che i dati in questione possano essere qualificati come dati personali (par. 49), pur tenendo conto del fatto che la possibilità di combinare i dati in questione con informazioni aggiuntive costituisce un mezzo ragionevole per poter identificare l'interessato, tenendo conto di tutti i fattori oggettivi come il costo di tali informazioni (par. 50).

45. La CGUE afferma inoltre in tale sentenza che è inerente all'identificazione indiretta di una persona che ulteriori informazioni devono essere combinate con i dati in questione al fine di identificare la persona interessata (par. 55) e che il richiedente non era tenuto a fornire la prova di essere stato effettivamente identificato da una di tali persone, poiché tale condizione non è prevista dall'articolo 3, paragrafo 1, del regolamento 2018.

46. Infine, nella causa IAB Europe contro Gegevensbeschermingsautoriteit (CGUE, Quarta Sezione, 7 marzo 2024, C-604/22), la Corte ha dichiarato che l'articolo 4, paragrafo 1, del GDPR deve essere interpretato nel senso che una stringa composta da una combinazione di lettere e caratteri, come la TC String [Transpar and Consent String, contenente le preferenze degli utenti da parte dei fornitori di siti o applicazioni Internet e degli intermediari di tali dati e delle piattaforme pubblicitarie, costituisce un dato personale ai sensi di tale disposizione nella misura in cui, qualora possa, con mezzi ragionevoli, essere associata a un identificatore, come in particolare l'indirizzo IP del dispositivo di tale utente, consente di identificare l'interessato. . Aggiunge che il fatto che, senza un contributo esterno, un'organizzazione settoriale che detiene questa catena non possa accedere o avere accesso ai dati trattati dai suoi membri in base alle norme da essa stabilite o combinare tale catena con altri elementi non impedisce che la stessa catena costituisca un dato personale ai sensi di tale

disposizione (paragrafo 51).

47. Infine, a titolo di chiarimento, la formazione limitata ricorda che, nel parere 05/2014 sulle tecniche di anonimizzazione del 10 aprile 2014, il Gruppo di lavoro articolo 29 sulla protezione dei dati (di seguito G29), divenuto Comitato europeo per la protezione dei dati (di seguito PSAC), afferma che un processo può essere definito di anonimizzazione in particolare quando resiste ai seguenti tre tipi di rischi:

- individualizzazione, che corrisponde alla possibilità di isolare alcuni o tutti i record che identificano un individuo nel set di dati;

- la correlazione, che consiste nella possibilità di collegare almeno due record relativi alla stessa persona o a un gruppo di persone;

- inferenza, ovvero la possibilità di dedurre, con un alto grado di probabilità, il valore di un attributo dai valori di un insieme di altri attributi.

48. Se i dati non resistono ai tre tipi di rischio sopra menzionati, non saranno necessariamente qualificati come pseudonimi. Possono essere classificati come anonimi nel caso in cui il responsabile del trattamento sia in grado di dimostrare che la reidentificazione non è possibile con mezzi ragionevoli, vale a dire che i rischi di reidentificazione sono trascurabili.

49. Il relatore sostiene, alla luce dei vari elementi derivanti dalla giurisprudenza e dalla dottrina, che non vi è dubbio che il quadro giuridico applicabile consenta di valutare la natura anonima o pseudonima dei dati trattati e di stabilire che, su base costante, il monitoraggio delle persone nel tempo, mediante un identificatore unico, consente di isolare un individuo in un insieme di dati e quindi aumenta il rischio di revocare lo pseudonimo.

50. Al contrario, la società ritiene che il quadro legale, giurisprudenziale e dottrinale intorno alla questione dell'anonimizzazione dei dati sia una fonte di incertezza giuridica per gli operatori. Sottolinea la mancanza di chiarezza di questo quadro e l'assenza di parametri, metodologie o requisiti tecnici per dimostrare la natura anonima di un insieme di dati. Sostiene che le pubblicazioni, in particolare

la CNIL, il G29 e il GEPD non garantiscono il rispetto del principio di prevedibilità del diritto derivante dal requisito costituzionale della certezza del diritto in lingua francese, in quanto non presentano requisiti tecnici, in particolare requisiti tecnici, sufficientemente chiari da consentire agli operatori di garantire una ragionevole fiducia nei risultati dei processi di anonimizzazione utilizzati o di garantire l'ammissibilità della prova di La società avanza una serie di argomenti a sostegno della propria posizione.

51. In primo luogo, la società fa riferimento a una decisione emessa dal giudice del tribunale di Milano (Tribunale di Milano, ordinanza del 4 dicembre 2023), nell'ambito di una controversia tra l'autorità italiana per la protezione dei dati ..., che svolge un'attività simile a quella della società CEGEDIM SANTÉ nell'ambito dell'osservatorio. Secondo la società, il giudice ha ritenuto che, in quanto gli elementi degli elementi, l'autorità italiana non avesse dimostrato che i dati non fossero anonimi e che si dovesse procedere a una perizia indipendente per verificare la natura anonima dei dati, le possibilità di re-identificazione delle persone, nonché il rischio specifico di tale re-identificazione tenendo conto dei tempi e dei costi necessari.

52. In secondo luogo, l'azienda sostiene che si basa sull'accettazione probabilistica del concetto di dati personali, considerando che l'analisi del rischio di identificazione non deve necessariamente mirare a ridurre tale rischio a zero, ma piuttosto a ridurre tale rischio a un livello accettabile in termini di sensibilità dei dati, contesto e finalità del trattamento. Ha citato un documento congiunto dell'Autorità spagnola per la protezione dei dati e del GEPD pubblicato nel giugno 2021, nonché un articolo pubblicato e coautore del relatore CASTELLUCCIA nel 2020.

53. In terzo luogo, sostiene che il fatto che un insieme di dati possa essere collegato a un identificatore non esclude che tali dati possano essere anonimi, come quelli contenuti nel database OpenDamir di SNIIRAM. L'azienda ritiene che se i dati di OpenDamir, che per molti aspetti sono più precisi di quelli elaborati da CEGEDIM, possono essere anonimizzati, non è possibile che i dati

siano anonimi.

SALUTE, potrebbero essere considerati anonimi, devono anche essere considerati anonimi.

54. Infine, l'azienda sostiene che anche quando l'identificazione di un codice paziente viene combinata con le informazioni note sull'individuo ricercato nel flusso CROSSWAY non porta necessariamente alla re-identificazione. Infatti, sostiene che esiste solo una certa probabilità che le informazioni trovate nel database siano quelle della persona ricercata. Ritiene che molteplici incertezze vanifichino la possibilità di re-identificazione, ad esempio perché un individuo può condividere le caratteristiche note con altri individui o perché non è possibile sapere se la persona ricercata sia presente o meno nel database. L'azienda cita un estratto di una pubblicazione del Research Directorate, Evaluation and Statistics Studies (DREES).

55. In via preliminare, la formazione limitata sottolinea che, sebbene il CNIL abbia la facoltà di pubblicare linee guida, raccomandazioni o parametri di riferimento per facilitare la conformità del trattamento dei dati personali con i testi relativi alla protezione dei dati personali (ai sensi dell'articolo 8, paragrafo 2, lettera b), della legge sull'informatica e le libertà), le norme giuridiche sono stabilite dai legislatori francesi ed europei e interpretate dai tribunali competenti. Pertanto, anche se la CNIL non ha pubblicato parametri di riferimento o linee guida specifiche per i concetti di pseudonimizzazione e anonimizzazione, la formazione ristretta sottolinea che la CNIL ha pubblicato linee guida che rimangono pertinenti. La formazione limitata sottolinea che gli scritti prodotti sia dal relatore sia dalla società rivelano che questi concetti sono oggetto di numerose pubblicazioni, sia giurisprudenziali sia dottrinali. L'assenza di parametri di riferimento, linee guida o raccomandazioni della CNIL non può quindi essere sufficiente per ritenere che il quadro giuridico applicabile non sia chiaro.

56. Passando alla decisione del tribunale di Milano, il collegio ristretto osserva che il tribunale ha deciso di sospendere l'efficacia esecutiva della decisione del Garante italiano per la protezione dei dati personali solo per quanto riguarda la

sanzione accessoria della pubblicazione sul sito del Garante.

sito web della società e di trasmissione agli ordini e alle federazioni interessate, in attesa dello svolgimento di una perizia indipendente, al fine di determinare se i dati trattati dalla filiale italiana di CEGEDIM SANTÉ sono pseudonimizzati.

57. Il collegio ristretto ritiene che il giudice non sospenda la multa e l'ingiunzione. Né sostiene che i dati trattati siano anonimi. La formazione ristretta sottolinea a questo proposito che il Garante italiano per la protezione dei dati personali ha affermato nella sua decisione che i dati trattati sono dati personali, in particolare perché a ogni paziente viene assegnato un identificativo unico.

58. Per quanto riguarda la base OpenDamir a cui fa riferimento l'azienda, la formazione ristretta dimostra che i due trattamenti non sono comparabili, poiché in OpenDamir ogni riga corrisponde a un rimborso dell'assicurazione sanitaria e non a un paziente. Un file viene modificato ogni mese ed è impossibile seguire il percorso medico di uno stesso paziente nel tempo tramite OpenDamir. Al contrario, nel trattamento in questione, la società CEGEDIM SANTÉ è in grado di identificare che diversi file trasmessi successivamente dallo stesso medico riguardano lo stesso paziente.

59. Inoltre, per quanto riguarda lo studio della DREES citato dalla società, la formazione ristretta fa notare che esso specifica anche che un accumulo di somiglianze con una persona nota potrebbe, con la trasmissione delle annate, come base dell'arricchimento annuale della base, portare a una probabilità di identificazione vicina all'unità, il che corrisponde al modo in cui è stato effettuato il trattamento da parte di CEGlo stesso medico nel tempo e che la società dispone di una grande quantità di dati. Questo stesso studio del DREES indica chiaramente che la sostituzione dell'identificatore iniziale di una persona con un altro identificatore arbitrario è una pseudonimizzazione e non un'anonimizzazione. Pertanto, la formazione ristretta ritiene che la mobilitazione di questo studio del DREES da parte della società non sia rilevante in questo caso.

60. Infine, la formazione ristretta sottolinea il fatto che non si discute, né in giurisprudenza né in dottrina, sul fatto che l'attribuzione di un codice o di un

identificatore a

persone al fine di consentirne il monitoraggio consente la loro individualizzazione nell'insieme dei dati. Inoltre, è stato chiaramente stabilito che, nel valutare il rischio di creazione di pseudonimi, si deve tenere conto della possibilità di combinare un primo set di dati con altri dati, che possono essere in possesso di terzi. Altri dati includono, ad esempio, i dati di geolocalizzazione.

(b) La natura dei dati trattati

61. Per quanto riguarda i dati dei pazienti, il relatore osserva che dai documenti del fascicolo risulta che a ogni paziente viene assegnato un identificativo unico per lo stesso medico all'interno del flusso CROSSWAY. Questo numero, che non si basa su alcun tratto identitario, è collegato ai dati medici e amministrativi dello stesso paziente e consente quindi di seguire la storia del paziente per lo stesso medico. Il relatore ritiene quindi che, grazie all'identificativo del paziente comunicatogli, la società CEGEDIM SANTÉ sia in grado di identificare che diversi file trasmessi successivamente dallo stesso medico riguardano lo stesso paziente all'interno del suo osservatorio.

62. Il relatore conclude che:

- da un lato, questo metodo, che consiste nel sostituire i dati direttamente identificativi con identificativi indiretti, ossia un identificativo unico per il paziente in questione dello stesso medico, corrisponde perfettamente alla definizione di pseudonimizzazione e permette di avere un follow-up longitudinale del paziente;

- d'altra parte, poiché è possibile isolare un individuo nell'insieme dei dati e aumentare nel tempo tutti i dati che lo riguardano, i dati dei pazienti sono sufficientemente ricchi da consentire la rimozione dello pseudonimo con mezzi ragionevoli.

63. Nel contesto degli scambi contraddittori con la società, il relatore ha prodotto una dimostrazione a sostegno della sua analisi in cui riesce a tracciare con precisione il percorso di cura di un bambino di 12 anni affetto da ALD a partire da poche righe di dati trasmessi solo dall'azienda nell'ambito della

procedura di controllo.

64. Per quanto riguarda i dati dei medici, il relatore osserva che la società genera un numero di pannello dal numero di cliente del medico e che questo numero compare nei file generati dai medici panelisti, trasmessi a CEGEDIM SANTÉ. Il relatore osserva inoltre che la società dispone di una tabella di corrispondenza tra il numero del panel e l'identità del medico e conclude che la detenzione di questa tabella rende ancora più precisi i dati in possesso della società. Il relatore ritiene che la società sia in grado di identificare, tra tutti i panelisti, lo stesso medico che gli fornisce i file e che, pertanto, si tratti di dati pseudonimi.

65. In difesa, la società ritiene che i dati siano anonimi. Ritiene che la dimostrazione del relatore sia teorica e completamente incentrata sulle possibilità di individualizzare le persone a partire dai dati del flusso CROSSWAY; il relatore non cerca in alcun momento di valutare in modo accurato e oggettivo i rischi effettivi e residui di reidentificazione dei pazienti secondo i mezzi ragionevoli probabilmente utilizzati dalla società, compresi, in particolare, gli elementi specifici del contesto.

66. Tuttavia, la società sostiene che il carattere identificabile di una persona, che consente di considerare i dati come dati personali, non può essere affermato per postulato, ma deve essere convalidato da un'analisi concreta dei mezzi ragionevoli che consentono l'identificazione. Ritiene che le citate decisioni Breyer e OC/Commissione europea dimostrino che tali mezzi ragionevoli devono corrispondere a mezzi giuridici applicabili in pratica, tenendo conto in particolare di fattori oggettivi, quali il costo dell'identificazione e il tempo necessario per effettuarla, tenendo conto delle tecnologie disponibili al momento del trattamento. Aggiunge che, oltre all'analisi degli elementi specifici del contesto e alla quantificazione della possibilità di realizzarli alla luce dei fattori oggettivi (tempo, costo, manodopera, tecnologie disponibili), è necessario prendere in considerazione anche le motivazioni delle persone che possono effettuare la reidentificazione.

67. A sostegno delle sue dichiarazioni, l'azienda dovrà produrre una valutazione

esterna effettuata dall'azienda..., su mandato dell'azienda..., sui dati del

database ... alimentato dal flusso CROSSWAY. La valutazione conclude che i dati sono anonimi.

68. Infine, per quanto riguarda la tabella di corrispondenza in possesso della società, la Commissione sostiene che la tabella che identifica i codici e l'identità dei medici che partecipano all'osservatorio non può essere considerata un mezzo ragionevole che può essere utilizzato per aiutare la re-identificazione dei pazienti. La società sostiene infatti che la tabella di corrispondenza è gestita da un team dedicato e distinto da quello incaricato di far funzionare il flusso CROSSWAY, su una postazione informatica isolata, con una totale suddivisione delle informazioni e una perfetta saldatura dei ruoli e delle responsabilità tra questi due team.

69. In primo luogo, la formazione ristretta sottolinea che la natura pseudonima o anonima dei dati rappresenta una questione particolarmente importante per gli interessati, poiché, se i dati non sono personali, non si applicano le norme sulla protezione dei dati e quindi l'uso che se ne può fare è completamente libero. In particolare, una banca dati anonima non è soggetta agli obblighi di sicurezza di cui all'articolo 32 del GDPR e può essere liberamente comunicata o pubblicata. L'organismo che gestisce tale base non è vincolato da alcun obbligo di informazione.

70. In questo caso, per quanto riguarda i dati dei pazienti, la formazione limitata sottolinea che CEGEDIM HEALTH, all'epoca della CNIL e fino al 2022, ha raccolto dai medici panelisti un'ampia gamma di dati sia sulla cartella amministrativa dei pazienti, sia sulla cartella clinica, sulle prescrizioni farmaceutiche e su altre prescrizioni. La formazione limitata sottolinea che l'azienda ha indicato, dal 2022, di non raccogliere più informazioni sulla categoria socio-occupazionale, sulla situazione familiare e sul numero di figli. Anche il codice regionale era stato abolito e la società aveva indicato di aver impoverito le misure di taglia e peso.

71. La formazione ristretta sottolinea che, anche se a ciascun paziente vengono assegnati identificatori diversi nel flusso CROSSWAY e nei file trasmessi dai medici alla società CEGEDIM SANTÉ, tutti i dati relativi allo stesso paziente dello stesso medico rimangono associati a questo secondo identificatore nell'insieme dei dati comunicati alla società CEGEDIM SANTÉ. Pertanto, grazie all'identificativo del paziente che le è stato comunicato, la società CEGEDIM SANTÉ è in grado di associare allo stesso identificativo diversi file trasmessi successivamente dallo stesso medico e relativi allo stesso paziente, che la società non contesta, e quindi di avere la sua carriera in cura presso quel medico.

72. Pertanto, la formazione ristretta indica la possibilità di isolare un individuo nel set di dati, nella misura in cui l'identificatore unico consente di seguire i pazienti nel tempo. Pertanto, per sua natura, il trattamento non resiste al rischio di individualizzazione come descritto nell'Avviso 05/2014 sulle tecniche di anonimizzazione del 10 aprile 2014 di cui sopra.

73. Per quanto riguarda i dati dei medici, la formazione limitata ha rilevato che CEGEDIM SANTÉ è in grado di identificare, tra tutti gli esperti del medico e l'identificatore del medico, che lo stesso medico gli fornisce i file.

74. In secondo luogo, la formazione ristretta osserva che i dati raccolti sono particolarmente ricchi e la profondità dei dati importante: da un lato perché l'azienda elabora molti dati; dall'altro perché, sebbene l'azienda conservi i dati solo per tre mesi nel suo database, recupera i dati tramite il teleservizio HRi per una profondità di 12 mesi, che contengono informazioni sulla storia dei rimborsi sanitari effettuati dall'assicurazione sanitaria di un paziente. Questo set di dati particolarmente ricco e completo permette quindi alla società di tracciare i percorsi di cura delle persone negli ultimi dodici mesi, il che comporta un rischio ancora più elevato di sollevamento della pseudonimia.

75. Poiché i tre criteri stabiliti nel parere 05/2014 sulle tecniche di anonimizzazione, citato in precedenza, non sono soddisfatti, la formazione ristretta conclude che è

necessario valutare concretamente il rischio di reidentificazione per stabilire la natura anonima o pseudonima dei dati.

76. In questo senso, osserva che il relatore è riuscito, nell'ambito dei suoi scritti, a tracciare il percorso di un bambino di 12 anni nell'ALD a partire da una serie ridotta di dati trasmessi dalla società. Osserva che, per farlo, ha dedicato poco tempo e poche risorse: il relatore ha svolto un'analisi sulla base dei dati forniti dalla società utilizzando solo il software Excel e la nomenclatura da essa fornita per associare i codici alfanumerici alle informazioni sul paziente e sulle procedure mediche previste. In questo contesto, il relatore non ha utilizzato fonti di dati di terze parti, ad esempio i dati dei data broker (intermediari di dati) o i dati di geolocalizzazione. Tuttavia, la formazione ristretta osserva che dalla dottrina citata dal relatore nei suoi scritti emerge che è possibile re-identificare una percentuale significativa di persone in un insieme di dati pseudonimizzati basati su dati di geolocalizzazione (si vedano in particolare gli studi Unique in the Shopping Mall: On the Re- identifiability of Credit Card Metadata di Yves-Alexandre de MONTJOYE o GeoTrouveT).

77. La formazione ristretta osserva quindi che una correlazione tra i dati di terzi e le informazioni in possesso di CEGEDIM SANTÉ (compresi i dati dei pazienti e le informazioni relative alle sue consultazioni) aumenterebbe notevolmente le possibilità di eliminare gli pseudonimi. Sebbene l'azienda contesti il possesso di informazioni geografiche, la formazione ristretta sottolinea che è stato raccolto un codice regionale fino al 2022 e che dispone anche di una tabella di corrispondenza tra i numeri di pannello dei medici e la loro identità.

78. L'azienda contesta anche la possibilità di utilizzare dati di terzi per valutare l'anonimato o meno di un insieme di dati. Tuttavia, la formazione ristretta ricorda a questo proposito che la CGUE ha affermato che, per qualificare le informazioni sui dati personali, non è necessario che queste informazioni da sole identifichino la persona interessata. La Commissione ha inoltre ritenuto che il fatto che ulteriori

informazioni, compresi i contributi esterni, non è possibile escludere l'interessato dal fatto che i dati in questione possano essere qualificati come dati personali (sentenze OC/Commissione europea, paragrafi 47 e 55, e IAB Europe/Gegevensbeschermingsautoriteit , par. 51, citate in precedenza).

79. La formazione ristretta sottolinea in ogni caso che se il relatore è riuscito a isolare un individuo e a seguire una parte della sua cura con un tale livello di dettaglio, solo a partire da un estratto notevolmente più ricco di un insieme di dati, e per di più senza ricorrere a informazioni aggiuntive, allora può essere possibile rimuovere lo pseudonimo degli individui con mezzi ragionevoli. La formazione ristretta in questo senso rispecchia la ricchezza dei dati in possesso dell'azienda: ha ricevuto più di ... righe tra il 1° gennaio 2021 e il 2 aprile 2021 (una riga corrisponde a un evento, per esempio una consultazione), ha detenuto ... codici paziente per il periodo da gennaio a marzo 2021 e ... codici preambolo nell'aprile 2021.

80. Inoltre, se il relatore non ha specificamente revocato lo pseudonimo del bambino di cui ha seguito parte del percorso di cura, la formazione limitata sottolinea che questa condizione non è necessaria per la qualificazione dei dati personali. Infatti, la CGUE ha affermato nella causa OC/Commissione che non è necessario fornire la prova di un'identificazione effettiva, poiché tale condizione non è prevista dall'articolo 3, paragrafo 1, del regolamento 2018/1725, che si limita a richiedere l'identificazione di una persona (paragrafo 61). La formazione ristretta ritiene che sia opportuno ragionare per analogia rispetto al GDPR, poiché la definizione di cui all'articolo 4, paragrafo 1, del GDPR è esattamente la stessa.

81. In terzo luogo, la formazione ristretta sottolinea che quando i tre criteri stabiliti nel citato parere del G29 non sono soddisfatti, la società deve effettuare un'analisi per poter dimostrare che il rischio di re-identificazione indotto dal processo è trascurabile. Tuttavia, l'azienda non ha effettuato tale analisi per quanto riguarda i risultati ottenuti al momento del controllo della CNIL. Solo nell'ottobre 2023 l'azienda ha dichiarato di aver effettuato una tale analisi, che

quindi applicato solo al trattamento dei dati dopo il 2022. Inoltre, per valutare i rischi di re-identificazione, la formazione limitata osserva che la società ha scelto di combinare solo un numero ridotto di dati tra quelli a sua disposizione, rendendo così il risultato del suo studio non sufficientemente affidabile (in questo caso, ha scelto di combinare nella sua valutazione solo l'anno di nascita del paziente, il suo sesso e l'informazione che abbia o meno figli, mentre al momento della sua esperienza, mentre al momento della sua età, costanti fisiologiche (glicemia, tensione, ecc.) e patologie diagnosticate).

82. Per quanto riguarda le conclusioni della valutazione effettuata dalla società, fornite in sede di contraddittorio, la formazione ristretta ritiene che esse non mettano in discussione tale valutazione. Infatti, la valutazione non riguarda il trattamento registrato il giorno del controllo, ma solo quello effettuato successivamente, che prevede nuove misure, consistenti in particolare nell'esaurimento della profondità dei dati trattati. Pertanto, la valutazione non consente di dimostrare l'anonimato dei dati il giorno del controllo.

83. In ogni caso, la formazione ristretta osserva che la perizia della società non include, nella sua valutazione, la robustezza delle tecniche di de-identificazione... e i risultati ottenuti per quanto riguarda l'anonimato dei set di dati, tutti fattori che permettono di rappresentare la ricchezza dei dati come risulta dal follow-up per diversi anni delle stesse persone.

84. Infine, ma non meno importante, la formazione ristretta osserva che la perizia della società giunge alla stessa conclusione del relatore per quanto riguarda la possibilità di isolare un individuo dalla base di dati di proprietà di CEGEDIM SANTÉ, la perizia porta anche alla conclusione che il k-anonimato è uguale a 1, ossia è possibile isolare un individuo nella base di dati. La k-anonimità è infatti un modello di misurazione della riservatezza che garantisce che per ogni identificatore all'interno di un insieme di dati esista una classe di equivalenza corrispondente contenente almeno K registrazioni. La formazione ristretta rileva quindi che, sebbene la perizia ... non concluda che la

possibilità di re-identificazione delle persone, conclude che è possibile isolare un individuo nell'insieme dei dati, il che corrisponde già al primo dei tre tipi di rischio individuati dal G29 nel suo parere 05/2014 sulle tecniche di anonimizzazione del 10 aprile 2014 sopra citato.

85. La seconda fase della perizia consiste nell'effettuare un'analisi dei rischi per verificare la probabilità che i dati in possesso della società siano resi accessibili, ad esempio, in caso di violazione dei dati, a persone che possano collegare questi dati all'identità esatta dei pazienti. La formazione ristretta evidenzia l'elevato livello di sicurezza promosso dalla società. D'altra parte, conclude che l'esercizio è il rischio di accesso ai dati e la probabilità di una violazione dei dati. Tuttavia, il livello di sicurezza in atto per garantire la riservatezza dei dati, per quanto elevato, non influisce sulla qualificazione dei dati trattati.

86. Da tutto ciò si evince che, il giorno del controllo e fino al 2022, i dati direttamente identificativi sono stati sostituiti da identificativi indiretti, ossia un identificativo unico per il paziente in questione, che ha permesso di trattare i suoi dati senza poterlo identificare direttamente. Ciononostante, lo pseudonimato potrebbe essere rimosso, vista l'importanza del patrimonio di informazioni.

87. Di conseguenza, la formazione ristretta ritiene che i dati trattati dalla società CEGEDIM SANTÉ fino al 2022 siano pseudonimi e non anonimi.

88. La formazione ristretta prende atto delle misure complementari messe in atto dall'azienda a partire dal 2022, vale a dire che non raccoglie più alcuni dati e che, per altri, non raccoglie più lo stesso livello di granularità. L'azienda ritiene che il suo trattamento sia così alterato e anonimo. Tuttavia, la formazione ristretta ritiene che l'analisi del nuovo stato di trattamento non fosse l'oggetto iniziale del procedimento e non è in grado di pronunciarsi su questo punto nel contesto della presente decisione. Invita l'azienda, se lo desidera, a inoltrare una richiesta di consulenza

alla CNIL di decidere sulla natura anonima o non anonima della banca dati nel suo nuovo stato.

(2) La qualificazione del trattamento in un magazzino di dati sanitari

89. La società sostiene che il trattamento che attua non è un magazzino di dati sanitari, ma una rete di medici che accettano di trasmettere dati anonimi delle loro cartelle cliniche ai partner di CEGEDIM SANTÉ, ossia le società ... e .... In particolare, la Commissione ritiene che la natura transitoria del flusso, in cui i dati sono conservati per soli tre mesi, dimostri che non si tratta di una banca dati perenne come un magazzino.

90. La formazione ristretta sottolinea che il concetto di deposito di dati sanitari non è contenuto nella legge sull'informatica e le libertà, ma costituisce una costruzione dottrinale della CNIL per l'applicazione degli articoli 65 e seguenti di tale legge. Viene valutato in base a un insieme di indici che tengono conto, ma non solo, del periodo di conservazione dei dati. I fattori determinanti per la qualificazione di un data warehouse sanitario includono il riutilizzo dei dati in trattamenti successivi, l'alimentazione dell'acqua dalla base e le finalità del trattamento.

91. Nel caso di specie, la formazione ristretta osserva che dai documenti del fascicolo risulta che CEGEDIM SANTÉ:

- raccogliere massicciamente dati sanitari da pazienti e medici (più di ... righe ricevute nel database tra il 1° gennaio 2021 e il 2 aprile 2021 - una riga corrispondente a un evento, ad esempio una consultazione; ... codici paziente detenuti nel periodo da gennaio a marzo 2021; ... codici prescrittivi detenuti ad aprile 2021;

- alimenta la sua base nel tempo, per ottenere un grande volume di dati (dati aggiornati quotidianamente dalle postazioni dei medici);

- mette i dati a disposizione dei propri clienti che effettuano studi e statistiche nel campo della salute. Tra questi clienti c'è la società...

92. La formazione ristretta prende atto delle modifiche sostanziali ed effettive del trattamento a partire dal 1° giugno 2024. In particolare, il riscontro dalla postazione del medico all'azienda non avviene più attraverso la società CEGEDIM SANTÉ. Dalla fine di luglio 2024, CEGEDIM SANTÉ non è più coinvolta nella gestione del flusso CROSSWAY dal software dei medici, che alimenta direttamente il sito aziendale .....

93. Alla luce di quanto sopra, la formazione ristretta ritiene che la società costituisse un deposito di dati sanitari al momento del controllo da parte della CNIL, fino all'effettiva riorganizzazione del 1° giugno 2024 con la quale i dati non passeranno più attraverso CEGEDIM HEALTH.

3) Sullo stato dell'azienda in termini di responsabilità per il trattamento

94. Ai sensi dell'articolo 4 del GDPR, il responsabile del trattamento è 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 (punto 7) e il subappaltatore è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta i dati personali per conto del responsabile del trattamento (punto 8).

95. A titolo di chiarimento, nelle linee guida 07/2020 sui concetti di responsabile e incaricato del trattamento nel GDPR, adottate il 7 luglio 2021, il GEPD spiega la definizione di responsabile del trattamento in questi termini: La determinazione delle finalità e dei mezzi equivale a decidere rispettivamente il "perché" e il "come" del trattamento: per un determinato trattamento, il responsabile del trattamento è l'attore che ha determinato lo scopo per il quale) e il modo in cui tale obiettivo sarà raggiunto (ossia quali mezzi devono essere attuati per raggiungere l'obiettivo). Una persona fisica o giuridica che esercita tale influenza sul trattamento dei dati personali partecipa quindi alla determinazione delle finalità e dei mezzi del trattamento in questione, secondo la definizione di cui all'articolo 4, paragrafo 7, del GDPR. Il responsabile del trattamento deve decidere sia le finalità che i mezzi del trattamento. (35 e 36).

96. Per quanto riguarda il subappalto, le suddette linee guida affermano che l'articolo 4, paragrafo 8, del GDPR definisce un subappaltatore come la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che tratta dati personali per conto del responsabile del trattamento e che, per essere considerato un subappaltatore, devono essere soddisfatte due condizioni fondamentali:

(a) essere un'entità separata dal controllore e

(b) trattare i dati personali per conto del responsabile del trattamento (paragrafi 73 e 76).

97. Il relatore ritiene che CEGEDIM SANTÉ definisca le finalità e i mezzi del trattamento in questione e costituisca un archivio di dati sanitari ai fini della propria attività, mettendo poi i dati a disposizione dei propri clienti che li utilizzano per studi e statistiche nel campo della salute.

98. In difesa, la società indica di agire come subappaltatore, da un lato, dei medici che utilizzano il software CROSSWAY e, dall'altro, delle società ... e ... per le quali gestisce il flusso CROSSWAY. Sostiene che la determinazione delle finalità e dei mezzi di trattamento invocata dal relatore si applica solo alla gestione e al reclutamento di un panel di medici da parte della società CEGEDIM SANTÉ, e non all'ottenimento dei dati dei pazienti di quest'ultima. Pertanto, non supporta l'utilizzo dei dati provenienti da questo flusso e non supporta l'utilizzo dei dati provenienti da questo flusso e limita il suo intervento a un ruolo di intermediario tecnico per il riscontro del flusso CROSSWAY dalla postazione del medico alle aziende partner.

99. A sostegno delle sue affermazioni, la società cita una lettera di stretto controllo del 26 novembre 2014 nei confronti della società CEGEDIM L SOFTWARE MEDICAUX FRANCE (sciolta nel 2021 e la cui intera attività è stata rilevata dalla società CEGEDIM SANTÉ) in cui la CNIL avrebbe concesso alla società questo status di subappaltatore. Ritiene che la presente lettera trovi ancora applicazione nella misura in cui le circostanze di fatto e di diritto applicabili

alla classificazione delle parti non sono cambiati e che la lettera costituisce un atto validamente adottato da una persona che ha l'autorità di rappresentare e vincolare la CNIL, ossia il presidente della Commissione. Inoltre, sostiene che l'età della posta non può essere un argomento valido, poiché la comprensione del concetto di anonimato non è stata sostanzialmente modificata dal GDPR o dalla legge sulle tecnologie dell'informazione e le libertà da allora.

100. In primo luogo, la formazione ristretta sottolinea che, nella sua valutazione d'impatto, la società si è autonominata responsabile del controllo del suo osservatorio e non solo del reclutamento del gruppo di medici. Dai documenti del fascicolo emerge inoltre che la società CEGEDIM SANTÉ è responsabile della raccolta dei dati dei medici idonei che desiderano aderire al suo osservatorio epidemiologico tramite contratti, e definisce anche le modalità di trasmissione di questi dati ai suoi partner [....

101. Per quanto riguarda le finalità del trattamento, la formazione ristretta osserva che la società determina l'ambito e le finalità dell'utilizzo dei dati del suo osservatorio nei confronti dei suoi partner. In particolare, il contratto stipulato con la società ... stabilisce che l'uso autorizzato dei dati è il seguente: analisi o studi sulla salute, diretti o tramite interposta persona, e la modifica del contratto stipulato con la società ... prevede, tra l'altro, che essa utilizzerà i dati relativi alle prescrizioni mediche trasmessi dal CLM [CEGEDIM SANTÉ] solo per realizzare studi. I risultati degli studi saranno commercializzati solo come statistiche. È vietata qualsiasi altra forma di commercializzazione dei dati (traduzione libera). Inoltre, l'azienda definisce il perimetro dei partecipanti all'osservatorio proponendo l'adesione e l'utilizzo del software CROSSWAY a un panel rappresentativo di medici cittadini, eleggibili secondo criteri geografici, di età e di specialità.

102. Per quanto riguarda i mezzi di trattamento, la formazione ristretta sottolinea che i contratti stipulati tra l'azienda e i medici panellisti non riguardano solo il mero reclutamento dei medici, ma dettagliano anche i mezzi di trattamento, comprese le modalità di raccolta e trasmissione dei dati. Come progettato,

I contratti impongono, ad esempio, ai medici le condizioni per la partecipazione alla rete e per la trasmissione dei dati alla società, in particolare per quanto riguarda le categorie di dati raccolti, le modalità di comunicazione dei dati e la frequenza della loro raccolta.

103. La formazione ristretta ritiene che dai documenti del fascicolo risulti che CEGEDIM SANTÉ determina le finalità e i mezzi del trattamento in questione, che organizza il trattamento per soddisfare le proprie esigenze e per attuare il proprio osservatorio e che non riceve una direttiva da eseguire.

104. La formazione ristretta specifica che la trasmissione dei dati a partner terzi, che riutilizzeranno i dati per proprio conto, non preclude la qualificazione della società CEGEDIM SANTÉ. In caso di trattamento a catena, ogni azienda agisce come responsabile del trattamento, determinando le modalità di trattamento per le proprie finalità.

105. In secondo luogo, la formazione ristretta ritiene che il trattamento possa essere valutato solo tenendo conto delle conclusioni della missione di monitoraggio del 30 marzo 2021 e alla luce della dottrina attuale e dello stato dell'arte. La formazione ristretta non si ritiene vincolata dalle conclusioni della missione di monitoraggio del 2012.

106. La formazione limitata rileva innanzitutto che il diritto alla protezione dei dati personali ha subito un'evoluzione significativa dalla chiusura della lettera di controllo inviata alla società CEGEDIM LAWINABLE MEDICALS FRANCE nel 2014, che faceva seguito alle missioni di verifica effettuate nel 2001 e nel marzo 2012. Questa lettera è anche precedente all'entrata in vigore del GDPR, testo di riferimento sulla protezione dei dati personali. L'evoluzione della dottrina si esprime in particolare nella terminologia utilizzata, con la menzione dell'anonimato del paziente, in un'epoca in cui il concetto di anonimato si riferiva all'assenza di dati direttamente identificabili e non all'impossibilità di identificare una persona fisica da un insieme di dati.

107. La formazione ristretta osserva poi che da questa lettera non risulta che la CNIL abbia ritenuto, in relazione alle sue missioni di verifica del 2002 e del 2014, che si trattasse di un trattamento di dati anonimizzati al di fuori del campo di applicazione della legge sull'informatica e le libertà. Se così fosse stato, non avrebbe elencato nella sua lettera di chiusura una serie di raccomandazioni da attuare per garantire la sicurezza dei dati trattati. Tuttavia, la lettera invitava l'azienda, in particolare, a implementare un meccanismo di cancellazione automatica dei file conservati sui posti dei medici o a designare un corrispondente per l'informatica e le libertà.

108. In ogni caso, la formazione ristretta sottolinea che è responsabilità del responsabile del trattamento tenere conto degli sviluppi dottrinali e rivalutare regolarmente le misure tecniche e organizzative del trattamento attuato.

109. In conclusione, la formazione ristretta non mette in discussione la validità della lettera del 2014 ma, tenendo conto della sua anzianità e dell'evoluzione del quadro giuridico e giurisprudenziale, ritiene di non essere legata a questa vecchia posizione, posizione che a sua volta si basa su una delibera della CNIL risalente a più di vent'anni fa e sulle relative osservazioni. La formazione ristretta ritiene che questa lettera da sola non possa dimostrare lo status di subappaltatore di CEGEDIM SANTÉ.

110. Alla luce di tutto ciò, la formazione ristretta ritiene che CEGEDIM SANTÉ sia responsabile del trattamento ai sensi dell'articolo 4, paragrafo 7, del GDPR. Pertanto, attuando il trattamento in questione, la società, se raccoglie e tratta dati personali in qualità di responsabile del trattamento, deve rispettare la normativa sulla protezione dei dati personali.

C. Sulla mancata osservanza dell'articolo 66 della Legge sulle tecnologie e le libertà dell'informazione

111. L'articolo 65 della legge sulle tecnologie dell'informazione e le libertà prevede che i trattamenti contenenti dati relativi alla salute delle persone siano soggetti alla sezione 3:

Trattamento dei dati personali nel campo della salute di cui al Capitolo III: Obblighi del responsabile del trattamento e del subappaltatore, ad eccezione delle diverse categorie di trattamento, elencate nei paragrafi da 1 a 6 del presente articolo.

112. L'articolo 66 della legge sulle tecnologie dell'informazione e le libertà prevede quanto segue:

I - I trattamenti di cui alla presente sezione possono essere effettuati solo alla luce della finalità di interesse pubblico che presentano. Garantire elevati standard di qualità e sicurezza dell'assistenza sanitaria e dei farmaci o dispositivi medici è un interesse pubblico.

II - I modelli di repertorio e di regolamento, ai sensi dell'articolo 8 (I) 2 (c), applicabili ai trattamenti di cui alla presente sezione sono stabiliti dalla Commissione nazionale dell'informatica e delle libertà, in consultazione con la piattaforma di dati sanitari di cui all'articolo L. 1462-1 del Codice della sanità pubblica e con gli organismi pubblici e privati rappresentativi degli attori interessati.

Il trattamento conforme a questi archivi può essere attuato a condizione che i loro funzionari inviino una dichiarazione di conformità prima della Commissione nazionale per l'informatica e le libertà. ...

III - I trattamenti di cui al punto I che non sono conformi a un sistema di riferimento di cui al punto II possono essere attuati solo previa autorizzazione della Commissione nazionale per l'informatica e le libertà. La domanda di autorizzazione deve essere presentata nella forma prevista all'articolo 33. . . .

113. Pertanto, ai sensi dell'articolo 66 III della legge sull'informatica e le libertà, il trattamento dei dati personali nel settore della salute, compresi i magazzini di dati sanitari, può essere attuato solo previa autorizzazione della CNIL o a condizione che sia conforme a un sistema di riferimento di cui all'articolo II, alla luce dell'interesse pubblico che presentano.

114. Il relatore ritiene che l'azienda raccolga dati pseudonimizzati dalle cartelle cliniche informatizzate dei pazienti, trasmesse dai medici del panel tramite il flusso CROSSWAY, al fine di creare questo magazzino di dati sanitari. In assenza del consenso degli interessati al versamento dei loro dati in un deposito di dati sanitari (ai sensi dell'articolo 9, paragrafo 2, lettera a), del GDPR), la creazione di tale deposito è soggetta a formalità preliminari presso la CNIL. Tuttavia, il relatore sottolinea che CEGEDIM SANTÉ non ha ottenuto il consenso esplicito delle persone interessate dalla raccolta, dalla registrazione e dalla conservazione dei dati sanitari inclusi nel deposito, non ha presentato alcuna domanda di autorizzazione per il trattamento in questione e non ha presentato alla CNIL alcuna dichiarazione che attesti la conformità del trattamento a un sistema di riferimento ai sensi dell'articolo 66, paragrafo II, della legge sull'informatica e le libertà. Il relatore conclude che l'azienda non ha rispettato gli obblighi previsti dall'articolo 66 della legge sull'informazione e le libertà nel campo della salute.

115. In difesa, la società sostiene che non sussiste una violazione dell'articolo 66 della legge sulle tecnologie dell'informazione e le libertà in quanto non tratta dati personali, compresi dati pseudonimi o dati sanitari. Sostiene che il flusso CROSSWAY contiene solo dati anonimi e che pertanto non costituisce un archivio di dati sanitari e non deve espletare le formalità previste dall'articolo 66 della legge sulle tecnologie dell'informazione e le libertà per poter trattare tali dati.

116. Inoltre, ritiene che non le si possa imputare di aver disatteso i propri obblighi in quanto il quadro giuridico applicabile, in particolare la definizione del concetto di anonimizzazione, manca di chiarezza. In particolare, la società sostiene che non le si può rimproverare di non aver presentato una richiesta di consulenza alla CNIL, in quanto quest'ultima non ha mai menzionato la possibilità per gli organismi di richiedere i metodi di anonimizzazione utilizzati e che, in ogni caso, ha ritenuto, in buona fede, che i dati trattati fossero anonimi.

117. In via preliminare, la formazione ristretta rileva che la CNIL ha effettuato alcune pubblicazioni sul proprio sito web prima del monitoraggio, ad esempio sulla definizione di dato sanitario (inizio 2018), sulle formalità da espletare per il trattamento dei dati sanitari (inizio 2018) o sulla distinzione tra un deposito di dati sanitari e una ricerca (fine 2019). Oltre alle proprie risorse, il CNIL trasmette altre fonti di informazione, come ha fatto, ad esempio, con il parere 05/2014 sulle tecniche di anonimizzazione del G29. Come già sottolineato, la formazione ristretta ricorda anche che il quadro giuridico è stabilito principalmente dal legislatore francese ed europeo.

118. Di conseguenza, la formazione ristretta ritiene che la società non potesse ignorare, il giorno del controllo, il regime giuridico applicabile al deposito di dati sanitari che sta costituendo, tanto più che altre società che effettuano trattamenti analoghi nello stesso mercato hanno richiesto autorizzazioni alla CNIL e che tali autorizzazioni sono pubbliche e accessibili sul sito www.legifrance.gouv.fr . Se l'azienda ritiene che tali autorizzazioni non siano paragonabili alla banca dati che sta costituendo, in particolare in relazione alla ricchezza dei dati raccolti da tali aziende, la formazione ristretta ricorda che, una volta che un'organizzazione costituisce un magazzino per se stessa, è tenuta a rispettare i suoi obblighi e in particolare l'articolo 66 della legge sull'informatica e le libertà, indipendentemente dalla ricchezza del magazzino e dalla granularità dei dati raccolti.

119. La formazione ristretta sottolinea che, per i motivi sopra esposti, CEGEDIM HEALTHY trattava, il giorno del controllo, dati sanitari in modo pseudonimizzato per costituire un magazzino di dati sanitari, per cui era tenuta a rispettare il GDPR e la legge sull'informatica e le libertà.

120. In primo luogo, la formazione ristretta osserva che l'unica eccezione prevista dagli obblighi di cui all'articolo 65 di tale legge che può applicarsi al caso di specie è quella in cui la persona interessata abbia dato il proprio consenso esplicito al trattamento

dei suoi dati personali per una o più finalità specifiche, ai sensi dell'articolo 65, paragrafo 1, con riferimento all'articolo 9, paragrafo 2, lettera a), del GDPR. Tuttavia, nel caso in questione, poiché CEGEDIM SANTÉ ritiene di non trattare dati personali, non ha attuato alcuna misura per conformarsi alle norme applicabili sul trattamento di tali dati. In particolare, l'azienda non ha implementato alcun meccanismo di raccolta del consenso esplicito e preventivo dei pazienti dei medici del panel per il trattamento in questione.

121. Di conseguenza, la formazione ristretta ritiene che, poiché la società ha trattato dati relativi alla salute nel giorno del controllo e non può avvalersi di nessuna delle eccezioni previste dall'articolo 65 della legge sull'informatica e le libertà, il trattamento che attua è soggetto alla sezione 3 del capitolo III della legge sull'informatica e le libertà.

122. In secondo luogo, la formazione ristretta sottolinea che, nel caso in questione, l'azienda non ha rispettato i requisiti dell'articolo 66 della legge sulle tecnologie dell'informazione e le libertà per creare un magazzino di dati sanitari.

123. In primo luogo, rileva che l'azienda non ha richiesto l'autorizzazione per garantire che il trattamento in questione sia considerato necessario per motivi di interesse pubblico nel campo della salute pubblica o necessario ai fini della ricerca scientifica.

124. In secondo luogo, la formazione ristretta sottolinea che, in assenza di un'autorizzazione della CNIL, il trattamento dei dati personali nel campo della salute può essere effettuato anche se è conforme a un sistema di riferimento ai sensi dell'articolo 66 della legge sull'informatica e le libertà, a condizione che il responsabile del trattamento invii una dichiarazione di conformità alla CNIL prima che quest'ultima attesti tale conformità. La formazione ristretta osserva che ciò non avviene nel caso in questione e che la società non ha presentato alcuna dichiarazione di tale conformità alla CNIL.

125. In terzo luogo, la formazione ristretta prende atto delle nuove misure attuate dopo il controllo.

126. Da un lato, la società ha indicato di non aver più raccolto alcuni dati dal 2022. Tuttavia, come spiegato in precedenza, la formazione ristretta ritiene che gli elementi comunicati dalla società nel corso del procedimento non le consentano di garantire che ora tratta dati anonimi. Rileva inoltre, in ogni caso, che le misure previste nel 2022 non possono esimere la società dalla responsabilità per il passato.

127. D'altra parte, la società ha comunicato che, a partire dalla fine di luglio 2024, non interverrà più nella gestione del flusso CROSSWAY, che ora alimenta direttamente la propria base. Pertanto, i dati del flusso CROSSWAY non passano più attraverso la società CEGEDIM SANTÉ.

128. Alla luce di tutto ciò, la formazione ristretta ritiene che la società abbia trattato dati sanitari il giorno del controllo e fino al luglio 2024 e che avrebbe dovuto soddisfare i requisiti dell'articolo 66 della legge del 6 gennaio 1978, e successive modifiche, al fine di istituire un magazzino di dati sanitari.

129. Di conseguenza, la formazione ristretta ritiene che l'azienda non abbia rispettato i suoi obblighi trattando dati personali nel campo della salute in violazione dell'articolo 66 della legge del 6 gennaio 1978, come modificata.

130. Alla luce delle misure adottate dalla società nel corso del procedimento, la formazione ristretta ritiene che non sia necessario emettere un'ordinanza per l'adeguamento alle disposizioni del suddetto articolo 66, come proposto dal relatore, poiché la società non è più coinvolta nella gestione del flusso CROSSWAY.

D. In caso di mancato rispetto dell'articolo 5, paragrafo 1, lettera a), del GDPR

131. Ai sensi dell'articolo 5, paragrafo 1, lettera a), del GDPR, i dati personali devono essere:

(a) trattati in modo lecito, equo e trasparente nei confronti della persona interessata (licenza, lealtà, trasparenza) .

132. L'articolo L. 162-4-3 del Codice della sicurezza sociale prevede che i medici possano, nel corso delle cure prestate e alle condizioni previste dall'articolo L. 161-31, consultare i dati risultanti dalle procedure di rimborso o di cura in possesso dell'ente a cui appartiene ciascun beneficiario dell'assicurazione sanitaria. In questo caso, informano preventivamente il paziente. L'assistito acconsente a tale accesso consentendo al medico di utilizzare, a tal fine, i mezzi elettronici di identificazione di cui all'articolo L. 161-31. Il registro dei dati messi a disposizione del medico contiene le informazioni necessarie per l'identificazione degli atti, dei prodotti o dei servizi oggetto delle cure prestate in città o in una struttura sanitaria, in particolare per quanto riguarda gli elenchi di cui agli articoli L. 162-1-7, L. 165-1 e L. 162-17. Il registro contiene anche il codice previsto per l'identificazione del paziente. Include anche il codice previsto per l'identificazione in questi elenchi, il livello di assistenza e, per i pazienti affetti da patologie di lunga durata, gli elementi costitutivi del protocollo sanitario di cui al settimo comma dell'articolo L. 324-1. . . .

133. L'articolo R. 162-1-10 dello stesso codice prevede che ai fini dell'articolo L. 162-4-3, gli enti che gestiscono i regimi di assicurazione sanitaria di base dovranno, per l'utilizzo di medici autorizzati o che lavorano in uno stabilimento o in un centro sanitario, nel corso dell'assistenza che forniscono, l'attuazione di un servizio di consultazione elettronica delle informazioni relative ai servizi forniti ai loro beneficiari.

134. Per l'attuazione di queste disposizioni, l'assicurazione sanitaria ha istituito, in particolare, due teleservizi:

- il teleservizio HRi: informazioni sulla storia dei rimborsi delle assicurazioni sanitarie di un paziente negli ultimi 12 mesi;

- Teleservizio ALDi: dati sulla malattia di lunga durata (ALD) riconosciuta dall'assicurazione sanitaria del paziente (compresa la data di consultazione, il

codice ALD, le date di inizio e fine della ALD e l'informazione che la ALD è coperta).

135. Nel caso in esame, la delegazione di vigilanza ha rilevato che i dati trasmessi dal flusso CROSSWAY alla società CEGEDIM SANTÉ sono dati provenienti da questi due servizi di telecomunicazione.

136. La delegazione è stata inoltre informata che le informazioni trasmesse a CEGEDIM SANTÉ attraverso il flusso CROSSWAY possono essere basate sull'interrogazione di servizi telematici o essere state fornite direttamente dai medici.

137. Il relatore sostiene che le disposizioni del Codice di previdenza sociale e del Codice di sanità pubblica prevedono solo il diritto di consultare i dati contenuti nei teleservizi introdotti dalla Cassa nazionale di assicurazione malattia (CNAM) da parte di professionisti autorizzati. Non prevedono la possibilità per un attore privato, attraverso il medico, di raccogliere questi dati direttamente dai teleservizi. Il relatore ritiene che la raccolta di tali dati da parte di CEGEDIM HEALTH sia illegittima ed effettuata in violazione dell'articolo 5, paragrafo 1, lettera a), del GDPR.

1) Sui dati di ALDi teleservice

138. La formazione ristretta sottolinea che le disposizioni del Codice della sicurezza sociale disciplinano solo le modalità di accesso diretto ai dati personali risultanti dal servizio di teleassistenza ALDi, ma non prescrivono l'accesso a questi stessi dati dalle cartelle informatizzate dei medici. La CNIL ha inoltre autorizzato in passato estrazioni pseudonimizzate di cartelle cliniche, per la creazione di banche dati sulla salute, senza escludere in linea di principio il fatto che i dati delle banche dati originariamente derivanti dalle basi dell'assicurazione sanitaria siano importati in queste banche dati, a condizione che il trattamento sia proporzionato e sufficientemente sicuro, e che siano rispettate le altre regole per il trattamento dei dati personali. In queste circostanze, la formazione ristretta ritiene che, come sostiene l'azienda, sia autorizzata a ricevere nel feed CROSSWAY i dati provenienti da ALDi teleservice nella misura in cui questi sono inclusi nella cartella informatizzata del medico stesso, allo stesso modo degli altri dati ivi registrati.

139. Tuttavia, dai documenti del fascicolo risulta che l'unico scopo dell'estrattore CROSSWAY è quello di consentire l'estrazione dei dati dalle cartelle cliniche informatizzate, ma non effettua alcun collegamento con il servizio di teleassistenza e non aspira i dati direttamente da esse. In particolare, la società sostiene che il medico può, in un primo momento, consultare i dati dal servizio remoto ALDi senza scaricarli e, in un secondo momento, decidere di scaricare questi dati e inserirli nella cartella clinica informatizzata del software CROSSWAY.

140. La formazione ristretta prende atto delle informazioni fornite dall'azienda e ritiene che il mancato rispetto dell'articolo 5, paragrafo 1, lettera a), del GDPR non si configuri nel caso della raccolta dei dati da parte del telesoccorso ALDi.

2) Sui dati del teleservizio HRi

141. Per quanto riguarda i dati provenienti dal servizio di telesoccorso HRi, la società sostiene in difesa che le disposizioni del Codice di sicurezza sociale non prevedono norme che prescrivano o vietino l'accesso alle cartelle informatizzate dei medici contenenti dati provenienti dal servizio di telesoccorso HRi, inoltre quando tale accesso riguarda solo dati anonimi. Pertanto, l'azienda ritiene di poter ricevere questi dati nel feed CROSSWAY, allo stesso modo degli altri dati contenuti nelle cartelle cliniche.

142. In particolare, l'azienda sostiene che i dati provenienti dal teleservizio HRi vengono registrati nel CROSSWAY live localmente sulla postazione del medico, dal medico stesso al momento della consultazione telematica, e che solo in una seconda fase i dati vengono recuperati dall'estrattore CROSSWAY. La società conclude che l'estrattore CROSSWAY non effettua alcuna aspirazione diretta di questi dati e che la raccolta non può quindi essere considerata illegale. Tuttavia, la società ha dichiarato di essere disposta, in alternativa e nel caso in cui la formazione limitata mantenesse la posizione del relatore, a sviluppare il software CROSSWAY in modo che il download dei dati HRi avvenga solo su un'opzione attivabile dai medici.

143. In ogni caso, la società insiste sulla sua trasparenza e buona fede, sostenendo che la CNIL era a conoscenza delle modalità di restituzione dei dati dello storico dei rimborsi alla società CEGEDIM SOFTWARE MEDIDAUX, poi CEGEDIM SANTÉ. A sostegno della sua difesa, produce una lettera del 25 aprile 2013 in cui CEGEDIM LSOLINES MEDIDAUX informava la CNIL dell'integrazione nel software dei medici di una funzionalità che permetteva di conservare i dati dello storico dei rimborsi.

144. Infine, l'azienda insiste sul fatto che l'accesso ai dati del teleservizio HRi da parte degli operatori sanitari è raccomandato dal GIE SESAME-Vitale e che, più in generale, questa funzionalità di accesso ai dati da parte dei medici ha un obiettivo di salute pubblica e di prevenzione della iatrogenesi dei farmaci, in modo che essi possano avere accesso alle informazioni sui farmaci, le cure e gli esami prescritti ai loro pazienti da altri medici.

145. Il relatore insiste sul fatto che la difficoltà non risiede nel fatto che il medico ha accesso ai dati di HRi teleservices e può trasmetterli nella cartella informatizzata del paziente, ma nel fatto che dal momento in cui il medico li inserisce, la società CEGEDIM SANTÉ viene trasmessa automaticamente, senza che il medico abbia ritenuto necessario inserire queste informazioni nella cartella del paziente all'interno del suo software di lavoro, prendendole nella cartella.

146. La formazione ristretta prevede che, a differenza dei dati del teleservizio ALDi, la consultazione dei dati del teleservizio HRi da parte del medico comporti il loro scarico automatico, per una durata di dodici mesi, nella cartella clinica informatizzata del software CROSSWAY.

147. Non prevedendo un passaggio intermedio attraverso il quale il medico possa consultare i dati senza che la consultazione effettui automaticamente il download nella cartella clinica, la formazione ristretta ritiene che CEGEDIM SANTE acquisisca automaticamente i dati dal teleservizio HRi nel flusso CROSSWAY, nel momento in cui il medico

si collega al software per consultare i dati e senza alcuna azione aggiuntiva da parte sua.

148. La formazione ristretta ritiene inoltre che il criterio di praticità invocato dalla società in difesa, secondo cui i medici hanno accesso diretto alle informazioni sui medicinali, le cure e gli esami prescritti ai loro pazienti da altri medici per individuare eventuali incompatibilità, non possa giustificare l'uso dei dati dei pazienti in contrasto con le norme.

149. La formazione ristretta sottolinea inoltre che non è l'accesso ai dati del teleservizio HRi da parte dei medici o il loro versamento nella cartella informatizzata del paziente a essere messo in discussione, ma il fatto che l'estrattore non preveda la possibilità di consultare i dati senza il download automatico nella cartella del paziente e quindi, di fatto, senza l'aspirazione di questi dati da parte della società CEGEDIM tramite l'estrattore CROSSWAY. La formazione ristretta ritiene che questa raccolta di dati avvenga in mancanza di consapevolezza degli articoli L. 162-4-3 e R. 162-1-10 del Codice di Sicurezza Sociale e dell'articolo R. 1111-8-6 del Codice di Sanità Pubblica, che non prevede che un attore privato raccolga direttamente, attraverso la mera consultazione da parte di un medico del teleservizio HRi, i dati in esso contenuti.

150. Infine, per quanto riguarda la lettera del 25 aprile 2013 prodotta dalla società, la formazione ristretta osserva che la società non dettaglia le modalità di consultazione, di scaricamento nella cartella clinica del paziente e di successiva trasmissione dei dettagli della storia dei rimborsi alla società CEGEDIM LAWICIELS MEDICAUX. Tuttavia, la formazione limitata sottolinea che non è l'accesso ai dati da parte dei medici a essere messo in discussione, ma il modo in cui vengono trasmessi alla società. Pertanto, il contenuto di questa lettera non è tale da influenzare la caratterizzazione dell'inadempienza.

151. Alla luce di quanto sopra, la formazione ristretta ritiene che l'inosservanza dell'articolo 5, paragrafo 1, lettera a), del GDPR sia costituita dalla raccolta di dati da parte di HRi teleservice.

III. Sulla consegna di misure correttive e sulla pubblicità

152. L'articolo 20, paragrafo IV, della legge sull'informatica e le libertà prevede: Se il responsabile del trattamento o il suo incaricato del trattamento non rispetta gli obblighi derivanti dal regolamento (UE) 2016/679 del 27 aprile 2016 o dalla presente legge, il presidente della Commissione nazionale per l'informatica e le libertà può anche, se del caso, dopo avergli inviato l'avvertimento di cui al punto I del presente articolo o dopo aver pronunciato nei suoi confronti una o più delle misure correttive, di più delle seguenti misure:

(2) l'ordine di conformare il trattamento agli obblighi derivanti dal regolamento (UE) 2016/679 del 27 aprile 2016 o dalla presente legge o di soddisfare le richieste presentate dall'interessato ai fini dell'esercizio dei suoi diritti, che può essere accompagnato, salvo i casi in cui il trattamento sia effettuato dallo Stato, da una sanzione pecuniaria, il cui importo non può superare i 100.000 euro per ogni giorno di ritardo dalla data fissata dalla formazione vincolata;

(7) Ad eccezione dei casi in cui il trattamento è effettuato dallo Stato, una sanzione amministrativa pecuniaria non superiore a 10 milioni di euro o, nel caso di un'impresa, al 2% del fatturato totale annuo dell'esercizio precedente, trattenendo l'importo più elevato. Nei casi di cui agli articoli 53 e 6 dell'articolo 83 del Regolamento (UE) 2016/679 del 27 aprile 2016, tali massimali sono aumentati rispettivamente a 20 milioni di euro e al 4% del fatturato. La formazione ristretta tiene conto, nella determinazione dell'importo dell'ammenda, dei criteri specificati nel medesimo articolo 83 .

153. L'articolo 83 del GDPR, richiamato dall'articolo 20(IV) della legge sulla protezione dei dati, prevede che ogni autorità di controllo garantisca che l'amministrazione

Le ammende inflitte ai sensi del presente articolo per le violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 devono essere, in ogni caso, effettive, proporzionate e dissuasive, prima di specificare gli elementi da prendere in considerazione per decidere se imporre un'ammenda amministrativa.

A. Sull'imposizione di una sanzione amministrativa e sul suo importo

154. L'azienda sostiene di non aver trattato dati personali in buona fede. Osserva che è stata avviata un'azione legale nei suoi confronti più di due anni dopo i controlli e i test, senza che la CNIL le avesse precedentemente notificato la sua posizione divergente sulla valutazione della natura dei dati trattati e non le avesse quindi dato la possibilità di espletare le formalità richieste. Sostiene inoltre che la CNIL era a conoscenza del trattamento effettuato dalla società a partire dai controlli effettuati con CEGEDIM LAWOGIA MEDICAUX nel 2002 e nel 2012, senza che la società sia stata invitata a presentare una domanda di autorizzazione. Infine, la società afferma che, dato il suo status di subappaltatore, non può essere ritenuta responsabile delle presunte violazioni, in quanto le disposizioni dell'articolo 66 della legge sulla protezione dei dati e dell'articolo 5, paragrafo 1, lettera a), del GDPR stabiliscono obblighi applicabili solo ai responsabili del trattamento.

155. Per quanto riguarda l'importo dell'ammenda proposta dal relatore, la società ritiene che sia sproporzionato e che non sia stato dimostrato come la quota del fatturato di CEGEDIM SANTÉ in relazione all'attività dell'osservatorio sia stata presa in considerazione nella determinazione di tale importo.

156. In primo luogo, la formazione ristretta sottolinea che le violazioni accertate ai sensi dell'articolo 66 della legge sull'informatica e le libertà e dell'articolo 5, paragrafo 1, lettera a), del GDPR le sono imputabili in qualità di responsabile del trattamento in questione.

157. In secondo luogo, al fine di valutare la fondatezza dell'ammenda, la formazione ristretta sottolinea che il criterio di cui all'articolo 83, paragrafo 2, lettera a), del GDPR relativo alla

La gravità della violazione deve essere applicata tenendo conto della natura, della portata del trattamento e del numero di persone interessate da quest'ultimo.

158. La formazione ristretta ritiene che le carenze individuate siano gravi. Infatti, sia il GDPR che la legge sulle tecnologie dell'informazione e le libertà prevedono un principio che vieta il trattamento di particolari categorie di dati, tra cui i dati sulla salute. Il regime previsto dalla sezione 3 ("Trattamento dei dati personali nel campo della salute") del capitolo III ("Obblighi del responsabile del trattamento e del subappaltatore") della legge sulle tecnologie dell'informazione e le libertà costituisce pertanto un'eccezione a questo principio di divieto di trattamento, che deve essere interpretato in modo rigoroso. Il rigoroso rispetto delle disposizioni di questa sezione da parte delle persone incaricate del trattamento che intendono trattare dati sanitari è quindi essenziale per non violare i diritti fondamentali delle persone interessate. Nel caso in questione, tuttavia, la formazione ristretta rileva che la società non ha rispettato gli obblighi previsti dall'articolo 66 della legge del 6 gennaio 1978, come modificata. Inoltre, raccogliendo dati dal servizio di telesoccorso HRi, il cui uso e accesso è strettamente regolamentato, la società ha violato il principio di liceità del trattamento dei dati personali a fini commerciali, che deve essere preso in considerazione nel determinare l'importo della multa.

159. La formazione limitata riflette anche la natura massiccia del trattamento. In effetti, il numero di linee ricevute tra il 1° gennaio 2021 e il 2 aprile 2021 dalla società CEGEDIM SANTÉE è superiore a [..., il che è considerevole e dimostra la portata del trattamento in questione. Questa ampiezza e la ricchezza dei dati elaborati si riflettono anche nella loro profondità storica: l'azienda recupera i dati attraverso il servizio di telesoccorso HRi da una profondità di dodici mesi.

160. In terzo luogo, la formazione ristretta ritiene che non si possa rimproverare alla CNIL di non aver chiesto alla società di regolarizzare prima il suo trattamento, anche se ne era a conoscenza prima del controllo effettuato nel 2021. La formazione ristretta sottolinea che, conformemente al principio di responsabilità introdotto negli articoli 5, paragrafo 2, e 24

del GDPR, spetta agli attori informarsi sui propri obblighi e compiere i passi necessari per essere in regola. La formazione ristretta ritiene, secondo il criterio di cui all'articolo 83, paragrafo 2, lettera b), del GDPR, che l'azienda sia stata negligente nel ritenere di potersi astenere dal rispettare l'articolo 66 della legge sull'informazione e sulle libertà per effettuare il trattamento dei dati sanitari. Nella misura in cui il trattamento dei dati sanitari è l'oggetto principale e storico dell'attività dell'azienda, la formazione ristretta ritiene che l'azienda non potesse, in buona fede, ignorare i propri obblighi ai sensi della normativa sulla protezione dei dati personali, in particolare in quanto attore specializzato nel settore della salute e alla luce della suddetta dottrina disponibile, tanto più che altre aziende che attuano trattamenti simili nello stesso mercato hanno richiesto autorizzazioni.

161. In quarto luogo, la formazione ristretta ritiene che il criterio di cui all'articolo 83, paragrafo 2, lettera g), del GDPR debba essere applicato alle categorie di dati personali interessate dalle carenze.

162. La formazione ristretta sottolinea che si tratta in particolare di dati sanitari, che costituiscono categorie particolari di dati ai sensi dell'articolo 9 del GDPR, i cosiddetti dati sensibili. Data la natura dei dati in questione e il settore in cui opera, la formazione limitata ritiene che l'azienda avrebbe dovuto mostrare una particolare vigilanza sul trattamento che sta effettuando.

163. Infine, la formazione ristretta osserva che, conformemente alle disposizioni dell'articolo 20, paragrafo IV, della legge sull'informatica e le libertà, CEGEDIM SANTÉ è passibile di una sanzione pecuniaria fino a 20 milioni di euro o al 4% del suo fatturato mondiale totale annuo per l'esercizio precedente; l'importo più elevato viene trattenuto. La Commissione osserva che il fatturato di CEGEDIM LAWICIELS MEDICAUX France, di cui la società CEGEDIM SANTÉ ha ripreso la totalità, è stato nel 2021.

164. Pertanto, alla luce delle carenze individuate, della capacità finanziaria della società e dei criteri pertinenti dell'articolo 83, paragrafo 2, del GDPR di cui sopra, la formazione ristretta ritiene che una multa di 800 000 euro (800 000 euro) sia giustificata.

B. Sulla questione dell'ingiunzione

165. Da un lato, per quanto riguarda l'ordine proposto dal relatore di anonimizzare i dati o di rendere il trattamento conforme alle disposizioni dell'articolo 66 della legge del 6 gennaio 1978, come modificata, la formazione ristretta osserva che la società ha indicato modifiche sostanziali al trattamento durante la procedura di sanzionamento. Secondo le informazioni fornite dalla società nelle sue osservazioni difensive, i dati del flusso CROSSWAY sono ora trasmessi direttamente alla società ..., senza l'intermediazione della società CEGEDIM SANTÉ.

166. Di conseguenza, in ogni caso, non è necessario emettere un'ordinanza per renderla conforme alle disposizioni dell'articolo 66 della legge del 6 gennaio 1978, modificata per il trattamento effettuato dalla società CEGEDIM SANTÉ, poiché quest'ultima non interviene più in tale contesto.

167. D'altra parte, la società chiede, se la formazione dovesse mantenere il mancato rispetto dell'articolo 5, paragrafo 1, lettera a), del GDPR, di non seguire la proposta del relatore di cessare la raccolta dei dati da HRi teleservice. Propone, in alternativa, di modificare il software CROSSWAY in modo da eliminare la funzionalità di scarico automatico dei dati HRi da parte dei medici e di prevedere lo scarico di questi dati nella cartella clinica solo su azione positiva dei medici.

168. La formazione ristretta riconosce che la società è disposta, in quanto produttrice del software, a sviluppare il flusso CROSSWAY in modo che il trattamento sia in linea con le disposizioni applicabili. Inoltre, per le ragioni sopra esposte, legate principalmente al fatto che CEGEDIM SANTE non è stata responsabile del trattamento

dal luglio di questo mese, ma solo l'editore del software, la formazione ristretta ritiene che non ci sia bisogno di un'ingiunzione.

C. Sulla pubblicità

169. Il relatore ritiene che la pubblicità della sanzione sia necessaria in considerazione della gravità delle infrazioni in questione e del numero di persone interessate. Ritiene che la pubblicità contribuirà a informare gli interessati dell'esistenza del trattamento dei loro dati, compresi quelli sanitari, di cui la grande maggioranza non è a conoscenza.

170. In difesa, l'azienda contesta la proposta del relatore di rendere pubblica la decisione e sostiene che se la violazione fosse così grave come sostiene il relatore, la CNIL non avrebbe permesso che continuasse senza azioni correttive dal 2014. Aggiunge che la pubblicità della delibera causerebbe un danno commerciale e creerebbe un rischio di divulgazione di informazioni sull'hosting e la trasmissione di dati che potrebbero influire sulla sicurezza dei dati.

171. L'azienda aggiunge di non avere i mezzi finanziari per comunicare con i medici al fine di convincerli a continuare a far parte dell'osservatorio e che, in generale, la pubblicità della sanzione la farebbe incorrere in un rischio reale per quanto riguarda la sua sopravvivenza e la sua precaria salute finanziaria.

172. Infine, ritiene che il relatore non possa utilmente far valere, sulla base della pubblicità della sanzione, la necessità di informare le persone sul trattamento effettuato dall'azienda, pur non ammettendo alcuna mancata detenzione delle informazioni degli interessati, che le persone sono state informate individualmente dal loro medico dell'esistenza del trattamento e che l'azienda non ha contatti diretti con le persone interessate.

173. La formazione ristretta ritiene che la pubblicità della presente decisione sia giustificata in considerazione della gravità delle infrazioni in questione e del numero di persone interessate. Ricorda che, in caso di pubblicità, le informazioni relative alla riservatezza dei casi di cui all'articolo L. 151 del Codice di commercio sono nascoste dalle decisioni pubblicate dalla formazione ristretta. Per quanto riguarda l'argomentazione relativa all'impatto della pubblicità sui rapporti con i medici partner, sottolinea che l'azienda sarà in grado di comunicare con i propri partner le azioni intraprese per rispettare i propri obblighi.

174. Per quanto riguarda l'informazione delle persone, la formazione ristretta ritiene che, sebbene la società non denunci il fatto di non aver informato le persone interessate del trattamento esistente nel presente procedimento, sembra essenziale che le persone interessate siano a conoscenza delle carenze commesse dalla società, in particolare per poter far valere i propri diritti.

175. La misura deve essere proporzionata, a condizione che la decisione non identifichi più la società per nome dopo due anni dalla sua pubblicazione.

DA QUESTI TERRENI

La formazione ristretta della CNIL, dopo aver deliberato, decide di:

ordinare una sanzione amministrativa nei confronti della società CEGEDIM SANTÉ per un importo di 800.000 euro (800.000 euro) alla luce delle violazioni dell'articolo 66 della legge n. 78-17 del 6 gennaio 1978, come modificata, e dell'articolo 5, paragrafo 1, lettera a), del GDPR;

rendere pubblica, sul sito web della CNIL e sul sito web di Legifrance, la sua delibera, che non permetterà più di identificare l'azienda per nome dopo un periodo di due anni dalla sua pubblicazione.

Il Presidente

Philippe-Pierre CABOURDIN

La decisione può essere appellata al Consiglio di Stato entro due mesi dalla sua notifica.